



CHAPTER 7

Managing Accounts

This chapter describes how to set and manage user roles and accounts. It includes these topics:

- [About User Account Management, page 7-1](#)
- [Managing User Accounts, page 7-7](#)
- [Setting Up Roles, page 7-12](#)
- [Configuring User Account Synchronization, page 7-18](#)

About User Account Management

VSOM supports the creation of user accounts for the administrators and operators who use the VSOM system. By creating user accounts, you can control who has access to the system and keep track of how the system is used and by whom.

User accounts include the following information:

- User information, including user name, password, and contact details.
- Predefined view that a user sees by default in the Operator page. See [“Managing Predefined Views” section on page 5-37](#) for more information.
- Schedules that optionally control when a user is able to access the system.
- Roles that determine which items a user can view and change within VSOM. Roles include settings, permissions, and rights, as described in the [“About Role Settings, Permissions, and Rights” section on page 7-2](#).
- Custom fields that you can use to store additional information about a user.

About Roles

Each user account comes with assignment of roles. Roles determine which items a user is permitted to view and change within VSOM. All users must be assigned at least one role and can be assigned up to 100 roles.

An administrator role can optionally include the Pseudo Root designation, which provides unrestricted access to the VSOM host. A user with a role that has Pseudo Root assigned can do everything that the root user can do with additional personalization of login information permitted. At least one administrator should be assigned a role with the Pseudo Root designation.

The following table describes the default roles. VSOM allows you to create additional roles, as described in the [“Setting Up Roles” section on page 7-12](#).

Table 7-1 **Default Roles**

Role	Description	Comment
Administrator	Provides authority to manage and display all VSOM resources. Can assign root-level access.	At least one administrator account is required to manage VSOM.
Operator	Provides limited authority, typically to display a portion of system resources, such as cameras and archives that a user is responsible for monitoring.	Create an operator account for each user.

About Role Settings, Permissions, and Rights

Each role includes specification of settings (or preferences), permissions, and rights. A role can be assigned to one or more users, and a single user can have one or more roles. If a user is assigned multiple roles, the role with the most generous permissions and rights takes precedence over the other roles.

Best Practices

- Use the default Administrator and Operator roles without modifying their settings (except to assign Pseudo Root to the Administrator role, if desired).
- If you want to assign additional permissions and rights to users, create new roles to do so.

The basic settings (*preferences*) for a role determine general privileges, which are sufficient for many installations. These settings include the following:

- Pseudo Root—This setting provides access to all resources. A user with a role that has Pseudo Root assigned can do everything the root user can do by using an individual user login rather than the general root user login. By using pseudo root, you can provide for better tracking of which user is logged in and using the system.
- Administrative Preferences—With this setting, a user can open the Administrator pages. The functions that the user can perform on the Administrator pages are determined by permissions and rights.



Note

The Pseudo Root preference does not automatically include access to the Administrative pages. You must specify Administrative Preferences to allow access to the Administration pages even if you also choose Pseudo Root.

- Operator Preferences—This setting determines the type of access and interaction that are permitted on the Operator page:
 - View Only—Provides access only to predefined views on the Operator page. This option restricts the privileges that are assigned to the default Operator role.
 - View Options—Restricts the ability to override the display options for a view.

Permissions and rights add finer-grained control of roles and are useful for large deployment in which users perform specialized functions.

- Permissions are action-based and determine the general ability of a user to perform operational functions, such as managing camera feeds, archiving local clips, and modifying schedules.

- Rights restrict privileges to specific device models, events, archives, schedules, servers, and views. For a user to have rights in any area, permission to that area must be granted.

For example, a user who is an installer may be assigned a “Pelco Installer” role, to manage Pelco cameras. The role must include *permissions* to manage cameras and feeds in general along with *rights* to manage Pelco cameras and feeds.

The following guidelines apply to roles:

- Each category for permissions and rights can be set to one of the following:
 - **None**—The category or item is not visible to the user
 - **View**—The user can see but not modify the category or item
 - **Manage**—The user can view, add, edit, and delete the category or item
- For roles with Administrator privileges, permissions are a prerequisite for rights. For example, an administrator must have permission to manage camera feeds to have the right to manage camera feeds for a specified type of camera.
- For roles with Operator but not Administrator privileges, only the rights for archives, camera feeds, monitors, and encoders apply. The camera feed rights determine which camera feeds are visible in the side menu of the Operator page.
- If a user is granted conflicting permissions and rights, then the most restrictive settings apply.

Table 7-2 shows examples of the relationship between permissions and rights.

Table 7-2 *Permission and Rights Examples*

Permissions	Rights	Description
None	None	The administrative icons for the resource are not displayed and individual items are not displayed in the side menu.

Table 7-2 *Permission and Rights Examples*

Permissions	Rights	Description
None	Manage	The administration icons for the resource are not displayed and the individual items with View rights are displayed in the side menu. (The use of Manage rights in this case adds no additional capabilities.)
Manage	View	The administration icon for the resource is not displayed and the individual items with View rights are listed inside the administration icon and in the side menu. This setting permits a role with Administrator privileges to display the settings for some resources.

About User Authentication

When a user tries to access VSOM, an authentication process takes place to determine whether access is allowed and, if allowed, to log the user in. The following options are supported for authenticating users who attempt to access VSOM:

- Local login/password—With this option, the VSOM server maintains user login information about locally on the VSOM server. Login information is entered in the User page, as described in the [“Adding a User” section on page 7-8](#).
- LDAP—With this option, an existing Lightweight Directory Access Protocol (LDAP) services is used to authenticate users. If you use this option, you cannot change the user password in the VSOM interface. For more information, see the LDAP configuration information in the [“Operations Manager Configuration Page” section on page 10-28](#).

Working with LDAP

LDAP is used to access directory servers. Directory servers access a database that holds information in a tree structure, similar to a hard disk directory structure. Administrators can navigate to the subdirectory by using path names similar to /usr/local/myapp/docs.

VSOM does not import groups or users from the LDAP server. You must create each LDAP user in VSOM and assign LDAP authentication (not local authentication) in the VSM Management Console (VSMC). The user name that is assigned for VSOM must be identical to the user name in the LDAP system. See [Chapter 10, “Using the VSM Management Console,”](#) for instructions on configuring LDAP authentication.

Use the Video Surveillance Management Console to configure VSOM to work with an LDAP server, as described in the [“Operations Manager Configuration Page”](#) section on page 10-28.

Table 7-3 lists the LDAP parameters. that are set in the Management Console.

Table 7-3 **LDAP Parameters**

Item	Description
LDAP_HOST_NAME	Enter the IP address or the host name of the LDAP server to be used to authenticate user log in credentials. For example, ds.cisco.com.
LDAP_HOST_PORT	Optional parameter. Port number of the LDAP server that is used to authenticate user log in credentials. If this field is blank, the value 389 is used.
LDAP_RDN_DN	LDAP RDN ¹ to be used for authentication. In the RDN, the token %username% is replaced dynamically with the user name when a user attempts to log in. For example: CN=%username%,OU=Employees,OU=cisco users.
LDAP_DCS	List of DCs ² in order of precedence and separated with semicolons (;). The system verifies the authentication bind against each DC in order until a successful bind is achieved or there are no more domain controllers. For example: DC=amer, DC=cisco,DC=com; DC=euro,DC=cisco,DC=com

1. RDN = Relative Distinguished Names.
2. DC = Domain Controller.

Managing User Accounts

Click **Users** on the side menu in the Administrator pages to open the Users page. [Table 7-4](#) [Table 7-4](#) lists the tasks that you can perform on this page.

Table 7-4 *Users Panel Tasks*

Task	Description	Reference
Add a user	Create a new user account	Adding a User, page 7-8
Edit or delete a user account	Make changes to an existing account or delete an account	Editing or Deleting a User, page 7-9
Edit user custom field labels	Create custom fields to store and display additional information	Creating Custom Field Labels for Users, page 7-10
Synchronize user accounts	Make user account information consistent across multiple VSOM servers	Configuring User Account Synchronization, page 7-18
Display current user account settings	Show the current configuration for a user account	Displaying User Information, page 7-10

Adding a User

Adding a new user involves specifying login and contact information and roles. You also can specify a default view and an access schedule.

Before You Begin

- Set up roles, as described in the [“Setting Up Roles” section on page 7-12](#).
- Decide whether to use local authentication or LDAP authentication, as described in the [“About User Authentication” section on page 7-5](#).
- Decide whether to set up parent/child relationships between servers, as described in the [“Managing Encoders” section on page 3-20](#).
- Define schedules, as described in the [“Managing Schedules” section on page 6-23](#).

To add a new user, follow these steps:

Procedure

- Step 1** In the Administrator pages, click **Users**.
- Step 2** Click **Add User**.
- Step 3** In the User Name field enter a unique user login name (up to 30 characters, including spaces). The name is not case-sensitive.
- Step 4** Choose the **Local Password** or the **LDAP** option to designate whether the user authentication is managed by the local VSOM server or by an LDAP server.
- If you choose **Local Password**, enter a password and then re-enter the password in the Confirm Password field. Passwords must contain 5-10 characters and are case-sensitive.
- If you are using LDAP, see the [“Working with LDAP” section on page 7-6](#).
- Step 5** Enter the user contact information in the First Name and Last Name (up to 64 characters each) and Email field (up to 255 characters).
- The e-mail address is used for notifications.
- Step 6** From the **Status** drop-down list, verify that the status is **Enabled**.
- A user must be enabled to be able to access VSOM.

Step 7 (Optional) Choose a view from the **Default View** drop-down list if you want the user to see a specified view when opening the Operator page.

See the “[Managing Predefined Views](#)” section on page 5-37 for information about configuring views. If you do not specify a view, the video pane in the Operator page presents a message indicating that a default view has not been configured and provides links to complete the setup or specify a view.

Step 8 (Optional) Click the **Schedule** tab to restrict user access according to a predefined schedules, as follows.

- **Default State**—Choose the user status (Enabled or Disabled) to apply when a schedule is not running. For example, if you want to allow the user to access VSOM only during specific times, choose **Disabled** as the default. Choose **Enabled** if you want to allow the user to access VSOM except as restricted by the schedule.
- **Simple Schedule**—Choose the schedule from the drop-down list. A simple schedule runs once from a specified start time to a specified end time.
- **Recurring Schedule**—Choose the schedule from the drop-down list. A recurring schedule runs multiple times according to specified rules.


See the “[Managing Schedules](#)” section on page 6-23 for information about defining schedules.

Step 9 Click the **Custom Fields** tab and enter values for any custom fields that have been defined (see the “[Creating Custom Field Labels for Users](#)” section on page 7-10).


Step 10 Click the **Roles** tab and check the check boxes for the roles that you want to assign to the user.

Step 11 Click **Submit**.

Editing or Deleting a User

To edit user settings, click the **Edit** icon  for the user in the Actions column on the Users panel and make changes on any of the tabs.

To change the user password, click the **Change Password** button on the Details tab. Enter the password, re-enter it to confirm, and then click **Submit**. Passwords must contain 5-10 characters and are case-sensitive.

To delete the user account from the VSOM database, click the **Delete** icon  and then click **Yes** to confirm. If a user account is deleted while a user is logged in, the user is allowed to complete the login session.

Creating Custom Field Labels for Users

Custom field labels allow you to specify custom fields to record additional information about a user. The custom fields are shown on the Custom Fields tab when you edit a user record.

To create custom fields labels, follow these steps:

Procedure

-
- | | |
|---------------|---|
| Step 1 | Click the Edit User Custom Field Labels link above the list of users to open the Custom Fields configuration page. |
| Step 2 | Enter up to 20 field labels in the order in which you want them to appear.
Labels that are left blank are ignored. |
| Step 3 | Click Submit . |
-

Displaying User Information

Click the underlined link for a user on the Users panel to display the current settings for the user, as described in [Table 7-5](#).

Table 7-5 **User Information**

Item	Description
Details Tab	
User Name	Name that the user uses to log in to VSOM.
Status	Indicates whether the user has system access (enabled) or is denied access to VSOM. Users are immediately logged out if their user status changes to disabled.
First Name	First name of the user.
Last Name	Last name of the user.
Description	Optional description.
Email	Optional e-mail address of the user.
Default View	Layout that the user sees by default when opening the Operator page.
Scheduling Tab	
Default State	State of the user account when there is no running schedule. Displayed only if a schedule is assigned to the user.
Simple Schedule	Information about the simple scheduled assigned to this user. Displayed only if a simple schedule is assigned to the user.
Recurring Schedule	Information about the recurring scheduled assigned to this user. Displayed only if a recurring schedule is assigned to the user.
Custom Fields Tab	
Custom Fields	Settings of any custom fields that have been defined.
Roles Tab	
Role Name	Roles assigned to the user.
Status	Indicates whether the role is active for or inactive for the user. If a role is active, then the user is subject to the permissions and rights assigned to that role. If multiple roles are assigned to the user, then the most restrictive role takes precedence.

Setting Up Roles

Roles determine which items a user is permitted to view and change within VSOM. All users must be assigned at least one role and can be assigned up to 100 roles.

Click **Roles** on the side menu in the Administrator pages to open the Roles page. This page contains links to manage roles. It also includes a table that lists information about roles and provides various links and buttons.

[Table 7-6](#) lists the tasks that you can perform on this panel. For more information about roles, see the [“About Roles” section on page 7-2](#).

Table 7-6 *Roles Panel Tasks*

Item	Description	Reference
Add a new role	Create a new role	Adding a Role, page 7-12
Modify, copy, or delete a role	Make changes to an existing role, create a new role with the same settings as a specified role, or delete a role	Editing, Copying or Deleting a Role, page 7-15
Assign users to roles	Understand the options for assigning users to role	Associating Users with Roles, page 7-15
Display current role settings	Show the current configuration for a role	Displaying Role Information, page 7-16

Adding a Role

When you add a new role, you specify the preferences, permissions, and rights for the role. See the [“About Role Settings, Permissions, and Rights” section on page 7-2](#) for information about these attributes.

Before You Begin

- Create a list of the roles that you need for your VSM installation. The list should include the permissions and rights for each role.

- Determine the desired administrative or operator settings for the role and whether any customer permissions or rights are required.
- Define any needed schedules, as described in the [“Managing Schedules” section on page 6-23](#). The schedule determines when the role is active.

To add a new role, follow these steps:

Procedure

- Step 1** In the Administrator pages, click **Roles**.
- Step 2** Click **Add New Role**.
- Step 3** In the Role Name field, enter a name to identify the role (up to 30 characters, including spaces).
- Step 4** (Optional) In the Description field, enter a description (up to 1024 characters, including spaces).
- Step 5** From the **Status** drop-down list, verify that the status is **Enabled**.
- Step 6** In the **PTZ Priority** field, determine the PTZ priority.
- The PTZ priority determines how a camera responds when it receives PTZ commands from two or more devices simultaneously. The command with the highest PTZ priority is applied to the camera and the lower priority commands are ignored.
- Step 7** In the Administrative Preferences area, choose **Pseudo Root** if you want the role to include access to all resources in the system, and choose **Administrative Preferences** if you want the role to allow access to the Administration pages.
- You must choose **Administrative Preferences** to allow access to the Administration pages even if you also choose **Pseudo Root**. For more information about preferences, see the [“About Role Settings, Permissions, and Rights” section on page 7-2](#).
- Step 8** In the Operator Preferences area, specify the following:
- Check the **View Only** check box if you want to allow a user to view video only with predefined views. A user who has a role with this setting sees an Operator page with the video player and a drop-down list of predefined views to select for display in the video player.

- Check the **View Option: Disabled** check box if you do not want users to have access to video play controls in the Operator page. If a user with this check box checked views the Operator page, video player control options such as title bars, video tools, and timestamps are disabled.

If you choose **View Only** you cannot also choose **View Options**. For more information about preferences, see the [“About Role Settings, Permissions, and Rights”](#) section on page 7-2.

Step 9 Click the **Schedule** tab and configure the following settings if you want to limit system access for users with this role to a specified schedule:

- **Default State**—Choose the user status (Enabled or Disabled) to apply when a schedule is not running. For example, if you want to allow the user to access VSOM only during specific times, choose **Disabled** as the default. Choose **Enabled** if you want to allow the user to access VSOM except as restricted by the schedule.
- **Simple Schedule**—Choose the schedule from the drop-down list. A simple schedule runs once from a specified start time to a specified end.
- **Recurring Schedule**—Choose the schedule from the drop-down list. A recurring schedule runs multiple times according to specified rules.

See the [“Managing Schedules”](#) section on page 6-23 for information about defining schedules.

Step 10 Click the **Permissions** tab and choose radio buttons to specify **None**, **View**, or **Manage** permissions for each permissions category:

- **None**—Users assigned to this role cannot view, add, modify, or delete items in this category.
- **View**—Users assigned to this role can view but not add, modify, or delete items in this category.
- **Manage**—Users assigned to this role can view, add, modify, and delete items in this category.

Click the **All** link at the top of the None, View, or Manage column to choose all of the permission categories in that column.

Step 11 Click the **Rights** tab, click the + symbol as needed to expand a functional area, and choose radio buttons to specify **None**, **View**, or **Manage** permissions for each area:

- **None**—Users assigned to this role do not have rights to view, add, modify, or delete items in this functional area.

- **View**—Users assigned to this role can view but not add, modify, or delete items in this functional area.
- **Manage**—Users assigned to this role can view, add, modify, and delete items in this functional area.

Click the **All** link at the top of the None, View, or Manage column for a general functional area to choose all of specific items in that functional area. For example, click **All** in the Manage column for cameras to specify management rights for all cameras in the VSOM database.

Step 12 Click **Submit**.



Associating Users with Roles


You can associate users with roles in either or both of the following ways:

- On the Roles Panel—Click the **Users** tab and check the check boxes for the users to which you want to assign the role.
- On the Users Panel—Click the **Roles** tab and check the check boxes for the roles that you want to assign to a user.

If you specify assignments by using one of these panels, your selections are shown when you open the other panel.

Editing, Copying or Deleting a Role

To edit role settings, click the **Edit** icon  for the role in the Actions column on the Roles page and make changes on any of the tabs, as described in the [“Adding a Role” section on page 7-12](#). To create a new role with the same settings as a specified role, click the **Copy** icon . Enter a new role name, change any other settings as desired.

To delete a role from the VSOM database, click the **Delete** icon  and then click **Yes** to confirm. When the role is deleted, it is removed from all the users who had that role assigned. If a role is deleted while a user with the role is logged in, the user is allowed to complete the login session, but permissions and rights for the deleted role are no longer available.

Displaying Role Information

To display settings for a role, click the underlined link for a role on the Roles panel. [Table 7-7](#) describes the role settings.

Table 7-7 **Role Settings**

Item	Description
Details Tab	
Role Name	Name that a user uses to log in to VSOM.
Description	Optional description.
Status	Indicates whether the role allows access to VSOM (enabled) or does not allow access.
PTZ Priority	Priority when a camera receives more than one PTZ command at the same time. The command with the highest PTZ priority is applied to the camera and the lower priority commands are ignored. PTZ priority applies to user actions and events.
Pseudo Root	Indicates that the role provides unrestricted access to the VSOM host. A user with a role that has Pseudo Root assigned can do everything that the root user can do with additional personalization of login information permitted.
Administrative Preferences	Indicates whether the role permits access to the Administrator pages. You must choose Administrative Preferences to allow access to the Administration pages even if you also choose Pseudo Root .
View Only	If checked, indicates that users with this role can view video only using predefined views. A user who has a role with this setting sees an Operator page with the video player and a drop-down list of predefined views to select for display in the video player.
View Options	If checked, users with this setting do not have access to video play controls in the Operator page. If a user with a role that has this setting logs in and views the Operator page, the video player control options such as title bars, video tools, and timestamps are disabled.

Table 7-7 Role Settings (continued)

Item	Description
Users Tab	
Role Users	List of the users who have this role assigned. Click the underlined user link to display details about the user.
Scheduling Tab	
Default State	State of the role when there is no running schedule. Displayed only if a schedule is assigned to the role.
Simple Schedule	Information about the simple scheduled assigned to this role. Displayed only if a simple schedule is assigned to the role.
Recurring Schedule	Information about the recurring scheduled assigned to this role. Displayed only if a recurring schedule is assigned to the role.
Permissions Tab	
Permission Type	<p>Level of permission assigned to each function in the list:</p> <ul style="list-style-type: none"> • None—No access to this function. Any associated GUI elements such as preferences, archive clips, and archive local clips are not displayed. • View—Read-only access to this function. Add, edit, and delete functions, icons, and links are not displayed. • Manage—Read/write access to this function.
Rights Tab	
Role Rights	<p>Rights assigned to the role for each function in the list (clicking the + symbol expands the list for a category and clicking the – symbol collapses the list for the category):</p> <ul style="list-style-type: none"> • None—No access to this function. Any associated GUI elements such as preferences, archive clips, and archive local clips are not displayed. • View—Read-only access to this function. Add, edit, and delete functions, icons, and links are not displayed. • Manage—Read/write access to this function.

Configuring User Account Synchronization

The user account synchronization feature allows you to automatically copy selected users and roles from one VSOM server to another VSOM server. For the purpose of user account synchronization, the server from which users and roles are copied is called the *parent* server and the server to which the users and roles are copied is called the *child* server. For example:

- If you are logged into Server A and define Server B as a parent server, Server A is the child server and user accounts are synchronized from Server B to Server A.
- If you are logged into Server A and define Server C as a child server, Server A is the parent server and user accounts are synchronized from Server A to Server C.

Before You Begin

- Determine the IP address or host name of each server that is to be a parent or child server.
- For each role and user that you want to include in synchronization, make sure that the user is chosen in the Users tab for the role (see the [“Setting Up Roles” section on page 7-12](#)).

To configure user account synchronization, follow these steps:

Procedure

-
- Step 1** In the Administrator pages, click **User Account Sync**.
- Step 2** Configure the following information for each VSOM server that you want to designate as the parent server:
- Check the **Authorize** check box.
 - In the Parent Server Name field, enter the name that is assigned to the server in VSOM.
 - In the Host IP/Name field, enter the host name or IP address of the server that you want to designate as a parent server.
 - In the Set Passphrase and Confirm Passphrase fields, enter and confirm a password that the child server uses to access the parent server.

- Step 3** To add an additional parent server, click **Authorize Another Parent Server** and enter information for that server.
- Step 4** Click the **Child Servers** tab.
- Step 5** Configure the following information for each VSOM server that you want to designate as the child server.:
- Check the **Add** check box.
 - In the Child Server Name field, enter the name that is assigned to the server in VSOM.
 - In the Host IP/Name field, enter the host name or IP address of the server that you want to designate as a child server.
 - In the Passphrase field, enter a passphrase for the child server to use to access the parent server.
 - In the Availability column, click **Check** to determine whether the child server is available for connection to the parent server. Availability is checked and the result appears in the Results column.
- Step 6** Click **Finished**.
- Step 7** For each role and user that you want to include in synchronization, make sure that the user is chosen in the Users tab for the role. See the [“Editing, Copying or Deleting a Role” section on page 7-15](#).
- User account synchronization is now configured, and user accounts and roles that are updated on the parent server are automatically updated on the child server.
-

The following information applies when managing parent/child relationships for user account synchronization (examples assume Server A is the child server and Server B is the parent server; however, note that multiple parent and child servers are supported):

- Synchronization affects only user accounts. It does not affect other configuration settings.
- To enable the two servers, A and B, to communicate with each other for user account synchronization, you must log in to Server A and set Server B as the parent, and also log in to Server B and set Server A as the child.
- The passphrases that you enter into Server A and Server B must be identical.

- You must check the **Authorize** check box on the Parent Servers tab of the User Account Synch panel for all of the parent servers that are involved in user account synchronization. To remove a parent server from the list of servers involved in synchronization, uncheck the **Authorize** check box. After you submit the change, the server is no longer available for synchronization.
- You must check the **Add** check box on the Child Servers tab of the User Account Synch panel for all of the child servers that are involved in user account synchronization. To remove a child server from the list of servers involved in synchronization, uncheck the **Add** check box. After you submit the change, the server is no longer available for synchronization.
- Role modifications on the parent server, including assignments of users to the role, are applied to the role on the child server when synchronization takes place.
- Roles that have a parent user assigned cannot be deleted.
- Users on the parent server cannot delete accounts on the child server or change the rights associated with roles on the child server.