CHAPTER 6

Configuring the System

This chapter provides information on configuring the system parameters of the Cisco Videoscape Distribution Suite, Internet Streamer (VDS-IS).

- Configuring AAA, page 6-1
- Changing a Password, page 6-7
- Configuring System Settings, page 6-8
- Viewing or Downloading XML Schema Files, page 6-24

For information on logs, see the "System Audit Logs" section on page 8-9. For information on upgrading the VDS-IS software, see the "Software Upgrade" section on page 9-1. For information on the ports used by the VDS-IS, see the "System Port Numbers" section on page 8-10.

Configuring AAA

Authentication determines who the user is and whether that user should be allowed access to the network or a particular device. It allows network administrators to bar intruders from their networks. It may use a simple database of users and passwords. It can also use one-time passwords.

Authorization determines what the user is allowed to do. It allows network managers to limit which network services are available to different users.

Accounting tracks what users did and when they did it. It can be used for an audit trail or for billing for connection time or resources used (bytes transferred).

Collectively, authentication, authorization, and accounting are sometimes referred to as AAA. Central management of AAA, that means the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices.

In the VDS-IS network, login authentication and authorization are used to control user access and configuration rights to the CDSM, SEs, and SRs. There are two levels of login authentication and authorization:

- Device
- CDSM

In a VDS-IS network, user accounts can be created for access to the CDSM, and independently, for access to the SEs and SRs that are registered to the CDSM.

This section describes login authentication and authorization for the CDSM. For information about device login authentication and authorization, see the "Login Access Control" section on page 4-53 and the "Authentication" section on page 4-60.

Login authentication is the process by which CDSM verifies whether the person who is attempting to log in has a valid username and password. The person logging in must have a user account registered with the device. User account information serves to authorize the user for login and configuration privileges. The user account information is stored in the AAA database. When the user attempts to log in, the CDSM compares the person's username, password, and privilege level to the user account information that is stored in the database.

Each user account can be assigned to a role and a domain. A *role* defines which CDSM configuration pages the user can access and which services the user has authority to configure or modify. A *domain* defines which entities in the network the user can access and configure or modify. You can assign a user account to zero or more roles, and to zero or more domains.

Creating, Editing, and Deleting Users

Note This section addresses users with administrator-level privileges (admin users) only.

Two default user accounts are preconfigured in the CDSM. The first account, called *admin*, is assigned the administrator role that allows access to all services and access to all entities in the system. This account cannot be deleted from the system, but it can be modified. Only the username and the role for this account are unchangeable. To change the password for this account, use the **username** *admin* **password** <*password*> command through the CLI.

The second preconfigured user account is called *default*. Any user account that is authenticated but has not been registered in the CDSM gets the access rights (role and domains) assigned to the default account. This account is configurable, but it cannot be deleted nor can its username be changed.

When you create a new user account in the CDSM, you have the option to create the user account in the CLI for the CDSM device at the same time. Using this option to create the new account in the CLI provides the following benefits:

- The user account is created in the primary and standby CDSM management databases and in the CDSM CLI from one central point.
- Users can change their passwords, and the password changes are propagated to a standby CDSM.

If you choose to create the user account from the CDSM *without* creating the user account in the CDSM CLI at the same time, the following results apply:

- The user account is created in the primary and standby CDSM management databases.
- No user account is created in the CDSM CLI, and the user *cannot* log in to the CDSM until an account is created from the CLI.
- Local users cannot change their passwords using the CDSM.
- Local users can change their passwords using the CLI; however, the password changes are not propagated from the CLI to the CDSM databases when the CLI user option is enabled in the CDSM.

  If a user account has been created from the CLI only, when you log in to the CDSM for the first time, the Centralized Management System (CMS) database automatically creates a user account (with the same username as configured in the CLI) with default authorization and access control. However, to change the password in this scenario, the user account must be explicitly configured from the CDSM with the CLI user option enabled.

To create or edit a user account, follow these steps:

Step 1 Choose **System > AAA > Users**. The User Table page is displayed.

Table 6-1 describes the icons for the User Table page.

Table 6-1 User Table Icons

Icon	Function
🗋	Creates a new entry.
📝	Edits an entry.
▤	Creates a filtered table. Filter the table based on the field values.
⊞	Views all table entries. Click this icon to view all entries after you have created a filtered table.
⟳	Refreshes the table.
🖶	Prints the current page.

Step 2 Click the **Create New** icon in the task bar. The User Account page is displayed.

To edit an account, click the **Edit** icon next to the username.

Note The User Account page can only be accessed by users with administrator-level privileges.

Step 3 In the **Username** field, enter the user account name. The username must be between 4 and 32 characters in length, and begin with a letter.

The following characters are not permitted in a username: ? . / ; [ ] { } " @ = |.

Step 4 If you want to create a local user account with a password and privilege level from the CDSM, check the **Create CLI User** check box. The user account is created automatically in the CLI. To prevent the creation of a CLI user account from the GUI, leave the check box unchecked.

Step 5 In the **Password** field, enter a password for the CLI user account, and re-enter the same password in the **Confirm Password** field.

The password strength must be a combination of alphabetic character, at least one number, at least one special character, and at least one uppercase character.

The following characters are not allowed: ?./;[]{}"@=|

Step 6 From the Privilege Level drop-down list, choose a privilege level for the CLI user account. The choices are 0 (zero) (normal user) or 15 (superuser). The default value is 0.

Note A superuser can use privileged-level EXEC commands, whereas a normal user can use only user-level EXEC commands.

Step 7 In the Username Information area, enter the following information about the user: First Name, Last Name, Phone Number, Email Address, Job Title, and Department.

Step 8 In the **Comments** field, enter any additional information about this account.

Step 9 Click **Submit** to save the settings.

Step 10 From the left-panel menu, choose **Role Management**. The Role Management Table page is displayed.

Table 6-1 describes the icons for the Role Management page.

Table 6-2 Role Management Icons

Icon	Function
🗋	Creates a new entry.
✎	Edits an entry.
▤	Creates a filtered table. Filter the table based on the field values.
🔍	Views all table entries. Click this icon to view all entries after you have created a filtered table.
⟳	Refreshes the table.
⇨	Assigns all roles.
⇦	Removes all roles.
👓	Views read-only items.
✓	Indicates that the current transaction was successfully completed.

To add roles, see the "Creating, Editing, and Deleting Roles" section on page 6-5.

To view the setting for the role, click the **View** (eyeglasses) icon next to the role.

Step 11 Click the **Assign** icon (blue cross mark) next to each role name that you want to assign to the user account. To remove the role from the user account, click the **Assign** icon again.

To assign all roles, click the **Assign all Roles** icon in the task bar. To unassign all roles, click the **Remove all Roles** icon in the task bar.

Step 12 Click **Submit** to save the settings.

A green arrow wrapped around the blue cross mark indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon.

Step 13 From the left-panel menu, choose **Domain Management**. The Domain Management Table page is displayed.

To add domains, see the "Creating, Editing, and Deleting Domains" section on page 6-6.

To view the setting for the domain, click the **View** (eyeglasses) icon next to the domain.

Step 14 Click the **Assign** icon next to each domain name that you want to assign to the user account.

To remove the domain from the user account, click the **Assign** icon again.

To assign all domains, click the **Assign All** icon in the task bar. To unassign all domains, click the **Remove All** icon in the task bar.

Step 15 Click **Submit** to save the settings.

To delete a user, in the User Table page, click the **Edit** icon next to the username, and from the User Account page, click the **Delete** icon in the task bar.

Note Deleting a user account from the CLI does *not* delete the corresponding account in the CDSM database. User accounts created in the CDSM should always be deleted from within the CDSM.

Creating, Editing, and Deleting Roles

Although the CDSM provides many types of services, not all users have access to all services. Users are assigned a role, which indicates the services to which they have access. A *role* is a set of enabled services.

Each user account can be assigned zero or more roles. Roles are not inherited or embedded. The CDSM provides one predefined role, known as the *admin role*. The admin role has access to all services and all VDS-IS network entities.

Note The admin user account, by default, is assigned to the role that allows access to all domains and all entities in the system. It is not possible to change the role for this user account.

To create or edit a role, follow these steps:

Step 1 Choose **System > AAA > Roles**. The Roles Table page is displayed.

Step 2 Click the **Create New** icon in the task bar. The Role page is displayed.

To edit a role, click the **Edit** icon next to the role name.

Step 3 In the **Name** field, enter the name of the role.

Step 4 To enable read-only access for this role, check the **Read-Only** check box. Users assigned to this role are only be able to view the CDSM pages. They are not able to make any changes.

Step 5 To expand a listing of services under a category, click the folder, and then check the check box next to the service or services that you want to enable for this role. To choose all of the services under one category simultaneously, check the check box for the top-level folder.

Step 6 In the **Comments** field, enter any comments about this role.

Step 7 Click **Submit** to save the settings.

To delete a role, in the Roles Table page, click the **Edit** icon next to the role name. Once the Role page is displayed, click the **Delete** icon in the task bar.

Creating, Editing, and Deleting Domains

A *domain* is a set of VDS-IS network entities or objects that make up the VDS-IS network. Whereas a role defines which services a user can perform in the VDS-IS network, a domain defines the entities to which the user has access. An *entity* can be a Service Engine, a device group, or a Delivery Service. These predefined entities are treated like services and can be enabled or disabled when you set up user roles.

When you configure a domain, you can choose to include Service Engines, device groups, or delivery services in the domain.

To create or edit a domain, follow these steps:

Step 1 Choose **System > AAA > Domains**. The Domains Table page is displayed.

Step 2 Click the **Create New** icon in the task bar. The Domain page is displayed.

To edit a domain, click the **Edit** icon next to the domain name.

Step 3 In the **Name** field, enter the name of the domain.

Step 4 From the **Entity Type** drop-down list, choose Service Engines, Device Groups, or Delivery Services.

Step 5 In the **Comments** field, enter any comments about this domain.

Step 6 Click **Submit** to save the settings. If the entity type you chose has not already been assigned to the domain, then a message is displayed indicating that the entity type has not been assigned.

Step 7 From the left-panel menu, choose **Entity Management**. The Entity Management page is displayed.

Step 8 Click the **Assign** icon (blue cross mark) next to each entity name that you want to include. A green arrow wrapped around the blue cross mark indicates an entity is assigned.

To assign all entities in the domain, click the **Assign All** icon in the task bar.

To remove an entity from the domain, click the **Assign** icon again.

To remove all entities from the domain, click the **Remove All** icon in the task bar.

Step 9 Click **Submit** to save the settings.

To delete a domain, in the Domain Table page click the **Edit** icon next to the domain name. Once the Domain page is displayed, click the **Delete** icon in the task bar.

Creating a Domain Example

The following is an example of the tasks used to create a domain for a non-administrator user to be able to see a playlist view and have rights access to the SE, Delivery Service, and device group assigned to the playlist:

1. Choose **System > AAA > Domains**, and create a domain for entity type Delivery Services. Make sure that the Delivery Service the playlist uses is assigned to this domain.
2. Choose **System > AAA > Domains**, and create a domain for entity type Service Engine. Make sure that the SE the playlist uses is assigned to this domain.
3. Choose **System > AAA > Domains**, and create a domain for entity type Device Group. Make sure that the Device Group the playlist uses is assigned to this domain.
4. Choose **System > Users**. Select a user and assign the domains only configured to this user.

The non-administrator user should be able to see the playlist.

Viewing Locked Users

If you log in as an administrator, you can see a list of locked users along with the type of user and the time. The administrator can also unlock a user account.

To view or unlock a user account, follow these steps:

Step 1 Choose **System > AAA > Locked users**. The Locked Users page is displayed.

Step 2 Click **Unlock** hyperlink, to unlock a user account.

Changing a Password

If you log in as a user, you can change your own CDSM and CLI user password if you meet the following requirements:

- Your CLI user account and password were created in the CDSM and not in the CLI.
- You are authorized to access the Password page.

Note If you log in to the CDSM with the built-in username(*admin*) and the initial password (*default*), you cannot change the password in the CDSM. However, you can change the password using the CLI. The password expiry enhancement is not available for users logged in through the built-in username and password.

Caution We do not recommend that you change the CLI user password from the CLI. Any changes to CLI user passwords from the CLI are *not* updated in the management database and are not propagated to the standby CDSM. Therefore, passwords in the management database do not match a new password configured in the CLI.
The advantage of initially setting passwords from the CDSM is that both the primary and the standby CDSMs are synchronized, and CDSM users do not have to access the CLI to change their passwords.

To change the CDSM and CLI user password for the user account that is currently logged in to the CDSM, follow these steps:

Step 1 Choose **System > Password**. The Password page is displayed.

Step 2 In the **New Password** field, enter the changed password.

The following characters are not allowed: ?./;[]{}"@=|

Step 3 In the **Confirm New Password** field, re-enter the password for confirmation.

Step 4 Click **Submit** to save the settings.

Starting with Release 4.0, the CDSM includes the following enhancements:

- If you log in as a user, the system home page will display the password expiration details.
- The CDSM prompts the user to change the password, if the password expires.

The following fields must be filled when the CDSM prompts you to change the password:

- Username—Name of the user.
- Password—User password.
- Confirm Password—Re-enter the user password.

Configuring System Settings

- System Properties, page 6-8
- Configuring Device Offline Detection, page 6-10
- Configuring Distribution QoS, page 6-11
- Configuring Service Routing, page 6-12
- Authorization File Registration, page 6-15
- NAS File Registration, page 6-16
- HTTPS Settings, page 6-17
- Configuring the CDSM to Communicate with an External System, page 6-23

System Properties

To modify the system properties, follow these steps:

Step 1 Choose **System > Configuration > System Properties**. The System Properties page is displayed.

Step 2 Click the **Edit** icon next to the system property that you want to change. The Modify Config Property page is displayed.

Step 3 For true or false values, choose a setting from the **Value** drop-down list. For other values, enter a new value. The range is displayed for each numeric value.

Table 6-3 describes the system properties.

Table 6-3 System Properties Fields

Field	Description
cdsm.gui.rowCount	Row count for all pages containing table. The default is 10.
cdsm.password.expiry.days	The number of days for password expiry. The default is 0. The range is from 0 to 365. **Note** The password will not expire if the value is set to 0.
cdsm.password.warning.days	The number of days for password expiry warning. The default is 30. The range is from 0 to 100. **Note** The password warning message is not displayed if the value is set to 0.
cdsm.login.attempts.limit	The number of failed login attempts allowed. The default is 0. The range is from 0 to 6. **Note** The login attempts will not be checked if the value is set to 0.

Table 6-3 System Properties Fields (continued)

Field	Description
cdsm.session.timeout	Length of a Content Distribution Manager session (in minutes). The default is 10. The range is from 5 to 120.
DeviceGroup.overlap	SE feature overlapping (enable or disable).
System.CmsUnsProgram Sync.Interval	Interval by which CMS synchronizes program import UNS objects (in minutes). The default is 1440 minutes. The range is from 1 to 43200.
System.datafeed.pollRate	Poll rate between the SE or the SR and the CDSM (in seconds). The default is 300. The range is from 30 to 1800.
System.device.recovery.key	Device identity recovery key. This property enables a device to be replaced by another node in the VDS network.
System.healthmonitor.collect Rate	Sets the collect and send rate in seconds for the CMS device health (or status) monitor. The default is 120. The range is from 5 to 3600.
System.Icm.enable	Local and CDSM feature (enable or disable). This property allows settings that are configured using the local device CLI or the CDSM to be stored as part of the VDS-IS network configuration data.
System.monitoring.collect Rate	Rate at which the SE collects and sends the monitoring report to the CDSM (in seconds). The default is 300 seconds. The range is from 30 to 1800.
System.monitoring.daily ConsolidationHour	Hour at which the CDSM consolidates hourly and daily monitoring records. The default is 1. The range is from 0 to 23.
System.monitoring.enable	SE statistics monitoring (enable or disable).
System.monitoring.monthly ConsolidationFrequency	Frequency (in days) with which the CDSM consolidates daily monitoring records into monthly records. The default is 14. The range is from 1 to 30.
System.monitoring.record LimitDays	Maximum number of days of monitoring data to maintain in the system. The default is 1825. The range is from 0 to 7300.
System.repstatus.update Enabled	Replication status periodic calculations on an SE (enable or disable).
System.repstatus.updateRate	Rate of replication status periodic updates calculated on an SE (in minutes). The default is 10. The range is from 5 to 1440.
System.repstatus.updateRate Sec	Rate of replication status periodic updates calculated on an SE (in seconds). The default is 600 seconds. Setting this rate overrides the update rate set in minutes. The ranges is from 30 to 86400. **Note** The rep_status_failed alarm gets triggered if the replication misses three times in a row. You can configure a lower value for the System.repstatus.updateRateSec to have the alarm trigger sooner.
System.repstatus.updateSync Enabled	Sending summary replication status with requested detailed status (enable or disable).
System.security.minPassword Length	Minimum number of characters required for a user password. The default is 6. The range is from 6 to 31.
System.security.minUser NameLength	Minimum number of characters required for a user name. The default is 4. The range is from 1 to 32.

Step 4 Click **Submit** to save the settings.

Configuring Device Offline Detection

Communication between all devices and the CDSM use User Datagram Protocol (UDP), which allows for fast detection of devices that have gone offline. UDP heartbeat packets are sent at a specified interval from each SE to the primary CDSM in a VDS-IS network. The primary CDSM tracks the last time it received a UDP heartbeat packet from each SE. If the CDSM has not received the specified number of UDP packets, it displays the status of the non-responsive SEs as offline.

Note In VDS-IS networks with heavy traffic, dropped UDP packets can cause the CDSM to incorrectly report the status of SEs as offline. To avoid this problem, configure a higher value for dropped UDP heartbeat packets.

To configure Device Offline Detection, follow these steps:

Step 1 Choose **System > Configuration > Device Offline Detection**. The Configure Device Offline Detection page is displayed.

Note The Device Offline Detection feature is in effect only when the CDSM receives the first UDP heartbeat packet from an SE. UDP port of the heartbeat on the CDSM must be reachable for all devices; otherwise, the device shows as offline.

Step 2 In the **Heartbeat Rate** field, specify how often, in seconds, the SEs should transmit a UDP heartbeat packet to the CDSM. The default is 10. The range is from 5 to 3600.

Step 3 In the **Heartbeat Fail Count** field, specify the number of UDP heartbeat packets that can be dropped during transmission from SEs to the CDSM before an SE is declared offline. The default is 3. The range is from 1 to 100.

Note Decreasing the heartbeat interval (Heartbeat Rate * Heartbeat Fail Count) may take twice the original configured time to take effect. During this time, the online device status is not changed to “Offline” or “Online [Waiting for data feed].”

Step 4 In the **Heartbeat UDP Port** field, specify the CDSM port number that the SEs use to send UDP heartbeat packets. The default is 2000. The range is from 1000 to 10000.

The **Maximum Offline Detection Time** field displays the product of the failed heartbeat count and heartbeat rate, where:

Maximum Offline Detection Time =Heartbeat Rate * Heartbeat Fail Count

Step 5 Click **Submit** to save the settings.

Configuring Distribution QoS

The Distribution QoS settings allow you to configure system-wide QoS priorities for Delivery Service distribution and metadata replication. The Delivery Service distribution priority (low, medium, or high) is set on the definition page for each Delivery Service.

Note When a single URL is associated with more than one Delivery Service, the content is distributed only one time to all of the Service Engines subscribed to each Delivery Service. When different QoS settings are configured for different delivery services that contain the same content, the Delivery Service priority setting determines which QoS settings are applied to the content distribution. The Delivery Service with the higher priority dictates which QoS settings are used.

To configure system-wide QoS settings, follow these steps:

Step 1 Choose **System > Configuration > Distribution QoS**. The Distribution QoS page is displayed.

Step 2 Check the **Set QoS for Unicast Data** check box to enable system-wide QoS settings for unicast data.

The unicast data refers to the ingest and distribution traffic among SEs.

Step 3 To set the QoS value for a Delivery Service with low priority, choose a Differentiated Service Code Point (SCDP) value from the **QoS value with low priority** drop-down list. Alternatively, enter a decimal value in the corresponding field.

Note See the "Setting DSCP Values for QoS Packets" section on page 6-11for more information. You can override the system-wide settings for unicast data by configuring QoS settings on a per-Delivery Service basis. See the "Creating Delivery Service" section on page 5-1 for more information.

Step 4 To set the QoS value for a Delivery Service with medium priority, choose a DSCP value from the **QoS value with medium priority** drop-down list. Alternatively, enter a decimal value in the corresponding field.

Step 5 To set the QoS value for a Delivery Service with high priority, choose a DSCP value from the **QoS value with high priority** drop-down list. Alternatively, enter a decimal value in the corresponding field.

Step 6 Set the QoS value for each priority (low, medium, and high) for a Delivery Service by choosing the Differentiated Service Code Point (DSCP) value from the QoS value drop-down list or by entering a decimal value in the corresponding field.

Step 7 Check the **Set QoS for metadata** check box to enable QoS settings for metadata replication.

Metadata is created based on the Manifest file and is part of the ingest and distribution traffic.

Step 8 Set the Qo**S value for metadata replication** by choosing the DSCP value from the QoS value drop-down list or by entering a decimal value in the corresponding field.

Step 9 Click **Submit** to save the settings.

Setting DSCP Values for QoS Packets

The VDS-IS allows you to set Differentiated Services Code Point (DSCP) values for Unicast QoS packets. DSCP values define relative priority levels for the packets. You can either choose a DSCP keyword from the drop-down list or enter a value in the corresponding field. (See Table 6-4.)

Note DSCP marking for Flash Media streaming is configured differently by Service Rule file.

Table 6-4 DSCP Values

Keyword	Description and Value
af11	Sets packets with AF11 DSCP (001010). **Note** The number in parentheses denotes the DSCP value for each per-hop behavior keyword.
af12	Sets packets with AF12 DSCP (001100).
af13	Sets packets with AF13 DSCP (001110).
af21	Sets packets with AF21 DSCP (010010).
af22	Sets packets with AF22 DSCP (010100).
af23	Sets packets with AF23 DSCP (010110).
af31	Sets packets with AF31 DSCP (011010).
af32	Sets packets with AF32 DSCP (011100).
af33	Sets packets with AF33 DSCP (011110).
af41	Sets packets with AF41 DSCP (100010).
af42	Sets packets with AF42 DSCP (100100).
af43	Sets packets with AF43 DSCP (100110).
cs1	Sets packets with CS1 (precedence 1) DSCP (001000).
cs2	Sets packets with CS2 (precedence 2) DSCP (010000).
cs3	Sets packets with CS3 (precedence 3) DSCP (011000).
cs4	Sets packets with CS4 (precedence 4) DSCP (100000).
cs5	Sets packets with CS5 (precedence 5) DSCP (101000).
cs6	Sets packets with CS6 (precedence 6) DSCP (110000).
cs7	Sets packets with CS7 (precedence 7) DSCP (111000).
default	Sets packets with the default DSCP (000000).
ef	Sets packets with EF DSCP (101110).

Configuring Service Routing

The Service Routing menu options consist of the following:

- Coverage Zone File Registration, page 6-12
- Configuring Global Routing, page 6-14

Coverage Zone File Registration

A coverage zone can be associated with one or more SEs: each SE can have its own unique coverage zone, or SEs can be associated with more than one coverage zone and have overlapping coverage zones. For more information about coverage zones, see the "Coverage Zone File" section on page 1-38.

See Appendix C, "Creating Coverage Zone Files," for information about creating a Coverage Zone file.

The system administrator places a Coverage Zone file where the CDSM or individual devices can access the URL. The administrator then registers the Coverage Zone file URL in the CDSM. Coverage Zone files can be applied globally to the entire VDS-IS network, or locally to a specific SR. If a Coverage Zone file is made global, then it is read and parsed by each SR that does not have a Coverage Zone file assigned. If the coverage zone is specified in an individual SR configuration, it is only applied to that particular SR.

You have the choice of using two types of coverage zones:

- Default coverage zones
- User-defined coverage zones

A default coverage zone consists of all of the SEs that reside in the same local network segment, or subnet. The CDSM provides a check box to specify whether the default coverage zone is to be used.

A user-defined coverage zone consists of all of the SEs that are specified in a Coverage Zone file. This file defines the network segments to be covered in the routing process. The Coverage Zone file is registered with the CDSM and then applied to an SR for routing definitions.

To apply a custom coverage zone to an SR, you first need to register a Coverage Zone file URL in the CDSM. After you have registered the Coverage Zone file URL with the CDSM, you can apply the Coverage Zone file in one of two ways:

- Globally—Deploy the Coverage Zone file across the entire VDS-IS network
- Locally—Deploy the Coverage Zone file on a specific SR

Note If you apply a Coverage Zone file locally for a device, this file overwrites the global Coverage Zone file for that device.

To register a Coverage Zone file, follow these steps:

Step 1 Choose **System > Configuration > Service Routing > Coverage Zone File Registration**. The Coverage Zone File Table page is displayed.

Step 2 Click the **Create New** icon in the task bar. The Registering Coverage Zone File page is displayed.

To edit a Coverage Zone file registration, click the **Edit** icon next to the registration that you want to edit.

Step 3 Choose a file import method from the **File Import Method** drop-down list:

- **Upload**—The upload method allows you to upload a Coverage Zone file from any location that is accessible from your PC by using the browse feature.
- **Import**—The import method allows you to import the Coverage Zone file from an external HTTP, HTTPS, or FTP server.

When you choose a method, the page refreshes and displays the configuration fields that are associated with the method that you chose.

Step 4 Enter the fields as appropriate. Table 6-5 describes the upload method fields. Table 6-6 describes the import method fields.

Table 6-5 Upload Method for Coverage Zone Files

Property	Description
Coverage Zone File Upload	Local directory path to the Coverage Zone file. To locate the file, click **Browse**. Click **Validate** to validate the Coverage Zone file.
Destination Filename	Name of the Coverage Zone file. This field is filled in automatically with the filename from the local directory path.

Table 6-6 Import Method for Coverage Zone Files

Property	Description
Coverage Zone File URL	The URL where the Coverage Zone file is located, including path and filename. Click **Validate** to validate the Coverage Zone file.
Destination File Name	Name of the Coverage Zone file.
Update Interval (minutes)	Frequency with which the CDSM looks for changes to the Coverage Zone file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the Coverage Zone file.
Password	User password for fetching the Coverage Zone file.

Step 5 To save the settings, click **Submit**.

Configuring Global Routing

After you have registered the Coverage Zone file, you can use this file as your global routing configuration.

To set a global Coverage Zone file, follow these steps:

Step 1 Choose **System > Configuration > Service Routing > Global Routing Config**. The Set Global Coverage Zone File page is displayed.

Step 2 From the **Coverage Zone File** drop-down list, choose a Coverage Zone file.

Step 3 In the **DNS TTL** field, configure the time period (in seconds) for caching DNS replies. Enter a number from 0 to 300. The default is 60 seconds.

Step 4 Click **Submit** to save settings.

To apply a Coverage Zone file to an individual SR for local coverage zone configuration, see the "Configuring the Service Router" section on page 4-103.

Authorization File Registration

The Authorization File Registration page is used to register a Service Rule file to the VDS-IS. A Service Rule file is associated with one or more delivery services. Each Delivery Service can have its own unique Service Rule file or multiple delivery services can have the same Service Rule file.

A Service Rule must be selected for a Delivery Service. For more information about Service Rule files, see Appendix E, "Creating Service Rule Files." To select a Service Rule file for a Delivery Service, you first need to register the Service Rule file in the CDSM.

To register a Service Rule file, follow these steps:

Step 1 Choose **System > Configuration > Authorization File Registration**. The Authorization Plugin Files Table page is displayed.

Step 2 Click the **Create New** icon in the task bar. The Registering Service Rule File page is displayed.

To edit a Service Rule file registration, click the **Edit** icon next to the registration that you want to edit.

Step 3 Choose a file import method from the **File Import Method** drop-down list:

- **Import**—The import method allows you to import an XML file from an external HTTP, HTTPS, or FTP server.
- **Upload**—The upload method allows you to upload an XML file from any location that is accessible from your PC by using the browse feature.

When you choose a method, the page refreshes and displays the configuration fields that are associated with the method that you chose.

Step 4 Enter the fields as appropriate. Table 6-5 describes the upload method fields. Table 6-6 describes the import method fields.

Table 6-7 Upload Method for XML Files

Property	Description
File Type	From the **File Type** drop-down list, choose **Rule File**.
Source File Upload	Local directory path to the file. To locate the file, click **Browse**. Click **Validate** to validate the XML file.
Destination Filename	Name of the file. This field is filled in automatically with the filename from the local directory path.

Table 6-8 Import Method for XML Files

Property	Description
File Type	From the **File Type** drop-down list, choose **Rule File**.
File URL	The URL where the file is located, including path and filename. Click **Validate** to validate the XML file.
Destination File Name	Name of the file.
Update Interval (minutes)	Frequency with which the CDSM looks for changes to the file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the file.
Password	User password for fetching the file.

Step 5 To save the settings, click **Submit**.

NAS File Registration

A NAS file is associated with the SEs in the root location of a Delivery Service. One SE in the root location of a Delivery Service acts as the Content Acquirer. The NAS file is associated with the Delivery Service by assigning the file to the content origin. Each content origin can have its own unique NAS file or multiple content origins can have the same NAS file.

Note NAS is only supported in lab integrations as proof of concept.

For information about assigning a NAS file to a content origin, see the "Content Origins" section on page 5-32. For information about creating a NAS file, see Appendix G, "Creating NAS Files." To assign a NAS file to a content origin, you first need to register the file in the CDSM.

To register a NAS file, follow these steps:

Step 1 Choose **System > Configuration > NAS File Registration**. The NAS File Table page is displayed.

Step 2 Click the **Create New** icon in the task bar. The File Registration page is displayed.

To edit a NAS file registration, click the **Edit** icon next to the registration that you want to edit.

Step 3 Choose a file import method from the **File Import Method** drop-down list:

- **Upload**—The upload method allows you to upload a NAS file from any location that is accessible from your PC by using the browse feature.
- **Import**—The import method allows you to import a NAS file from an external HTTP, HTTPS, or FTP server.

When you choose a method, the page refreshes and displays the configuration fields that are associated with the method that you chose.

Step 4 Enter the fields as appropriate. Table 6-5 describes the upload method fields. Table 6-6 describes the import method fields.

Table 6-9 Upload Method for XML Files

Property	Description
Source File Upload	Local directory path to the file. To locate the file, click **Browse**. Click **Validate** to validate the XML file.
Destination Filename	Name of the file. This field is filled in automatically with the filename from the local directory path.

Table 6-10 Import Method for XML Files

Property	Description
File URL	The URL where the file is located, including path and filename. Click **Validate** to validate the XML file.
Destination File Name	Name of the file.
Update Interval (minutes)	Frequency with which the CDSM looks for changes to the file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the file.
Password	User password for fetching the file.

Step 5 To save the settings, click **Submit**.

HTTPS Settings

Certificate Authority's (CA's) root certificates are expected to be available to all clients initiating HTTPS communication; most browsers are installed with well-known CA root certificates. Trusted CA certificates are expected to be provided for the purpose of Origin server and Client certification validation.

Note A single subject alternative name (SAN) certificate is installed for all delivery services in the VDS-IS.

For more information about HTTPS Settings and how to configure it, see the "HTTPS Settings" section on page 2-25.

Uploading certificate and key files consists of the following pages:

- **Root CA File Registration**—Upload or import the certificates for the Origin servers participating in HTTPS
- **CRL File Registration**—Upload the CRL certificates for the Service Engine participating in HTTPS
- **CRL File Scheduling**—Schedule CRL file notification to the Web Engine on each SE that is participating in an HTTPS Delivery Service
- **HTTPS Certification Files Registration**—Upload client certificate and key file for all SEs
- **HTTPS Certification File Scheduling**—Schedule client certificate and key file notification to the Web Engine on each SE that is participating in an HTTPS Delivery Service

The procedures involved in uploading certificate and key files consist of the following:

- Configuring HTTPS General Settings
- Uploading or Importing a Root CA FileUploading a CRL FileScheduling a CRL File
- Uploading Certificate and Key Files
- Scheduling Web Engine Notification of Certificate and Key Files

Configuring HTTPS General Settings

Starting with Release 3.3, The CDSM GUI offers the ability to enable HTTPS or HTTP for streaming to clients as well as ingesting from the Origin server for each Delivery Service.

To configure the HTTPS settings, follow these steps:

Step 1 Choose **System > Configuration > HTTPS Settings > General Settings**. The HTTPS General Settings is page displayed.

Step 2 Enter the settings as appropriate. See Table 6-11 for a description of the fields.

Table 6-11 General Setting Fields

Field	Description
Delivery Streaming Mutual Authentication	Check the **Delivery Streaming Mutual Authentication** check box to enable delivery streaming mutual authentication for the individual Delivery Service. The default is unchecked.
Delivery Streaming Supported Cipher List	Input the Cipher list. The default is empty. When the Web Engine is acting as an HTTPS server, the **Delivery Streaming Supported Cipher List** is used to negotiate and accept HTTPS connections from the client player. **Note** When it is empty, the backend will use the default string.

Step 3 Click **Validate**, to verify if the cipher list is valid.

Step 4 Click **Submit** to save the settings.

Uploading or Importing a Root CA File

The root certificates are used by SEs to validate the Origin server certificates, one or more root certificates can be uploaded to the CDSM.

After a new root certificate is uploaded to the CDSM, it is distributed to all SEs immediately. The SE does not notify the Web Engine of the existence or update of a root certificate file; instead, the Web Engine fetches them when necessary.

To upload or import a root CA file, follow these steps:

Step 1 Choose **System > Configuration > HTTPS Settings > Root CA File Registration**. The Root CA File Registration table is displayed.

Step 2 Click the **Create New** icon in the task bar. The File Registration page is displayed.

To edit a root CA file, click the **Edit** icon next to the file that you want to edit.

Step 3 Choose a file import method from the **File Import Method** drop-down list:

- **Upload**—Uploads a file from any location that is accessible from your PC using the browse feature.

- **Import**—Imports a file from an external HTTP, HTTPS, or FTP server.

When you choose a method, the page refreshes and displays the configuration fields that are associated with the method that you chose.

Step 4 Enter the fields as appropriate. Table 6-12 describes the upload method fields. Table 6-13 describes the import method fields.

Table 6-12 Upload Method for Root CA Files

Property	Description
Source File Upload	Local directory path to the file. To locate the file, click **Browse**.
Destination Filename	Name of the file. This field is filled in automatically with the filename from the local directory path.

Table 6-13 Import Method for Root CA Files

Property	Description
File URL	The URL where the file is located, including path and filename.
Destination File Name	Name of the file.
Update Interval (minutes)	Frequency with which the CDSM looks for changes to the file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the file.
Password	User password for fetching the file.

Step 5 To save the settings, click **Submit**.

Uploading a CRL File

A Certification Revocation List (CRL) is a list of certificates that is revoked before their scheduled expiration date. It is maintained by a CA, and it provides information about revoked certificates that were issued by that CA. After uploading the CRL file from the CA, it should be imported into the SE.

To upload and schedule the CRL files, follow these steps:

Step 1 Choose **System > Configuration > HTTPS Settings > CRL File Registration**. The CRL File Registration File page is displayed.

Step 2 Click the **Create New** icon in the task bar. The File Registration page is displayed.

To edit a root CRL file, click the **Edit** icon next to the file that you want to edit.

Step 3 Choose a file import method from the **File Import Method** drop-down list:

- **Upload**—Uploads a file from any location that is accessible from your PC using the browse feature.
- **Import**—Imports a file from an external HTTP, HTTPS, or FTP server.

When you choose a method, the page refreshes and displays the configuration fields that are associated with the method that you chose.

Step 4 Enter the fields as appropriate. Table 6-14 describes the upload method fields. Table 6-15 describes the import method fields.

Table 6-14 Upload Method for CRL Files

Property	Description
Source File Upload	Local directory path to the file. To locate the file, click **Choose File**.
Destination Filename	Name of the file. This field is filled in automatically with the filename from the local directory path.

Table 6-15 Import Method for CRL Files

Property	Description
File URL	The URL where the file is located, including path and filename.
Destination File Name	Name of the file.
Update Interval (minutes)	Frequency with which the CDSM looks for changes to the file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the file.
Password	User password for fetching the file.

Step 5 To save the settings, click **Submit**.

Scheduling a CRL File

After the CRL files have been uploaded to the CDSM and distributed to all of the SEs in the system, the Web Engine on each SE participating in an HTTPS Delivery Service needs to be notified of the newly uploaded CRL files.

To schedule Web Engine notification of certificate and key files, follow these steps:

Step 1 Choose **System > Configuration > HTTPS Settings > CRL File Schedule**. The Scheduling Tasks table is displayed.

Step 2 Click the **Create New** icon in the task bar. The Certificate Schedule Task page is displayed.

The table lists the scheduled tasks, the SEs assigned to that task, and the status of the task (expired or active).

To edit a schedule, click the **Edit** icon next to the schedule that you want to edit. Expired tasks cannot be edited.

Step 3 To schedule the task to run immediately, check the **Immediately Run** check box.

To schedule the task to run at a specific date and time, follow these steps:

a. Click the **Calendar** icon next to the **Schedule Date and Time** field to enter the date and time. The Calendar dialog box is displayed.

b. From the **Month** drop-down list, choose the month.

c. To change the year, use the right arrow and left arrow on either side of the current year.

d. To select the day of the month, click the day in the calendar displayed. The current date is highlighted in yellow.

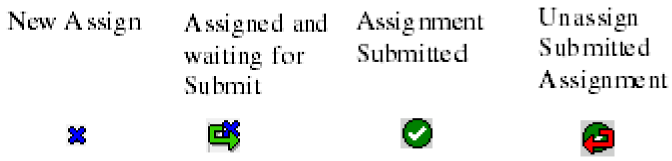
e. In the **Time** field, using the 24-hour clock, enter the time of day.

   To reset the date and time to today, click **Set Today**.

f. Click **Apply**. The date and time you selected is entered in the **Schedule Date and Time** field.

Step 4 Click the **Assign** icon (blue cross mark) next to the SE that you want to assign to this task. Alternatively, in the task bar, click **Assign All Service Engines**. The SE assignment states are described in Figure 6-2.

Figure 6-1 Content Origin Assignment State


New Assign
Assigned and waiting for Submit
Assignment Submitted
Unassign Submitted Assignment

A green arrow wrapped around the blue cross mark indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon.

Step 5 To schedule the task, click **Submit**. The task is displayed in the Scheduling Tasks table.

To delete all expired tasks from the Scheduling Tasks table, click the **Delete All** icon. To delete a specific task, click the **Edit** icon next to the task that you want to delete, and when the task is displayed, click the **Delete** icon.

Uploading Certificate and Key Files

The certificate and key files are uploaded to the CDSM, then the CDSM immediately distributes them to all of the SEs in the system. The certificate and key file distribution is independent of notifying the Web Engine of the newly uploaded certificate and key files, which occurs based on the defined schedule or immediately if the **Immediately Run** check box is checked.

One pair of certificate and key files are used by all SEs in the system to send to HTTPS clients for authentication. Uploading new certificate and key files overwrites the existing ones. The certificate and key files work as a pair, so updating one of them requires the other one be updated as well.

To upload the client certificate and key files, follow these steps:

Step 1 Choose **System > Configuration > HTTPS Settings > HTTPS Certification Files Registration**. The HTTPS Certification File page is displayed.

Step 2 To upload a certificate file, click the **Browse** button for the Certification File and navigate to the file.

Step 3 To upload a key file, click the **Browse** button for the Key File and navigate to the file.

Step 4 To save the settings, click **Submit**.

To delete a certificate or key file, click the **Delete** icon next to the file type. Deleting a certificate file or key file deletes the file from the CDSM and all SEs in the system, and impacts the HTTPS feature. The files should only be deleted if the HTTPS feature is no longer used. File deletion can only occur when there are no active HTTPS certificate file tasks scheduled.

Scheduling Web Engine Notification of Certificate and Key Files

After the certificate and key files have been uploaded to the CDSM and distributed to all of the SEs in the system, the Web Engine on each SE participating in an HTTPS Delivery Service needs to be notified of the newly uploaded certificate and key files.

To schedule Web Engine notification of certificate and key files, follow these steps:

Step 1 Choose **System > Configuration > HTTPS Settings > HTTPS Certification Files Schedule**. The Scheduling Tasks table is displayed.

Step 2 Click the **Create New** icon in the task bar. The Certificate Schedule Task page is displayed.

The table lists the scheduled tasks, the SEs assigned to that task, and the status of the task (expired or active).

To edit a schedule, click the **Edit** icon next to the schedule that you want to edit. Expired tasks cannot be edited.

Step 3 To schedule the task to run immediately, check the **Immediately Run** check box.

To schedule the task to run at a specific date and time, follow these steps:

a. Click the **Calendar** icon next to the **Schedule Date and Time** field to enter the date and time. The Calendar dialog box is displayed.

b. From the **Month** drop-down list, choose the month.

c. To change the year, use the right arrow and left arrow on either side of the current year.

d. To select the day of the month, click the day in the calendar displayed. The current date is highlighted in yellow.

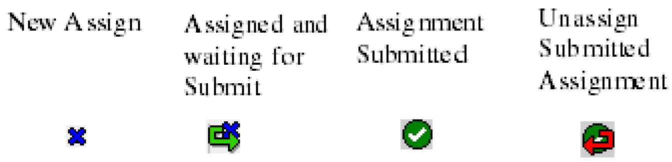
e. In the **Time** field, using the 24-hour clock, enter the time of day.

To reset the date and time to today, click **Set Today**.

f. Click **Apply**. The date and time you selected is entered in the **Schedule Date and Time** field.

Step 4 Click the **Assign** icon (blue cross mark) next to the SE that you want to assign to this task. Alternatively, in the task bar, click **Assign All Service Engines**. The SE assignment states are described in Figure 6-2.

Figure 6-2 Content Origin Assignment State


New Assign
Assigned and waiting for Submit
Assignment Submitted
Unassign Submitted Assignment

A green arrow wrapped around the blue cross mark indicates an SE assignment is ready to be submitted. To unassign an SE, click this icon.

Step 5 To schedule the task, click **Submit**. The task is displayed in the Scheduling Tasks table.

To delete all expired tasks from the Scheduling Tasks table, click the **Delete All** icon. To delete a specific task, click the **Edit** icon next to the task that you want to delete, and when the task is displayed, click the **Delete** icon.

Configuring the CDSM to Communicate with an External System

CDSM can be configured to communicate with external systems. Currently, Prime Central is supported as one type of external system.

Cisco PRIME for service providers is an experience delivery management architecture that enables the integrated design, fulfillment and assurance of customer experiences such as video, mobility, and managed cloud services delivered on converged IP networks.

As part of Cisco PRIME, the CDSM forwards alarms as SNMP traps to Prime Central. The CDSM supports the following functionality to provide communication to Prime Central:

- CDSM configuration settings to allow communication with Prime Central
- Registration of the CDSM on Prime Central
- Sending SNMP traps to Prime Central

Registering and De-Registering with Prime Central

The CDSM registers with Prime Central by checking **Register** check box in the External System page.

The registration process takes about 10 to 20 seconds. After registration is complete, the CDSM updates the status (Registered or Registration Failed) of Prime Central.

Note CDSM should be de-registered from the Prime Central before deleting the configuration settings of Prime Central. Excluding **Fault Manager Server IP** and **Fault Manager Server Port** fields, the configuration settings of the Prime Central listed in Table 6-16 cannot be modified when the status is Registered.

To configure the settings for an external system (Prime Central), follow these steps:

Step 1 From the CDSM GUI, choose **System > Configuration > External Systems**. The External Systems table is displayed.

Step 2 Click the **Create New** icon in the task bar. The External System page is displayed.

To edit an external system, click the **Edit** icon next to the external system name.

Step 3 Enter the settings as appropriate. See Table 6-16 for a description of the fields.

Table 6-16 External System Parameters

Field	Description
Name	Name of the External System
Type	Prime Central is the only option.

Table 6-16 External System Parameters (continued)

Field	Description
Status	Registration status, It can have the following values: Registered Unregistered Registering Registration Failed Deregistering
Register	Check the **Register** check box to register the CDSM with Prime Central.
IP address	IP address of the Prime Central.
Database SID	Database schema ID of the Prime Central.
Database Port	Database Port Number of the Prime Central.
Database User	Database User Name of the Prime Central.
Database Password	Database Password of the Prime Central.
Fault Manager Server IP	IP address of the Prime Central Fault Manager, used by CDSM to send SNMP traps to the Prime Central.
Fault Manager Server Port	Port number of the Prime Central Fault Manager, used by CDSM to send SNMP traps to the Prime Central.
Comments	Description of the External System.

Step 4 Click **Submit** to save the settings.

Viewing or Downloading XML Schema Files

The XML Schema Files page provides links to the XML schema files for viewing or downloading. All XML files can be validated through the CDSM by clicking **Validate** on the associated CDSM page. However, if you want to use an external XML validation program, you can save the XML schema file to use for that purpose. The following XML schema files are available:

- CDSAuthorization.xsd—Geo/IP file used to specify the geographic regions and IP networks that are allowed or denied access to a Delivery Service.
- CDSRules.xsd—Service Rule file used by a Delivery Service to specify the Service Rules for all SEs in a Delivery Service.
- CdsCoverageZone.xsd—Coverage Zone file is used to customize the networks and geographic regions each SE services.
- CdsOrigin.xsd—NAS file used for defining a NAS device.
- CdnManifest.xsd—Manifest file is used to specify the content to be prefetched and to control the delivery of the prefetched content for a Delivery Service.
- ContentDeletionTask.xsd—Content Deletion Task file is used to specify the content to be deleted for delivery services.

To open or save an XML schema file, follow these steps:

Step 1 Choose **System > CDS-IS Files > XML Schema Files**. The CDS-IS XML Schema page is displayed with a link to each XSD (schema) file.

Step 2 Click the link for the file. Depending on the browser program used, one of the following or something similar happens:

- The file is displayed in a new page and the File Download dialog box is also displayed.
- The opening dialog box is displayed.
- The file is displayed in a text editor program.