



CHAPTER 2

Managing Administrative Settings for Cisco DMS Components and Users

Revised: March 12, 2009, OL-15762-02



Activation

Software feature modules for Cisco DMS are purchased and licensed separately. Features are hidden from all users until you purchase and install the required license to use them, and even then remain hidden from users whose privilege levels are low. To understand feature licenses and learn how to install them, see [Managing Licenses for Features and Components of Cisco DMS, page 2-3](#). To learn how user access to features is restricted by the combination of licenses and user privilege levels, see [Understanding User Roles in DMS-Admin, page 2-9](#). To learn which software feature modules are available for you to purchase, see <http://www.cisco.com/go/dms>.

Topics in this chapter describe features of User Guide for Cisco Digital Media Manager 5.1.xDMS-Admin that help you to create and administer user accounts, permissions, and profiles for Cisco DMS products, configure the settings for authentication, administer the licenses for software feature modules, and more.

- [Using Dashboard Gauges for DMS-Admin, page 2-2](#)
- [Managing Licenses for Features and Components of Cisco DMS, page 2-3](#)
- [Managing User Accounts and Authentication Settings, page 2-5](#)
- [Backing Up and Restoring, page 2-18](#)
- [Managing Email, SNMP, Alerts, and Notifications, page 2-18](#)
- [Viewing Appliance Processes and Restarting Appliances Remotely, page 2-22](#)

Starting DMS Administration Module (DMS-Admin)

Procedure

- Step 1** Do one of the following:
- Click **Administration** on the DMM dashboard.
 - Choose **Administration** from the global navigation.
-

Using Dashboard Gauges for DMS-Admin

When you start DMS-Admin after you have installed at least the license key to use one software feature module, the landing page by default is a dashboard that shows five gauges. In addition, you can choose to see and use this dashboard at any time.

The dashboard for DSM-Admin centralizes all features for system monitoring and log collection. If problems of any kind interfere with the data-collection processes that populate its gauges, they will show question marks in addition to the best data that is available. In this case, check that your systems and network are configured and working correctly.

Procedure

Step 1 Click the **Dashboard** tab.

Related Topics:

[UI Reference: Dashboard Gauges, page 2-2](#)

UI Reference: Dashboard Gauges

Navigation Path

Administration > Dashboard.

Table 2-1 DMS-Admin Gauges

Name	Description
Alerts	Shows the total count of email and SNMP notification messages delivered in the past 1 hour. To jump directly to the Alerts page, click View Alerts .
License Features	Lists software feature module licenses that are installed on your DMM appliance and describes any constraints that these licenses impose.
Status	<p>Summarizes the current state of your Video Portal appliance and of all registered DMPs in your network, assuming that you set up the hardware and installed the separately licensed software features for these device types. This gauge organizes data in these subsections:</p> <ul style="list-style-type: none"> Digital Media Players—Counts the total number of registered DMPs and specifies how many were reachable or unreachable when you loaded this gauge in your browser. Click View All DMPs and DMP Groups to jump directly to the DMP Manager page. Video Portal Appliance—Shows you whether your Cisco Video Portal appliance was unreachable at any time in the past 1 hour. Counts the number of Video Portal deployments that were pending or completed when you loaded this gauge in your browser. To jump directly to the live HTTP URL of your Video Portal, click Go to Video Portal. To jump directly to the DMM-VPM landing page, click Manage Video Portal. This DMM release supports your use of only one Video Portal appliance. <p>To update the data that this gauge shows, refresh your browser.</p>

Table 2-1 DMS-Admin Gauges (continued)

Name	Description
System Information	<p>This gauge:</p> <ul style="list-style-type: none"> • Tells you the installed release version of your DMM server software. • Shows free disk space and used disk space on your DMM appliance and Video Portal appliance. <ul style="list-style-type: none"> – The disk space descriptions for your DMM appliance pertain only to the /dm2 partition where local copies of assets are stored temporarily after you upload them. – Even though your Video Portal appliance might report that it has ample free disk space, you should not use it to store video files or any other data except the files that Cisco DMS generates. We do not support any use of your Video Portal appliance as a storage server. Any unsupported data that you store on it will be lost irretrievably each time that you upgrade, restore, or reinstall Cisco software. • Tells you whether the most recent replication of data succeeded between your Cisco DMS appliances.
Users Logged In (Past 1 Hour)	<p>Counts the total number of users who logged in to each of your DMS appliances over the past 1 hour. To jump directly to the Users page in DMS-Admin, click View All Users.</p>

Related Topics

- [Using Dashboard Gauges for DMS-Admin, page 2-2](#)
- [Managing User Accounts and Authentication Settings, page 2-5](#)
- [Managing Email, SNMP, Alerts, and Notifications, page 2-18](#)
- [Managing and Grouping Your DMPs, page 3-12](#)
- [Chapter 4, “Managing Desktop Video.”](#)

Managing Licenses for Features and Components of Cisco DMS

This section contains these topics:


- [Obtaining and Installing License Keys for Software Features, page 2-3](#)
- [Viewing the List of Installed Licenses, page 2-5](#)

Obtaining and Installing License Keys for Software Features

When you log in to DMM before you have installed the license key to use *any* software feature module, the landing page by default is the page in DMS-Admin (at Licensing > Install/Upgrade Licensing) where you can install a license key.

To obtain a license key and use it to activate the DMM software feature modules that you have purchased, do the following:

Procedure

-
- Step 1** Confirm that you know the serial number and IP address for your DMM appliance. If you do not know the serial number or IP address, do the following:
- a. Use the **admin** username and its associated password at the login prompt on your DMM appliance, to log in to AAI. In the displayed menu, the SHOW_INFO option is highlighted by default.
 - b. Press **Enter**, and then write down these values that AAI shows to you:
 - The IP address for your DMM appliance.
 - The 10-character serial number for your DMM appliance.
- Step 2** Compose an email message that includes or identifies *all* of the following:
- All Cisco sales order numbers that were associated with your Cisco DMS purchase (such as, appliances, software modules for DMM, and DMPs), including even the sales order numbers for all purchased products and services that are not components of Cisco DMS.
 - The 10-character DMM appliance serial number that AAI showed to you in Step 1-b.
 - Your email address.
 - The name of your organization.
 - The department name within your organization.
 - The DMM software feature module (or modules) that you purchased.
 - If you purchased DMM software feature modules for digital signage or enterprise TV, include the number of DMPs that you will manage centrally. Permitted increments for the number of DMPs are multiples of 10.
- Step 3** Send the email message to dms-softwarekeys@cisco.com.
- Step 4** After you receive the license key file from Cisco, save a local copy of it.
- Step 5** To load DMM in a web browser, use the DMM appliance IP address that you saw in AAI (http://<DMM_IP_address>:8080/).
- Step 6** To use DMS-Admin, do one of the following:
- Click **Administration** on the DMM dashboard, .
 - Choose **Administration** from the global navigation.
- Step 7** Choose **Licensing > Install/Upgrade Licensing**.
- Step 8** Click **Browse**, find and click the license file where you saved it, and then click **Open**.
-  **Note** The format for licenses in Cisco DMS 5.x differs from the obsoleted format that was used in earlier DMS releases. This release does not support license files that use the obsoleted format, and will reject such licenses as invalid if you try to install them.
-
- Step 9** Click **Install License**.
- The pertinent software feature module is now enabled.
-

**Tip**

If you receive multiple license key files, repeat the procedure until all of your licenses are installed.

Related Topics

- [Viewing the List of Installed Licenses, page 2-5](#)

Viewing the List of Installed Licenses

To see which DMS features you have licensed:

Procedure

Step 1 Choose **Licensing > View Licensing**.

Alternatively, the License Features gauge on the DMS-Admin dashboard also lists software feature module licenses that are installed on your DMM appliance. See [Using Dashboard Gauges for DMS-Admin, page 2-2](#).

Related Topics

- [Obtaining and Installing License Keys for Software Features, page 2-3](#)

Managing User Accounts and Authentication Settings

Features of DMS-Admin help you to:

- Assign differing levels of access and permissions to users of DMM feature modules, Video Portal Reports, and Video Portal, depending on their roles and responsibilities.
- Make choices to enable or disable user authentication.
- Choose and configure an authentication method, such as LDAP (Active Directory). Optionally, import from your LDAP server the basic settings for any of its user accounts and user groups.

This section contains these topics:

- [Understanding User Management Concepts and Workflow, page 2-6](#)
- [Configuring User Accounts Manually, page 2-7](#)
- [Understanding User Roles in DMS-Admin, page 2-9](#)
- [Configuring Authentication Settings, page 2-9](#)

Understanding User Management Concepts and Workflow

This worksheet will help you to understand the expected sequence of user management tasks as well as the important concepts that underlie them:

✓	Task
<input type="checkbox"/>	<p>1. Work with any preexisting user accounts that you migrated from an earlier Cisco DMS release.</p> <p>If you upgraded to Cisco DMS 5.1.x from any 4.1.x release on which you had licensed the features for digital signage networks, it is possible that some formerly redundant usernames from your licensed software modules are now unique. This will have occurred if an identical username was configured for use in both DMM-VPM and DMM-DSM. As just one possible example, you might have configured the username <i>admin</i> to work in both of these software modules. Migration during your upgrade will have consolidated all user accounts into DMS-Admin, and any redundant usernames from your preexisting DMM-DSM configuration now have a suffix appended to them. The suffix is exactly: <i>_dsm</i>. So, where this scenario supposes that the twice-used username was <i>admin</i> in Cisco DMS 4.1.x, the two migrated usernames in this newer Cisco DMS release would be:</p> <ul style="list-style-type: none"> • <i>admin</i> (for the user account that you migrated from DMM-VPM). • <i>admin_dsm</i> (for the user account that you migrated from DMM-DSM). <p>You might now want to assign sufficient access rights and permissions to <i>one</i> of the migrated accounts so that you can delete the <i>other</i> account safely, without disrupting the approvals workflow or other established practices in your organization. In this example scenario, the ideal result might be that you are left with only one user account called <i>admin</i>, whose assigned rights and permissions across all of your installed Cisco DMS products are at least sufficient to manage all suitable features for desktop video and digital signage.</p>
<input type="checkbox"/>	<p>2. Create new user accounts. To create user accounts manually for DMM software modules, Video Portal Reports, and your Video Portal, you use DMS-Admin. Any user accounts that you create manually will be in addition to those whose creation you automate by importing user account data from an Active Directory server.</p> <p>By default, each new user account that you create has the DMS-Admin user role of “Other” until you assign access rights and privileges to it in at least one DMM software module. User accounts are severely limited in their access when they have this user role.</p>
<input type="checkbox"/>	<p>3. Create user groups. To create a new user group, choose Administration > Users > Create Group, and then enter the required values. To save your work, click Save.</p>
<input type="checkbox"/>	<p>4. Assign access rights and permissions.</p> <p>After you create user accounts, you assign access rights and privileges separately for these users in the DMM software modules that pertain to them. The access rights and privileges that you assign to a user account are always specific to an environment for desktop video or digital signage (the latter of which includes enterprise TV). Therefore, you assign access rights and privileges to users in the individually licensed and separately installed DMM software modules that are applicable per user:</p> <ul style="list-style-type: none"> • For desktop video, choose Video Portal > Users > User Accounts. • For digital signage or Enterprise TV, choose Digital Signage > Settings > User Accounts.
<input type="checkbox"/>	<p>5. Assign users to user groups.</p> <p>When you first create a user account in DMS-Admin, you can associate the account with a user group immediately or you can do so after you assign access rights and permissions to the user.</p>

Related Topics

- [Configuring User Accounts Manually, page 2-7](#)
- [Deleting User Accounts, page 2-8](#)

- [Configuring Authentication Settings, page 2-9](#)
- [Understanding User Roles in DMS-Admin, page 2-9](#)
- [Chapter 3, “Managing Digital Signage and Enterprise TV”](#)
- [Chapter 4, “Managing Desktop Video”](#)

Configuring User Accounts Manually

This section contains these topics:

- [Creating and Editing User Accounts, page 2-7](#)
- [Deleting User Accounts, page 2-8](#)

Creating and Editing User Accounts



Tip

You cannot create any new user accounts manually while your authentication method is LDAP. To understand the authentication options for Cisco DMS products, see [Configuring Authentication Settings, page 2-9](#).

You can create a new user account or to edit the settings manually for an account.

Procedure

- Step 1** Click the **Users** tab, and then do one of the following:
- To create a new account, click **Add New User**, and then enter the required values in the Add New User dialog box.
 - To edit an account, click its entry in the untitled table that describes all user accounts, choose **Options > Edit User**, and then make changes to its values in the Edit User dialog box.
- If you do not understand your options in the {Add New|Edit} User dialog box, see [Table 2-2 on page 2-8](#).
- Step 2** (Optional) Enter contact information and assign the user to a user group.
- Step 3** Click **Save**.
-

Related Topics

- [UI Reference: Elements to Configure User Account Settings, page 2-8](#)
- [Deleting User Accounts, page 2-8](#)

UI Reference: Elements to Configure User Account Settings

Navigation Path

Administration > Users

Table 2-2 Elements for Creating and Editing User Accounts Manually

Element	Description
First Name	This required value might be identical for multiple users.
Last Name	This required value might also be identical for multiple users.
Email Address	The email address to be associated with this user account.
Username	A unique username. The name is unique in the sense that you have not used it as the name for any other user account for any component of Cisco DMS. You must enter the username.
Password	The password for the user account. You must enter a password, then reenter it.
Re-enter password	
Active list	Signifies whether the account holder is an active or inactive user of Cisco DMS. Alternatively, signifies whether the account holder is active in your organization.

Optional Contact Info

Company	The agency, corporation, nonprofit organization, or other such institution to be associated with this user account.
Department	The department within the institution.
Phone	The telephone number to be associated with this user account.

Optional Group Selection

Unlabeled check box	Marks the groups to which this user should belong.
Groups column	Shows the group name.
Description column	Optional, brief description of the group and its purpose.

Deleting User Accounts

You cannot delete the superuser account but you can delete any other user account.

Procedure

-
- Step 1** Click the **Users** tab and then, in the untitled table, click the user account that should be deleted.
To mark multiple user accounts for deletion, Ctrl-click.
- Step 2** Choose **Options > Delete User**.
-

Related Topics

- [Creating and Editing User Accounts, page 2-7](#)
- [UI Reference: Elements to Configure User Account Settings, page 2-8](#)

Understanding User Roles in DMS-Admin

User roles in DMS-Admin are the automatic result of a logical operation. You cannot use DMS-Admin to assign a user role directly to any user.

In some cases, users who are authorized to log in to one DMM software module will be authorized also to log in to at least one additional software module. The DMS-Admin user role that you see for a user account is based on *all* privileges and access settings that the user has, combined across *all* of your licensed and installed DMM software modules.

Table 2-3 Logic That Determines User Role Designations in DMS-Admin

User Role	Logic
Admin	This user role is assigned automatically to any user who is an administrator in any DMM software module. These users have full read/write access to all users and user groups in DMS-Admin and can manage settings for them.
Group Admin	This user role is assigned automatically to any user who is a content author for desktop video but is not an administrator in any DMM software module. These users cannot see information about user accounts and groups in DMS-Admin, nor can they create, edit, or delete them. However, these users can create user groups as part of the workflow in DMM-VPM when they assign the rights to view a new or preexisting video part.
Read-Only	This user role is assigned automatically to any user who is neither a content author for desktop video nor an administrator in any DMM software module. These users can see information about users and user groups in DMS-Admin but cannot create, edit, or delete them.
Other	This user role in DMS-Admin is assigned automatically to any user who has not been granted any explicit access settings or privileges in any DMM software module, or who is part of the audience for a Video Portal but has no other privileges. These users are prevented from logging in to any DMM software module.

Configuring Authentication Settings

Two types of user authentication are available in Cisco DMS. *Embedded authentication* is completely native to DMM, while *LDAP authentication* causes Cisco DMS products to rely on a Microsoft Active Directory server.

Although Cisco DMS always requires one kind of authentication or the other, you can enable or disable authentication for users of Video Portal and Video Portal Reports. In addition, you can choose the user authentication method for DMM-DSM, DMM-ETV, DMM-VPM, Video Portal, and Video Portal Reports.

Procedure

Step 1 Choose **Settings > Authentication**.

The Authentication page contains four tabbed property sheets: *Select Mode*, *Define Filter*, *Synchronize Users*, and *Manage Attributes*. In most production environments, you can expect to use the Select Mode property sheet only one time. Nonetheless, your choices on the Select Mode property sheet determine whether you have access to the other three property sheets. Therefore, Select Mode is by default the only active tab.

Step 2 Use elements on the Select Mode property sheet to enable or disable authentication and to choose an authentication mode.

Step 3 Click **Update**, and then consider which of the following scenarios applies to you.

- No Authentication
 - If you disabled authentication—where you had not used *any* authentication mode previously—you are done with this procedure. You did not change anything.
 - If you disabled authentication—where you had used LDAP authentication previously—you must explicitly choose whether Cisco DMS should keep a local copy of the user account data that originated from your Active Directory server. If you want to save the local copy, check the **Save LDAP Users** check box. Otherwise, the local copy is discarded. You are done with this procedure.
- Embedded Authentication
 - If you enabled embedded authentication—where you had not used *any* authentication mode previously—you are done with this procedure.
 - If you enabled embedded authentication—where you had used LDAP authentication previously—you must explicitly decide whether Cisco DMS should keep a local copy of the user account data that originated from your Active Directory server. If you want to save the local copy, the **Save LDAP Users** check box. (When you save a local copy, DMS-Admin changes all of the user passwords in it automatically to *CiscoDMMvp99999*. This security feature protects your network and user data if anyone gains unauthorized access to the exported file, because your Active Directory server recognizes that the password as incorrect if anyone attempts to use it.) Otherwise, the local copy is discarded. You are done with this procedure.
- LDAP Authentication

If you enabled LDAP authentication, the three tabs—*Define Filter*, *Synchronize Users*, and *Manage Attributes*—that were previously dimmed are now available for you to click and use. To actually use LDAP authentication after you choose it as the mode, you must also use features under the Define Filter tab to configure and add a new agreement, and then use features under the Synchronize Users tab to submit the new agreement for synchronization.

Step 4 (Optional) Click **Define Filter**, and then use elements on the Define Filter property sheet to define, validate, and add one LDAP filter at a time.

Step 5 Do both of the following:

- a. Choose **Synchronize Users > LDAP Bookmarks**, and then use elements on the LDAP Bookmarks property sheet to do any or all of the following:
 - Choose the synchronization type for, and specify the default access privileges that you will assign to, user accounts that you will import to Cisco DMS because they correspond to a defined Active Directory filter.
 - Use the synchronization type that you chose, so that Cisco DMS synchronizes user accounts that correspond to a defined Active Directory filter.
 - Delete from Cisco DMS all of the user accounts that correspond to a defined Active Directory filter and delete the entry for that filter from DMS-Admin.
- b. Choose **Synchronize Users > Scheduling**, and then use elements on the Scheduling property sheet to choose between manual synchronization and automatic synchronization.



Note Until you have defined at least one filter on the Define Filter property sheet, you will not see any of the elements that [Table 2-6](#) describes.

Step 6 Click **Update**.

- Step 7** (Optional) Click **Manage Attributes**, and then use elements on the Manage Attributes property sheet to:
- Set the associations between DMS-Admin attribute names and their corresponding Active Directory attribute names.
 - Use the predefined and typical names for Active Directory attributes (shown in grey text) or edit those attribute names so they match the names that your Active Directory server uses.
 - Enter the values to use by default in DMS-Admin when a user account attribute is not defined on your Active Directory server.

You must enter a value for each mandatory attribute. You cannot enter a value to use by default for user names, because each user name is unique.

- Step 8** Click **Update**.

The authentication settings that you changed are now in effect.

Related Topics

- [UI Reference: Elements to Choose and Enable the Authentication Mode, page 2-11](#)
- [UI Reference: Elements to Define, Validate, and Add LDAP Filters, page 2-14](#)
- [UI Reference: Elements to Use Manual or Automatic Synchronization, page 2-15](#)
- [UI Reference: Elements to Manage Attributes, page 2-17](#)

UI Reference: Elements to Choose and Enable the Authentication Mode

Navigation Path

Administration > Settings > Authentication > Select Mode

Table 2-4 *Elements for the Authentication Mode*

Element	Description
No Authentication	Requires users who log in to authenticate (enter a username and password) against the user account database for DMM, but does not impose any authentication restrictions for access to Video Portal or Video Portal Reports.
Embedded Authentication	Requires users who log in to DMM-DSM, DMM-ETV, DMM-VPM, Video Portal, and Video Portal Reports to authenticate against a user account database that is native to DMM and is independent of every other type of authentication that you might use in your network.

Table 2-4 Elements for the Authentication Mode (continued)

Element	Description
LDAP Authentication	<p>Automatically deletes all user accounts, except the superuser account. Requires future users to authenticate against the user account data from your Active Directory server when they log in to DMM-DSM, DMM-ETV, DMM-VPM, Video Portal Reports, or Video Portal.</p> <p>Although the user account data originates from your Active Directory server, Cisco DMS <i>does not</i> synchronize (replicate) the data automatically, in real time. Instead, you must resynchronize the user account data whenever you think it is appropriate to do so. You can resynchronize manually or you can schedule synchronizations to recur in the future at intervals that you specify.</p> <p>Note Lightweight Directory Access Protocol (LDAP) is a highly complex data model and communications protocol for user authentication. The LDAP features in Cisco DMS are meant for use by qualified and experienced administrators of Microsoft Active Directory. Unless you are an Active Directory and LDAP expert, we recommend that you choose another option than LDAP.</p> <p>Even though it is possible in Active Directory to use a blank value for a password, Cisco DMS does not allow it. Therefore, when you use LDAP authentication, any user whose Active Directory password is blank will be prevented from logging in to DMM-DSM, DMM-ETV, DMM-VPM, Video Portal, and Video Portal Reports until the password is changed on the Active Directory server. There is no requirement to resynchronize the affected user account in DMS-Admin after you change its password on your Active Directory server.</p> <p>DMS-Admin synchronizes all user accounts in the Active Directory user base that you specify in a filter, excluding the users whose accounts are marked as disabled on your Active Directory server.</p>
SSO Authentication	Enable single sign-on for web-based software that is served from your DMM appliances and Video Portal appliances.
Anonymous	<p>Enables or disables an anonymous LDAP connection between your DMM appliance and your Active Directory server. An anonymous connection is suitable when you want to see or use <i>public</i> information on the Active Directory server. In contrast, if you want to see or use <i>privileged</i> information on your Active Directory server, the server will require you to enter login credentials to prove that you have sufficient access rights. In the latter case, your Active Directory server will reject any attempt to use an anonymous login.</p> <p>This check box is available to you only when you choose LDAP Authentication or SSO Authentication.</p>
Host	Enter the routable IP address or DNS-resolvable hostname for the Active Directory server. This field is available to you only when you choose LDAP Authentication or SSO Authentication.
Port	<p>Enter the TCP port number that your Active Directory server uses for its LDAP communications. This field is available to you only when you choose LDAP Authentication or SSO Authentication.</p> <p>The Active Directory port number by default is 389 for LDAP communications and 636 for LDAPS (Secure LDAP or LDAP over SSL) communications.</p>

Table 2-4 Elements for the Authentication Mode (continued)

Element	Description
Use SSL Encryption	<p>A check box, by which you enable or disable encrypted sign-on. To enable encryption, check the check box; to disable encryption, uncheck it. This check box is available to you only when you choose LDAP Authentication or SSO Authentication.</p> <p>If you chose LDAP Authentication, enabling SSL causes the connections between your DMM appliance and your Active Directory server to use LDAPS. An LDAPS connection is suitable when you want to prevent untrusted third parties from reading credentials that the servers exchange.</p>
Active Directory Certificate File	<p>The method by which to upload the digital certificate that your Active Directory server uses for LDAPS communications. This field is available to you only if you checked the Use SSL Encryption check box.</p> <p>The X.509 certificate that you provide must be DER-encoded and can be supplied in binary or printable (Base64) encoding. If you use Base64 encoding, the certificate file must include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines.</p> <p>To open and use the Upload Certificate File dialog box:</p> <ol style="list-style-type: none"> 1. Click Upload, then, click Add. 2. Browse to the file on a local volume. 3. Click the filename and press Enter. 4. To save your work and dismiss the dialog box, click OK.
Current Certificate File	Identifies the digital certificate that is installed in DMS-Admin for use during LDAPS communication with your Active Directory server.
Administrator DN	<p>Enter the Active Directory server administrator distinguished name.</p> <p>This field is available to you only if you chose LDAP Authentication and unchecked the Anonymous check box.</p>
Password	<p>Enter the password that is associated with the Administrator DN.</p> <p>This field is available to you only if you chose LDAP Authentication and unchecked the Anonymous check box.</p> <p>Tip If an error message tells you that your Active Directory password is not valid, confirm on your Active Directory server that you have not set the “User must change password at next login” flag. DMS-Admin cannot change your password on an Active Directory server. Instead, you must use the user interface that your Active Directory server provides for that purpose. While this flag is set, you are prevented from logging in to any Cisco DMS component until you have changed your password on the Active Directory server.</p>
Update	Saves and applies your work on the Authentication Mode property sheet.
Cancel	Discards your work on the Authentication Mode property sheet and resets all values to their previous configuration.

Related Topics

- [Configuring Authentication Settings, page 2-9](#)
- [UI Reference: Elements to Define, Validate, and Add LDAP Filters, page 2-14](#)
- [UI Reference: Elements to Use Manual or Automatic Synchronization, page 2-15](#)

- [Synchronization Mode](#), page 2-16
- [UI Reference: Elements to Manage Attributes](#), page 2-17

UI Reference: Elements to Define, Validate, and Add LDAP Filters

Navigation Path

Administration > Settings > Authentication > Define Filter

Table 2-5 Elements for Filters


Element	Description
Description	Enter a human-readable description for the filter.
User Base DN	Enter the distinguished name of the Active Directory user base that you will search. Note Never use a filter in which you define the user base at the domain level. As one example, the following filter would be unacceptable: <code>dc=cisco, dc=com</code> . Instead, you should use filters that define the user base at a lower level, like this example does: <code>ou=sanjose, dc=cisco, dc=com</code> .
User Filter	Enter a user filter to limit the number of matching user accounts to import from the user base that you specified.
Add	Adds the filter, exactly as entered, without first validating it.
Validate	Validates the filter to confirm, before you add it, that it will return meaningful results. Tip If an error message tells you that filter validation failed, confirm on your LDAP server that your filter did not make any reference to an empty organizational unit (OU) container. Filters fail when they point to empty containers.
Clear	Clears all entries from the Define Filters property sheet.

Related Topics

- [Configuring Authentication Settings](#), page 2-9
- [UI Reference: Elements to Choose and Enable the Authentication Mode](#), page 2-11
- [UI Reference: Elements to Use Manual or Automatic Synchronization](#), page 2-15
- [UI Reference: Elements to Manage Attributes](#), page 2-17

Configuring the Settings for Automatic Synchronization

Procedure

-
- Step 1** Click the calendar icon () to choose the start date for synchronization.
- Step 2** Choose the hour and minute when synchronization should begin, and then choose either AM or PM as the period.

Step 3 From the Repeat Interval list, choose the interval of recurrence:

Interval	Description
Never	Synchronization will occur one time and will not recur.
Every Day	Synchronization will recur once every 24 hours, starting at the specified hour and minute.
Every Week	Synchronization will recur once every 7 days, starting at the specified hour and minute.
Every Month	Synchronization will recur once each month, starting at the specified hour and minute.
Custom	Synchronization will recur at the interval you define, starting at the specified hour and minute. Choose whether the interval type is Days, Weeks, or Months. If the interval type is Days, choose a day of the month from 1 to 30. If the interval type is Weeks, choose the day of the week. If the interval type is Months, choose an interval of recurrence from 1 to 6.

Step 4 (Optional) If, in addition to the start date and time that you specified, a one-time synchronization should also start immediately, check the **Synchronize users immediately** check box. This check box is available to you only if you clicked the Automatic Synchronization radio button.

UI Reference: Elements to Use Manual or Automatic Synchronization

Navigation Path

Administration > Settings > Authentication > Synchronize Users

Table 2-6 Elements for Synchronization

Element	Description
LDAP Bookmarks property sheet	
Synchronization	<p>Tip We recommend that you use the Initial synchronization option and the Overwrite synchronization option during <i>off-peak</i> hours only. These synchronization types are CPU-intensive for your DMM appliance and might cause its performance to drop temporarily to an unacceptable level.</p> <p>One of the following:</p> <ul style="list-style-type: none"> • Initial—Runs a one-time synchronization for a new filter that you never synchronized previously. • Update—Runs an incremental, fast update to find and make up for any differences between user accounts that match your Active Directory filter and your local copy of those user accounts. • Overwrite—Overwrites your local copy of user accounts that correspond to your Active Directory filter with new copies of those user accounts. In addition, deletes your local copy of each user account that has been deleted from Active Directory since the last time that you ran a synchronization. • Delete—Deletes your local copy of user accounts that correspond to a defined Active Directory filter and deletes the entry for that filter from DMS-Admin.

Table 2-6 Elements for Synchronization (continued)

Element	Description
Access Rights	One or both of the following: <ul style="list-style-type: none"> VP—When checked, this check box enables login access to your Video Portal for users who match the corresponding Active Directory filter. When you uncheck the check box, those same users are prevented from logging in to your Video Portal. VPR—When checked, this check box enables login access to see and use Video Portal Reports for users who match the corresponding Active Directory filter. When you uncheck this check box, those same users are prevented from seeing and using Video Portal Reports.
Update	Submits your selections for the type of synchronization and the scope of access that you chose and configured. Synchronization of the specified type starts immediately.
Cancel	Discards any changes you made to the configuration of behaviors for synchronizations and the scope of access, and resets all entries to their previous values on the LDAP Bookmarks property sheet and the Scheduling property sheet.

Scheduling property sheet

Synchronization Mode	Enables one or the other of two possible modes, which are mutually exclusive, to receive updated user account information from your Active Directory server. Click one radio button: <ul style="list-style-type: none"> Manual Synchronization—Mode that requires during each subsequent synchronization of each configured LDAP bookmark that you must choose Administration > Settings > Authentication > Synchronize Users > LDAP Bookmarks; then, click Update. When you choose this mode, you delete any schedule that you configured previously to define automatic synchronizations. Automatic Synchronization—Mode that automates and schedules the recurrence of incremental updates of all user accounts that correspond to your defined Active Directory filters in DMS-Admin. As soon as you click this radio button, fields and elements that were hidden from you become available for your use, so that you can complete this required procedure: Configuring the Settings for Automatic Synchronization, page 2-14.
Update	Submits your selections for the type of synchronization and the scope of access that you chose and configured. Synchronization of the specified type starts immediately.
Cancel	Discards any changes you made to the configuration of behaviors for synchronizations and the scope of access, and resets all entries to their previous values on the LDAP Bookmarks property sheet and the Scheduling property sheet.

Related Topics

- [Configuring Authentication Settings, page 2-9](#)
- [UI Reference: Elements to Choose and Enable the Authentication Mode, page 2-11](#)
- [UI Reference: Elements to Define, Validate, and Add LDAP Filters, page 2-14](#)
- [UI Reference: Elements to Manage Attributes, page 2-17](#)

UI Reference: Elements to Manage Attributes

Navigation Path

Administration > Settings > Authentication > Manage Attributes

Table 2-7 Elements for Attributes Management

Element	Description
DMM Attribute Name	Values that DMS-Admin uses to describe and identify various attributes that it associates with each user account. You cannot change the values in this column. They are for your reference only, to help you enter suitable values (and recognize suitable values when you see them) in the LDAP Attribute Name column and the Values to Use by Default column.
LDAP Attribute Name	<p>Values that your Active Directory server uses—which correspond one-to-one with values in the DMM Attribute Row column—to describe and identify attributes of each user account. In its factory-default configuration, DMS-Admin prepopulates all fields in this column with the most commonplace values that Active Directory servers use for this purpose. If the values for these attributes differ on your Active Directory server or if you prefer to import objects that use other Active Directory attributes, you can edit the values in this column.</p> <p>Ordinarily, DMS-Admin <i>will not</i> import any user account from your Active Directory server when the value in it is blank for any of these attributes:</p> <ul style="list-style-type: none"> • Login User Name—This required value always must be unique. • First Name—This required value might be identical for multiple users. • Last Name—This required value might also be identical for multiple users. <p>However, you can import and synchronize all of the Active Directory user accounts that match your filters, even if some of the user accounts are incomplete because one or more of their attributes have blank values. To prevent these undefined attributes from blocking the import of the user accounts they are meant to describe, you can enter generic values for most attributes in the Values to Use by Default column. DMS-Admin takes the generic values that you enter, and then inserts them automatically where they are needed. Nonetheless, you cannot ever enter a value to use by default for the Login User Name attribute, because each username is unique.</p>
Values to Use by Default	<p>Enter text to insert automatically when the value is blank for the corresponding attribute in an Active Directory user account that you import or synchronize. To ensure that DMS-Admin imports each valid user account that matches a filter, we recommend that you enter values for these attributes:</p> <ul style="list-style-type: none"> • First Name • Last Name <p>For your convenience, you can also enter values to insert automatically when the values are blank for other attributes—such as Company, Department, or Phone Number—but this is optional.</p> <p>Note You cannot enter a value to use by default as the Login User Name value.</p>
Reset to Factory Default	Returns all values in the LDAP Attribute Name column to the most commonplace values that Active Directory servers use. If you entered different values manually because the labels for these attributes differ on your Active Directory server or because you prefer to import user accounts that use other Active Directory attributes, DMS-Admin deletes what you entered.
Update	Saves and applies your work in the Manage Attributes property sheet.

Related Topics

- [Configuring Authentication Settings, page 2-9](#)
- [UI Reference: Elements to Choose and Enable the Authentication Mode, page 2-11](#)
- [UI Reference: Elements to Define, Validate, and Add LDAP Filters, page 2-14](#)
- [UI Reference: Elements to Use Manual or Automatic Synchronization, page 2-15](#)

Backing Up and Restoring

**Note**

Backups that you generate from DMS-Admin in this release do not include any media assets that are stored on any device for any purpose. We recommend that you use another method to create backups of these files.

You can save backups of data on your DMM appliance and your Video Portal appliance (if you have one), and restore from backups that you saved.

Procedure

Step 1 Click **Backup**.

Step 2 Do one of the following:

- Click **Download** to save an encrypted, local copy of the XML data, metadata, database records, and license keys for all of your Cisco DMS components.
 - To restore your DMS components from an encrypted backup file that you saved previously, click **Browse**; then, find and select that file in its subdirectory, press **Enter**, and click **Submit**.
-

Managing Email, SNMP, Alerts, and Notifications

DMS-Admin supports email (SMTP) natively; in addition, you can purchase and install a license key to activate SNMP. In the context of this basic framework for notifications and queries, you can associate alarms with system events and configure the settings to use email or SNMP for the delivery of notification messages.

This section contains these topics:

- [Enabling or Disabling Email, page 2-19](#)
- [Enabling or Disabling SNMP, page 2-19](#)
- [Configuring Alert Reports and Notification Settings, page 2-20](#)
- [Understanding Event Types, page 2-21](#)

Enabling or Disabling Email

You can enable or disable the email service (SMTP) on your DMM appliance. When this service is enabled, DMS-Admin can send email notifications automatically to you or other interested parties whenever system events of predefined types occur.

Before You Begin

To see and use the Settings tab, you must be logged in as an administrator.

Procedure

- Step 1** Choose **Settings > SMTP Server** and then enter the required values so that your DMM appliance can run or will stop the email service. You must enter these values or you cannot send notification messages:

Value	Description
Server Status	Click the radio button to enable or disable the email service.
Host	The routable IP address or DNS-resolvable hostname.
Port	The number to identify which TCP port is reserved for SMTP traffic.

- Step 2** Click **Save**.

Enabling or Disabling SNMP



Caution

SNMPv1 and SNMPv2c are not secure protocols. You cannot use a firewall to secure SNMP traffic.

After you purchase and install a license key to use the SNMP Notification Module, your copy of DMS-Admin can use either the *SNMPv1* protocol or the *SNMPv2c* protocol to respond to Cisco DMS MIB schema-compliant queries from your NMS and send notification messages automatically to your NMS whenever system events of predefined types occur for:

- The MCS hardware platform that underlies DMM and Video Portal appliances.
- Digital Media Manager software modules and Video Portal.
- DMPs (in the sense that, when your DMPs report their events to your DMM appliance, it forwards the appropriate SNMP alerts).



Note

In this release, the SNMP Notification Module does not support:

- The SNMPv3 protocol.
- Any monitoring of Cisco Digital Media Encoders (DMEs). However, you can use the DME console in DMM-VPM for this purpose.

After you purchased a license key to use the SNMP Notification Module, you received (or were told how to obtain) a network management MIB file called *CISCO-DIGITAL-MEDIA-SYSTEMS-MIB.my*, and you received the *agent capabilities* file that describes which MIB objects are supported in this release of

Cisco DMS. You can load the MIB file into the MIB browser for any dedicated NMS that supports SNMP, such as CiscoWorks or HP OpenView. Your NMS can then send SNMP queries to DMS-Admin and represent the responses correctly. The supported MIB objects in this release allow monitoring of:

- **DMS Systems Group**—Models all distributed component parts of this Cisco DMS installation as a single, abstract system.
- **DMS Features Group**—Categorizes licensed and unlicensed features.
- **DMS Inventory Group**—Lists the devices that constitute this Cisco DMS installation and describes their operational status.

SNMP features in this release are read-only; your NMS can use SNMP to submit queries to DMS-Admin but cannot use SNMP to edit the configuration of any Cisco DMS component.

Use the following checklist to track your work with the separately licensed features for SNMP:

✓	Task
☐	<p>1. Configure SNMP server settings for your DMM appliance.</p> <p>a. Choose Settings > SNMP, and then enter the required values so that your DMM appliance can run or will stop the SNMP server service:</p> <ul style="list-style-type: none"> • Server Status—Click the radio button to enable or disable SNMP monitoring. • Host—The routable IP address or DNS-resolvable hostname of the NMS. • Port—The number to identify which UDP port is reserved for SNMP traffic. • Community String—A password that identifies the community of the external SNMP server to which DMS conveys notifications. By default, the entry is <i>public</i>. <p>b. Click Save.</p>
☐	<p>2. Load both the <i>CISCO-DIGITAL-MEDIA-SYSTEMS-MIB.my</i> file and its corresponding “agent capabilities” file into the MIB browser for your NMS. Manufacturer documentation for your NMS should tell you how to load these files. When your NMS prompts you to enter the SNMP port number for your DMM appliance, use the port number 161.</p>

**Note**

You cannot edit the (default) community string of your DMM appliance.

Configuring Alert Reports and Notification Settings

Procedure

-
- Step 1** Click the **Alerts** tab.
- Step 2** (Optional) To define the parameters for an alert report:
- a. Click **Alert Reports**, then click the radio button to use either Live Event Mode or Snapshot Mode:
 - Live Event Mode—
 - Snapshot Mode—
 - b. Choose the range of dates,
 - c. Choose an event type from the Type list, and then click **Apply**.

Step 3 (Optional) To define the settings for notifications:

- a. For each event type, choose a notification method. The methods are:
 - **No Notification**—Disables notifications for all events of the corresponding type.
 - **Email**—Enables automatic delivery of email notification messages for all events of the corresponding type. Activates the Recipient field, so that its email address value is editable; enter the email address that should receive notification messages. You can enter a unique recipient address for each of the notification event types. Requires that you have enabled SMTP.
 - **SNMP**—Enables automatic delivery of notification messages to your NMS for all events of the corresponding type, using SNMPv2c. Requires that you have purchased, installed, and enabled the SNMP Notification Module.
 - **Both**—Enables automatic delivery of email notification messages and automatic delivery of notification messages to your NMS for all events of the corresponding type. Activates the Recipient field, so that its email address value is editable; enter the email address that should receive notification messages. You can enter a unique recipient address for each of the notification event types. Requires that you have enabled SMTP and that you have purchased, installed, and enabled SNMP.
- b. Do one of the following:
 - To save all settings that you have defined for notifications and put them into effect immediately, click **Save**.
 - To clear your selections, so that you can start over again, click **Reset**.

Understanding Event Types

Alarms and notifications use these event types:

Type	Description
All Notifiable Events	All of the following.
DMP Outages	Messages list all registered but inaccessible DMPs.
DMP Restarts	Messages list all registered DMPs that restarted recently.
DMP IP Conflicts	Messages list all registered DMPs with IP address conflicts. An address conflict occurs when a DHCP server assigns to one registered DMP the exact dynamic IP address that some other registered DMP used previously. If the DMP that previously used the address is no longer in active use, you should delete the record of it in DMM-DSM. If the DMP that previously used the address is one that should still be active, confirm that it is still running and still connected to the network, then restart it and confirm that its DHCP server does not assign IP addresses with expiration dates.
DMP IP Registrations	Messages list all newly registered DMPs.
Video Portal Outages	Messages list registered but inaccessible Video Portal appliances.
Video Portal Restarts	Messages list registered Video Portal appliances that restarted recently.

Type	Description
Deployment Failures	Messages list recently failed deployments of content for use on a Video Portal.
Deployment Successes	Messages list recently successful deployments of content for use on a Video Portal.
All Internal Events	Messages list all signals exchanged between and among the internal components of Cisco DMS. Most users attribute little or no significance to these events.

Related Topics

- [Managing and Grouping Your DMPs, page 3-12](#)

Viewing Appliance Processes and Restarting Appliances Remotely

Procedure

-
- Step 1** Click the **Services** tab.
- Step 2** To see which processes are running on a DMS appliance, do one of the following:
- For a DMM appliance, click **DMM Server**.
 - For a Video Portal appliance, click **VP Server**.
- Step 3** (Optional) To restart the appliance remotely, choose **Options > Restart Server**.
-