Configuring the System

This chapter provides information on configuring the system parameters of the VDS-OS. This chapter has the following major topics:

For information on logs, see the "System Audit Logs" section on page 1-6.

For information on upgrading the VDS-OS software, see the "Software Upgrade" section on page 1-1.

For information on the ports used by the VDS-OS, see the "System Port Numbers" section on page 1-7.

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

- Device
- VOSM

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

This section covers login authentication and authorization for the VOSM. For information about device login authentication and authorization, see the "Login Access Control" section on page 1-19 and the "Authentication" section on page 1-27.

Login authentication is the process by which VOSM 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 VOSM 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 VOSM 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 is addressed to users with administrator-level privileges (admin users) only.

Two default user accounts are preconfigured in the VOSM. 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 VOSM 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 VOSM, you have the option to create the user account in the CLI for the VOSM device at the same time. Using this option to create the new account in the CLI provides the following benefits:

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

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

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

  If a user account has been created from the CLI only, when you log in to the VOSM 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 VOSM with the CLI user option enabled.

To create or edit a user account, do the following:

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

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

Table 1-1 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 window.

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 VOSM, 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 **Branding String** field, enter a name or phrase that you want to appear in the CDSM banner, when this user logs in.

Step 9 In the **Comments** field, enter any additional information about this account.

Step 10 Click **Submit** to save the settings.

Step 11 From the left-panel menu, click **Role Management**. The Role Management Table page is displayed.

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

Table 1-2 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 1-5.

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

Step 12 Click the **Assign** icon (blue cross mark) next to each role name 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 13 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 14 From the left-panel menu, click **Domain Management**. The Domain Management Table page is displayed.

To add domains, see the "Creating, Editing, and Deleting Domains" section on page 1-6.

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

Step 15 Click the **Assign** icon next to each domain name 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 16 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 VOSM database. User accounts created in the VOSM should always be deleted from within the VOSM.

Creating, Editing, and Deleting Roles

Although the VOSM 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 VOSM provides one predefined role, known as the *admin role*. The admin role has access to all services and all VDS-OS 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, do the following:

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

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

Table 1-3 Role Management Icons

Icon	Function
	Creates a new entry.
	Edits an entry.
	Creates a filtered table. Filter the table based on the field values.

Table 1-3 Role Management Icons (continued)

Icon	Function
	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.

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 VOSM 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 you want to enable for this role. To choose all 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-OS network entities or objects that make up the VDS-OS network. Whereas a role defines which services a user can perform in the VDS-OS network, a domain defines the entities to which the user has access. An *entity* can be a Service Engine, a device group, or an origin 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 origin services in the domain.

To create or edit a domain, do the following:

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 Origin 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 displays indicating that the entity type has not been assigned.

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

Step 8 Click the **Assign** icon (blue cross mark) next to each entity name 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.

Changing a Password

If you are a user *without* admin privileges and you are logged in to the VOSM, you can change your own VOSM and CLI user password if you meet the following requirements:

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

Caution We do not recommend changing 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 VOSM. Therefore, passwords in the management database do not match a new password configured in the CLI.
The advantage of initially setting passwords from the VOSM is that both the primary and the standby VOSMs are synchronized, and VOSM users do not have to access the CLI to change their passwords.

To change the VOSM and CLI user password for the user account that is currently logged in to the VOSM, do the following:

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.

Configuring System Settings

This section covers the following topics:

System Properties

To modify the system properties, do the following:

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

Step 2 Click the **Edit** icon next to the system property 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 1-4 describes the system properties.

Table 1-4 System Properties Fields

Field	Description
VOSM.gui.rowCount	Default row count for all pages containing a table. The default setting is 10.
VOSM.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 VOSM (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-OS 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.

Table 1-4 System Properties Fields (continued)

Field	Description
System.Icm.enable	Local and VOSM feature (enable or disable). This property allows settings that are configured using the local device CLI or the VOSM to be stored as part of the VDS-OS network configuration data.
System.monitoring.collect Rate	Rate at which the SE collects and sends the monitoring report to the VOSM (in seconds). The default is 300 seconds. The range is from 30 to 1800.
System.monitoring.daily ConsolidationHour	Hour at which the VOSM 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 VOSM 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.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 VOSM 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 VOSM in a VDS-OS network. The primary VOSM tracks the last time it received a UDP heartbeat packet from each SE. If the VOSM has not received the specified number of UDP packets, it displays the status of the nonresponsive SEs as offline.

Note In VDS-OS networks with heavy traffic, dropped UDP packets can cause the VOSM 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, do the following:

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 VOSM receives the first UDP heartbeat packet from an SE. UDP port of the heartbeat on the VOSM 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 VOSM. 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 VOSM 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 datafeed]."

Step 4 In the **Heartbeat UDP Port** field, specify the VOSM 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 Service Routing

Coverage Zone File Registration

See Appendix 1, "Creating Coverage Zone Files," for information about creating a Coverage Zone file.

The system administrator places a Coverage Zone file where the VOSM or individual devices can access the URL. The administrator then registers the Coverage Zone file URL in the VOSM. Coverage Zone files can be applied globally to the entire VDS-OS 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 the SEs that reside in the same local network segment, or subnet. The VOSM provides a check box to specify whether the default coverage zone is to be used.

A user-defined coverage zone consists of all 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 VOSM 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 VOSM. After you have registered the Coverage Zone file URL with the VOSM, you can apply the Coverage Zone file in one of two ways:

- Globally—Deploy the Coverage Zone file across the entire VDS-OS 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, do the following:

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 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 1-5 describes the upload method fields. Table 1-6 describes the import method fields.

Table 1-5 Upload Method for Coverage Zone Files

Property	Description
Coverage Zone File Upload	Local directory path to the Coverage Zone file. To locate the file, use the **Browse** button. Click the **Validate** button 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 1-6 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 the **Validate** button to validate the Coverage Zone file.
Destination File Name	Name of the Coverage Zone file.
Update Interval (minutes)	Frequency with which the VOSM looks for changes to the Coverage Zone file. The default value is 10 minutes.

Table 1-6 Import Method for Coverage Zone Files

Property	Description
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

Step 1 **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 60. 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 1-66.

Asset Resolver File Registration

Step 1 Create the Asset Resolver file. Make sure it contains both the HDS or HLS rule and the DASH rule.

For sample Asset Resolver files, see the "Creating Asset Resolver Files" appendix.

Step 2 Choose **System > Configuration**. The Configuration Properties page is displayed.

Step 3 From the left-panel menu, click **Asset Resolver File Registration**. The Asset Resolver Files Registration page is displayed.

Step 4 Click the **Create New Asset Resolver File** icon.

a. Select **Upload** as the File Import Method and **Asset Resolver File** as the File Type.

b. Source File Upload is the Asset Resolver file that you are uploading.

c. Enter the Destination File Name, if different from the source file name.

d. Click **Validate**.

e. Verify that the **File Validation Result** shows no errors, then click **Submit**.

The Asset Resolver file is registered with VOSM.

For information about assigning the new Asset Resolver file to Service Engines assigned to origin services, see the "Asset Resolver Settings" section on page 1-6.

Defining Network Storage Shares

"Assign Network Storage Shares" section on page 6-5"Assign Network Storage Shares" section on page 1-5. For information about Network Storage Shares, see the "External Storage Devices—NAS" section on page 1-25.To assign a Network Storage Share to an origin service, you first need to define it.

Note Network traffic performance can be impacted by too small a value for the TCP parameter: net.inet.tcp.rexmit_slop. If it is determined that network throughput performance is impacted, the net.inet.tcp.rexmit_slop value on the NSS server should be reviewed.

To define a Network Storage Share, do the following:

Step 1 Choose **System > Configuration > Network Storage Shares**. The Network Storage Share Table page is displayed.

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

To edit a Network Storage Share, click the **Edit** icon next to the Network Storage Share you want to edit.

Step 3 Enter the settings as appropriate. See Table 1-7 for a description of the fields.

Table 1-7 Network Storage Shares Fields

Field	Description
Name	Unique name for the Network Storage Share. **Note** Spaces are not allowed in the Network Storage Share name. The Network Storage Share name can consist of alphanumeric characters and the underscore (_) and hyphen (-). The maximum length is 15 characters.
Storage Type	From the **Storage Type** drop-down list, select the storage type. **Note** Only NFS is supported.
Location	From the **Location** drop-down list, select a location. **Note** Only one location is supported.
Shared Directory	Shared directory on the Network Storage Share.
Mount Path	Local path on the Service Engine to mount the Network Storage Share.
Number of Mounts	Enter the number of servers that are to be mounted from the cluster pool.
IP Range <1–4)	IP address ranges that the Network Storage Share can be mounted on.Up to four IP address ranges can be specified.

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

To delete a Network Storage Share, first unassign it from the live channels and origin services, then from the Network Storage Share Table page, click the **Edit** icon next to the Network Storage Share you want to delete, and click the **Delete** icon in the task bar.

The following guidelines should be considered when defining NSSs:

- NSS should be network accessible

- Shared directory is the NFS exported file system that needs read (ro) access for VOD content and read write (rw) access for live and Live-to-VOD content
- File system exported should have sufficient file-mode access to read, or read and write
- For read/write access the mount option profile must be defined with Read-Write access

Creating Mount Option Profiles for Network Storage Shares

"Activating a Service Engine" section on page 5-9"Activating a Service Engine" section on page 1-9.

Note The mount option change takes effect on a SE reload, and only affects new mounts, not existing mounts.

To create a mount option profile, do the following:

Step 1 Choose **System > Configuration > Mount Option Profiles**. The Mount Option Profiles Table page is displayed.

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

To edit a Mount Option Profile, click the **Edit** icon next to the Mount Option Profile you want to edit.

Step 3 Enter the settings as appropriate. See Table 1-8 for a description of the fields.

Table 1-8 Mount Option Profiles Fields

Field	Description
Name	Unique name for the Mount Option Profile. **Note** Spaces are not allowed in the Mount Option Profile name. The Mount Option Profile name can consist of alphanumeric characters and the underscore (_) and hyphen (-). The maximum length is 256 characters.
NFS Access Mode	Select either **Read-Only** or **Read-Write**.
NFS Read Block Size	Read block size (in bytes) for NFS. The range is from 32768 to 524288.
NFS Write Block Size	Write block size (in bytes) for NFS.The range is from 32768 to 524288.
NFS Timeout	Time interval (in deciseconds) in which the SE has to respond to the Network Storage Share. After which the message is retransmitted. The range is from 1 to 6000. The default is 600.
NFS Retrans	Number of times to retransmit a message after a timeout has been reached. The range is from 1 to 60. The default is 3.
NFS Retry	Time (in minutes) to wait between retransmissions. The range is from 0 to 60. The default is 2.

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

To delete a Mount Option Profile, from the Mount Option Profile Table page, click the **Edit** icon next to the mount option profile you want to delete, and click the **Delete** icon in the task bar.

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 VOSM by clicking the **Validate** button on the associated VOSM 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:

- VOSCoverageZone.xsd—Coverage Zone file is used to customize the networks and geographic regions each SE services.

  VDS-OS uses the VOSCoverageZone.xsd XML schema file to customize the networks and geographic regions that are serviced by each SE.

- VOSCaptureSchedule.xsd—Capture Schedule file used to convert live content to VOD content (such as catch-up-to-live and start over)

To open or save an XML schema file, do the following:

Step 1 Choose **System > Files > XML Schema Files**. The VOS-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:

- File is displayed in a new window and the File Download dialog box is also displayed
- Opening dialog box is displayed
- File is displayed in a text editor program.