System Maintenance

This chapter explains how to perform common administrative tasks including, updating system software, restarting services, and shutting down the Vault and Streamer servers. This chapter covers the following topics:

Note If Virtual Video Infrastructure (VVI) with split-domain management is enabled, the CDSM pages associated with the Vaults and Caching Nodes display only on the VVI Manager (VVIM), and the CDSM pages associated with the Streamers display only on the Stream Manager. For more information, see Virtual Video Infrastructure, page F-8.

Note You must have read/write privileges to perform the functions described in this chapter.

Caution Many of the functions discussed in this chapter involve rebooting a VDS server. Rebooting a Vault server does not interrupt stream services, but causes current ingests to fail. If your VDS does not have stream failover, rebooting a Streamer without offloading it interrupts all stream services. If possible, you should perform functions that require a system restart during times when the least number of users are actively connected to your system.

User Access

Login authentication is used to control user access and configuration rights to the CDSM. Login authentication is the process by which the CDSM verifies whether the person who is attempting to log in to the CDSM has a valid username and password. If the local database is used, the person logging in must have a user account created on the CDSM. If an external server is used, the user account information is stored in an authentication database, and the CDSM must be configured to access the particular authentication server (or servers) where the database is kept.

Each user is assigned an access level. The VDS provides the following levels of user configuration rights:

- *Read only* access provides access to the monitoring capabilities, reports, and user manuals.
- *Read/write* access provides the ability to change the configuration settings and monitor all aspects of the system. In addition, a user with read/write access can perform software upgrades, restart servers, and restart services in a VDS.
- *Master* access has all the privileges of the read/write level and can add, delete, and change the level of access of the other users.
- *Engineering* access is primarily used for initializing the VDS at the time of installation and for VDS diagnostics. After your VDS has been configured, you should not require a user with engineering access level for day-to-day operations.

There is one built-in user, “admin,” that has master user capabilities. This is the only user that exists on a new system.

Caution If you are using RADIUS or TACACS+ for login authentication, make sure the configuration is correct and the server is operating correctly. If RADIUS or TACACS+ is not configured correctly, or if the RADIUS or TACACS+ server is not online, then the users may be unable to log in to the CDSM.

Local Database User Password Encryption

Passwords are not stored as clear text in the local database. They are stored using Secure Hash Algorithm (SHA), which includes a salt that is randomly generated for increased security. When a user logs in to the CDSM, SHA-1 is used to generate the hashed version of the user password, including the randomly generated salt, which is then sent for authentication. If the hashed version stored in the database matches what the user entered, the user is allowed access to CDSM; otherwise, access is denied.

CDSM User Login Checks

System checks are performed on the CDSM during the user login process and during access to the CDSM GUI. If any one of the checks does not pass, access to the CDSM is denied and an error message is displayed with information on which check failed.

Table 7-1 describes the system checks that are performed during the user login process and during user access to the CDSM.

Table 7-1 CDSM Checks for User Login

Check	Description	Additional Information	Error Message

Disk Space	Verify that all drives have not exceeded 95 percent storage capacity.	Disk space is checked every time an HTTP request is received by the CDSM. If any drive exceeds the threshold, the CDSM access is denied and the user is navigated to the login window where an error message is displayed.
		The drive names and threshold values can be configured in CDSM.ini file in the /arroyo/www/htdocs/CDSM/VDSTV/conf directory.
		`[disk-partition]`
		`drive.names = /arroyo,/arroyo/db`
		`drive.threshold = 95`
			CDSM is running out of disk space (/arroyo). Contact the System Administrator for further assistance.

User Account Locked	Verify that the user attempting to log in does not have this attribute enabled on the account.	The **User Account Locked** check box is checked on the Edit User page for the account. Only a user with Master-level access can check or uncheck the **User Account Locked** check box.	User account is locked. Contact the System Administrator for further assistance.
Concurrent User Sessions	Verify that the number of concurrent user sessions has not been exceeded.	The **Concurrent User Sessions** field is set on the Edit User page for the account. If the number of sessions the user is concurrently logged in to does not exceed the setting, access is allowed; otherwise, access is denied until the user logs out of one of the other sessions.	Maximum number of concurrent sessions reached. Try again later.
Password Expiration Interval	Verify that the password has not expired.	The **Password Expiration Interval** field is set on the System Authentication page. If this field is set, and the password has expired, the user is denied access to the CDSM.	Password has expired. Contact the System Administrator for further assistance.

If the checks described in Table 7-1 all pass, the user is authenticated and if authentication is successful, the following checks are performed:

1. If the **Force Password Change** check box is checked for the user account, then the user is navigated to the Edit User page and the user is forced to change the password.
2. If the **Password Expiration Reminder** interval has started, the user is navigated to the Edit User page and notified that the password is about to expire. The user can, however, ignore the reminder and continue without changing the password.

Adding Users

The VDS provides one built-in user, “admin,” that has master level access and cannot be deleted. The master user can add additional users with different levels of access.

To add a user, do the following:

Step 1 Choose **Maintain > Users > Add User**. The Add User page is displayed.

Step 2 Fill in the fields as described in Table 7-2.

Table 7-2 Add User Fields

Field	Description
New User	Login ID. A user name may have up to 25 characters. Any 7-bit characters from the American National Standards Institute (ANSI) character set are allowed.
Password	Password associated with the user login name. The password must be at least 5 characters. The maximum is 20.
Confirm Password	Confirm the password entered in the **Password** field.
Override Password Check	Passwords are validated for complexity; To override the password complexity validation, check the **Override Password Check** check box. The Override Password Check is not available when the user password is changed for the currently logged in user.
Access	Choose the appropriate access level from the drop-down list. See the beginning of User Access, page 7-2, for descriptions of the access levels.

Step 3 Click **Add User** to add this user.

To clear the fields and start over, click **Reset**.

Add User—Force Password Change

When a new user is added, the **Force Password Change** attribute for the user is checked. When the user logs in to the CDSM for the first time, the Edit User page is displayed and the user is forced to change the password.

Note When changing the password, browser-saved passwords may be requested to be changed.

During a password change, the new password is validated for complexity based on the Password Complexity Rules set on the System Authentication page. The password complexity check can be overridden if the change password is performed by a user with Master-level access and the **Override Password Check** check box is checked**.** The **Override Password Check** check box is available on the Add Users page and the Edit Users page if the user has Master-level access.

Editing User Settings

The Edit User page is used to update the user settings.

Note Only users with Master-level access can change the access level, delete a user, and configure the user-level account settings.

To edit the user settings, do the following:

Step 1 Choose **Maintain > Users > Edit User**. The Edit User page is displayed.

Step 2 From the **Action** drop-down list, choose one of the following:

- **Change Password**
- **Change Access**
- **Manage User Account**

Step 3 From the **User Name** drop-down list, choose a user name.

Step 4 The fields that are available are based on the Action selected. Table 7-3 describes the fields associated with each Action.

Table 7-3 Edit User Fields

Field	Description	Action
New Password	Password associated with the user login name. The range is 5 to 20 characters.	Change Password
Confirm Password	Confirm the password entered in the **Password** field.	Change Password
Override Password Check	Passwords are validated for complexity; To override the password complexity validation, check the **Override Password Check** check box. The Override Password Check is not available when the user password is changed for the currently logged in user.	Change Password
Access	Choose the appropriate access level from the drop-down list. See the beginning of User Access, page 7-2, for descriptions of the access levels.	Access
Lock Account on Failed Login	When the **Lock Account on Failed Login** check box is checked, the user is locked out of the CDSM GUI if the number of failed login attempts exceeds the allowed number of failed attempts configured in the System Authentication page. This setting overrides the Lock Account on Unsuccessful Login setting on the System Authentication page.	Manage User Account
User Account Locked	To lock a user out of the CDSM GUI, check the **User Account Locked** check box.	Manage User Account

Table 7-3 Edit User Fields (continued)

Field	Description	Action
Force Password Change	To force a password change for the user, at the next login, check the **Force Password Change** check box. If this check box is checked, the user is taken to the Edit User page at the next CDSM GUI login and must initiate a password change.	Manage User Account
Concurrent User Sessions	Maximum number of concurrent sessions allowed for this user.	Manage User Account

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

To clear the fields and start over, click **Reset**.

Deleting a User

To delete a user from the list of users, do the following:

Step 1 Choose **Maintain > Users > Edit User**. The Edit User page is displayed (Figure 7-1 on page 7-7).

Step 2 From the **Action** drop-down list, choose **Delete User**.

Step 3 From the **User Name** drop-down list, choose a user.

Step 4 Click **Submit** to delete the user.

To clear the fields and start over, click **Reset**.

Viewing User Settings

To view all user settings, you must log in with master access level. Choose **Maintain > Users > View Users**. The View Users page is displayed.

Changing User Default Settings

The User Default Settings page allows you to specify your settings for the Media Scheduler or Playout Scheduler pages so that each time you log in to the CDSM, your settings are recalled. If you have master level access, you can specify the settings for all users.

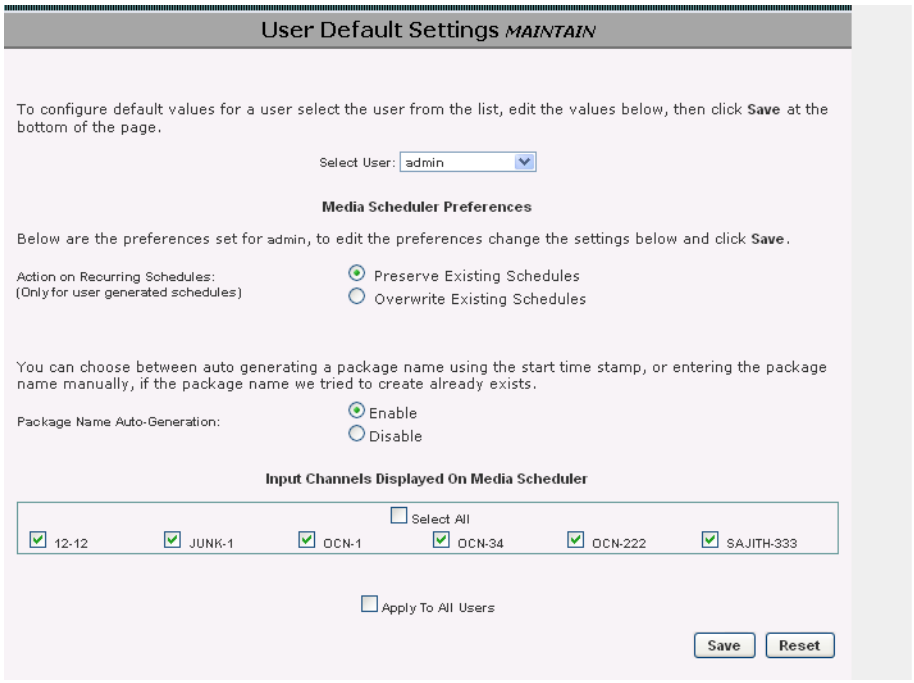
For more information about the Media Scheduler, see Configuring the Media Scheduler, page 4-56.

To change the default settings for a user, do the following:

Step 1 Choose **Maintain > Users > User Default Settings**. The User Default Settings page is displayed.

Step 2 From the **Select User** drop-down list, choose a user. The User Default Settings page refreshes and displays the user settings (Figure 7-1).

Figure 7-1 User Default Settings Page



Step 3 Enter the settings as appropriate. See Table 7-4 for descriptions of the fields.

Table 7-4 User Default Preferences

Field	Description
Media Scheduler	
Action on Recurring Schedules	Choose either **Preserve Existing Schedules** or **Overwrite Existing Schedules**. This option is only for user-generated schedules; this option is not for uploaded electronic program guide (EPG) data. **Preserving Existing Schedules** keeps any content that is currently scheduled for the day and channel you selected and only fills in the empty timeslots. **Overwrite Existing Schedules** overwrites any content that is currently scheduled for the day and channel you selected.
Package Name Auto-Generation	When you schedule an event that originated from an uploaded EPG file, the Media Scheduler creates a package name combining the channel name, title brief, and the word "package." If the package name already exists and you want a new package name auto-generated, choose **Enable** and the start time is added to the package name. If the package name already exists and you want to create the package name using the Metadata Editor, choose **Disable**.
Playout Scheduler	
Action on Recurring Schedules	Choose either **Preserve Exiting Schedules** or **Overwrite Existing Schedules**. This option is only for user-generated schedules; this option is not for imported playout schedules. **Preserving Existing Schedules** keeps any content that is currently scheduled for the day and channel you selected and only fills in the empty timeslots. **Overwrite Existing Schedules** overwrites any content that is currently scheduled for the day and channel you selected.

Table 7-4 User Default Preferences (continued)

Field	Description
Content Selection	Choose either the **Use Suggester** option or the **Use Select Box** option. **Use Suggester** displays a text box for selecting content, and **Use Select Box** displays a drop-down list. If there are a large number of content objects, the **Use Suggester** is the preferred choice. • If **Use Suggester** is selected, as you type in the text box, content matching the text is displayed in a list. If you click **Search**, The Content List window is displayed with the following options: – Quick Lists—Click **Most Recent Ingests**, and the 25 most recently ingested content objects are listed. – Browse Content—Click a character in the Browse Content section, and all content objects beginning with that letter are listed. – Content List—Displays the results of the Search, the Quick List, or the Browse Content selection. The content name and ingest time are listed. You can select a content object from the Content List, or select Close in the upper-right corner of the window and start your search again. • If **Use Select Box** is selected, use the down arrow of the drop-down list to display the list and select the content object.
Output Channels Displayed	Check the check boxes for the channels you want displayed, or check the **Select All** check box to chose all channels.
Manual Ingest FTP Preferences	
FTP username	The username to log into the FTP server.
FTP password	The password to log into the FTP server.
FTP host	The IP address or Fully Qualified Domain Name (FQDN) of the FTP server.
FTP Directory	The directory path where the content files are located. This can be an absolute or virtual path, depending on how the FTP server is configured. Make sure you begin the FTP path with a forward slash (/). The search includes all subdirectories.
File Extensions	The extensions of the types of content file you want retrieve. Separate multiple file extensions with a semicolon (;), and begin each file extension with a period (.). For example, to retrieve all MPEGs with a .mpg extension and transport streams with a .ts extension, you would enter the following: .mpg;.ts.

Step 4 In the Input Channels Displayed on the Media Scheduler section of the page, check the check boxes for the channels you want to schedule, or check the **Select All** check box to choose all channels.

Step 5 If you have master level access and you want to apply the user default settings of this page to all users, check the **Apply To All Users** check box.

Step 6 Click **Save** to save the changes.

To clear the fields and start over, click **Reset**.

Configuring System Authentication Settings

The System Authentication page is only visible to users with Master-level access. The System Authentication fields apply system wide to all users of the CDSM GUI. Table 7-5 describes the System Authentication fields.

Table 7-5 System Authentication Fields

Field	Description
Lock Account on Unsuccessful Login	If the **Lock Account on Unsuccessful Login** check box is checked, a user account is locked after the number of **Unsuccessful Login Attempt Count** has been reached within the **Unsuccessful Login Attempt Period**. For example, if the **Unsuccessful Login Attempt Count** is set to 3, the **Unsuccessful Login Attempt Period** is set to 1 day, and **Lock Account on Unsuccessful Login** is checked; then after 3 unsuccessful attempts within 1 day, the user account is locked.
Unsuccessful Login Attempt Count	Number of login attempts to allow the user before the account is locked. If the account is locked, the master-level user can unlock the account by unchecking the **User Account Locked** check box on the Edit Users page.
Unsuccessful Login Attempt Period	Time interval for which the number of unsuccessful login attempt count is persisted. When the time interval lapses, and if the account is not locked, the **Unsuccessful Login Attempt Count** is reset to 0.
Enable Password History	The history of user passwords is stored in the database if the **Enable Password History** check box is checked. During a password change, if the **Enable Password History** check box is checked, the new password is compared with the history of the user's passwords, and the password change is only successful if the new password is different than the passwords that were previously used.
Password History Size	Specify the number of old passwords to store for each user in the database. The default is 2.
Password Change Interval	Minimum interval between non-administrative password changes for a given user. The default is 24 hours.
Password Expiration Interval	Maximum lifetime of the password. If the password has not been changed within the **Password Expiration Interval**, then the user account is automatically disabled.
Password Expiration Reminder	Interval prior to the password expiration that the user is notified about the password expiration.
Idle Session Timeout Interval	Maximum time a session can be idle. If the time lapse between user requests exceeds the Idle Session Timeout Interval setting, the user is redirected to the Login page.

As an example, if the **Password Expiration Interval** is set to 6 months (180 days) and the **Password Expiration Reminder** is set to 15 days; then 15 days before the password expires, the user is taken to the Edit Users page where a message is displayed stating the password is soon to expire. The message also includes the number of days the current password is active before it expires. The user has the option to change the password or continue without changing the password.

If the password expires, the user cannot log in to the CDSM. A Master-level user can change the user password and unlock the user account. Anytime the user password is changed by the Master-level user, the **Force Password Change** check box is checked and the next time the user logs in to the CDSM, the user is taken to the Edit Users page and is forced to change the password. The user is not able to access any of the other CDSM GUI pages until a password change has occurred.

Password Complexity Rules

Password Complexity Rules apply to any password change performed by the user. These rules can be overridden by Master-level users when the **Override Password Check** check box is checked on the Add Users page or the Edit Users page.

Configuring User Authentication

The VDS software offers the following database options for maintaining user authentication data:

- Local database (located on the CDSM)
- RADIUS server (external database)
- TACACS+ server (external database)

The User Authentication page displays the configuration settings of the Authentication Protocol, which is configured through the **cdsconfig** script. The user authentication settings consist of choosing an external access server (TACACS+ or RADIUS) or the internal (local) CDSM authentication database for user access management, and setting the challenge key and timeout. The default is to use the local database for authentication. The **cdsconfig** script prompts you for the primary and backup external access server configuration. If the CDSM does not get a response from the primary server within the timeout period, the backup server is contacted.

Note The CDSM does not cache user authentication information. Therefore, if an external server is used, the user is reauthenticated against the Remote Authentication Dial In User Service (RADIUS) server or the Terminal Access Controller Access Control System Plus (TACACS+) server each time a user logs in to the CDSM. If the authentication is successful, a user session is created and is used to grant access to the different pages of the CDSM GUI. The session is destroyed when the user logs out of the CDSM. To prevent performance degradation caused by many authentication requests, install the CDSM in the same location as the RADIUS or TACACS+ server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

Server Maintenance

The Server Maintenance pages provides the ability to offload and shutdown a server for maintenance, and to restart a server without shutting it down. The Server Maintenance pages include the following:

- Restarting a Server
- Shutting Down a Server
- Offloading a Server
- Upgrading the VDS Software
- Setting System Thresholds

Restarting a Server

Caution Restarting a Vault or Streamer server while there are still active ingests and streams causes the current ingests and streams to fail.

Restarting a server briefly shuts down the unit, then restarts it using the installed version software image. This action does not power off the unit.

To restart a server, do the following:

Step 1 Choose **Maintain > Servers > Server Restart**. The Server Restart page is displayed.

Step 2 From the **Server IP/Name** drop-down list, choose the IP address or nickname of the server and click **Display**. The server type and ID, as well as the array ID, are displayed.

Step 3 From the **Restart** drop-down list, choose **Yes** and click **Submit**.

Shutting Down a Server

Caution Shutting down a Vault or Streamer server while there are still active ingests and streams causes the current ingests and streams to fail.

Shutting down by simply powering off the unit using the chassis power button is not recommended, as this may result in corruption of the configuration information, including system status when the shutdown occurred.

Shutting down and restarting using the CDSM is the recommended procedure. The Server Shutdown shuts down and powers off the selected unit.

To shut down and power off a server, do the following:

Step 1 Choose **Maintain > Servers > Server Shutdown**. The Server Shutdown page is displayed.

Step 2 From the **Server IP/Name** drop-down list, choose the IP address or nickname of the server and click **Display**. The server type and ID, as well as the array ID, are displayed.

Step 3 From the **Shutdown** drop-down list, choose **Yes** and click **Submit**.

Offloading a Server

The Server Offload page lets you set a server to **Online** or **Offline**. When a server is offline, the server is configured to reject new provisioning; that is, new ingests are not allowed on a Vault and new streams are not allowed on a Streamer and existing streams are moved to another Streamer gracefully.

Caching Nodes and Streamers

If HTTP is used as the cache-fill protocol between Caching Nodes and Streamers and the Caching Node hosting the locate port is set to Offline, then a backup or available Caching Node in the same Cache Group becomes the primary host of the locate port. If a backup or available Caching Node is set to Offline, the state is changed from backup or available to not usable. This failover scenario is similar to the Setup and Control server failover scenario for Streamers, in that all servers in the same group advertise their availability to act as the primary with a backup taking over as primary if the primary becomes unavailable because of offline status, losing connectivity, or failure.

Vaults

The Vault or ISV has two options for setting a server to offline:

- **Offline (No Ingest)**
- **Offline (No Ingest & Fill)**

The **Offline (No Ingest)** option enables the Vault or ISV to continue handling cache-fill requests and mirroring activities, but the server does not participate in any new content ingests. The **Offline (No Ingest & Fill)** option stops all cache-fill requests and any new content ingests, but the server still participates in mirroring activities.

Note The protocoltiming log file only displays the "WARNING: Server is going OFFLINE" message when the **Offline (No Ingest & Fill)** option is selected for Vaults.

The **Offline (No Ingest)** option for Vaults does not take the Vault completely offline, the Vault still participates in mirroring and cache-fill traffic; therefore, the server going offline message is not displayed in the protocoltiming log. The TRICKLE_DOWN file is used to determine the state of the Vault for the **Offline (No Ingest)** option.

To set a server to offline, do the following:

Step 1 Choose **Maintain > Servers > Server Offload**. The Server Offload page is displayed.

Step 2 From the **Server IP/Name** drop-down list, choose the IP address or nickname of the server and click **Display**. The server type, server ID, array ID, and current status of the server are displayed.

Step 3 In the New Server Status drop-down list, select the appropriate setting and click **Submit**.

After setting a server to offline, current traffic activity can be monitored, and when the server offline is complete, the software can be updated. To view activity on a Vault server, see Monitoring Content Objects, page 5-18. To view activity on a Streamer, see Monitoring Stream Objects, page 5-28. If the server is an ISV, verify that activity is completed for both content objects and stream objects before updating the software.

Note The Server Status setting is persistent through a system reboot.

Server Offload—Online

After the software upgrade or maintenance is complete, you need to set the server to online so that the server can again participate in the system.

To set a server to online, do the following:

Step 1 Choose **Maintain > Servers > Server Offload**. The Server Offload page is displayed.

Step 2 From the **Server IP/Name** drop-down list, choose the IP address or nickname of the server and click **Display**. The server type and ID, as well as the array ID, are displayed.

Step 3 In the New Server Status drop-down list, select **Online** and click **Submit**.

Vault Decommissioning

The Server Offload page offers the ability to gracefully decommission a Vault from the system. Content on the Vault is moved to other Vaults during the decommission process so that no content is lost.

The process of decommissioning a Vault requires that the Vault first be put into Offline (No Ingest & Fill) mode. After the Vault is offline the option to decommission is listed in the Server Offload page.

To decommission a Vault, do the following:

Step 1 Choose **Maintain > Servers > Server Offload**. The Server Offload page is displayed.

Step 2 From the **Server IP** drop-down list, select the IP address or nickname of the Vault and click **Display**.

Step 3 From the **New Server Status** drop-down list, select **Offline (No Ingest & Fill)**.

Step 4 Click **Submit**. The Current Server Status displays “Offline For Ingest & Fill.”

Note Before continuing, make sure the Vault has been offloaded by checking the protocol timing log.

Step 5 From the **New Server Status** drop-down list, select **Decommission**. The Decommission option is only displayed when the Vault is in the “Offline For Ingest & Fill” state.

Step 6 Click **Submit**. The Current Server Status displays “Decommission (Inactive).”

After the decommissioning starts the Current Server Status displays “Decommission (Active).”

When the decommissioning is complete the Current Server Status displays “Decommission (Completed)” and the **Shutdown** button is displayed.

Step 7 Click **Shutdown** to shut down the services running within CServer and completely isolate the Vault from the VDS.

After the decommission is complete, the Vault is isolated from the VDS. If the Vault is rebooted, it has the state of “Offline (No Ingest & Fill). The Vault entries in the database and .arroyorc remain intact. To remove the Vault entries from the database and .arroyorc file, the avsdb and statsd processes must be restarted, which impacts the serviceability of the system. Removal of a Vault from the database and .arroyorc file should be performed during a maintenance window.

Upgrading the VDS Software

The Software Upgrade page offers the ability to upgrade the VDS servers (Vault, Caching Node, and Streamer) remotely through the CDSM GUI. Before upgrading any of the VDS servers, first upgrade the CDSM/VVIM. If your system has redundant CDSMs/VVIMs, upgrade the secondary CDSM/VVIM followed by the primary CDSM/VVIM.

Manually upgrading each VDS server is still supported.

The Software Upgrade page offers the option to upgrade all VDS servers in the system, VDS servers in a specific group (Stream Group, Vault Group, Cache Group, or SSV Group), or a specific VDS server in a specific group.

Remote Software Upgrade Workflow

The Remote Software Upgrade feature performs the following tasks:

1. Sends parameters set in the CDSM GUI or through the Web Services API to the VDS server.
2. Logs in to the VDS server using the credentials specified in the parameter settings and copies the new **cdsinstall** script, the .bin image file, and the required libraries.
3. Runs the new **cdsinstall** script on the VDS server, which performs the following tasks:
   a. Copies ISO image file from specified location. If the file is already present, this step is skipped.
   b. Backs up the essential configuration files

      /etc/hosts

      /etc/rc.local

      /etc/sysconfig/network

      /etc/sysconfig/network-scripts/ifcfg-eth()

      /home/isa/.arroyorc

      Output of the **ifconfig -a** command to a new file (/root/ifconfig_<*system_date*>

      Note A backup of the /arroyo/db/DATADIR and /arroyo/test is not performed.

   c. Performs the pre-upgrade checks.
   d. Backs up existing software image.
   e. Performs the upgrade process.
4. Sends the upgrade status to statsd by writing into the /tmp/.upgrade_status file.

After upgrading the software on the VDS server, restart the server by logging in to the Linux operating system on the server as user *root* and enter the **reboot** command. After the VDS server has rebooted, set the server to online (**Maintain > Servers > Server Offload**).

Configuring the Software Upgrade Settings

Before upgrading the software, perform the following tasks:

1. Download the Cisco VDS software file and copy it to the server that will be accessed during the upgrade (this could be “Local Image,” which is the VDS server that is being upgraded).

   For information on getting the Cisco VDS-VR (formerly TV VDS) software file, see the *Cisco TV VDS 3.5 Installation, Upgrade, and Maintenance Guide*.

2. Offload each VDS server you want to upgrade (**Maintain > Servers > Server Offload**).

To configure the software upgrade settings, do the following:

Step 1 Choose **Maintain > Servers > Software Upgrade**. The Software Upgrade page is displayed.

Step 2 From the **Transfer Mode** drop-down list, select one of the following options:

- **FTP**
- **SCP**
- **HTTP**
- **Local Image**

FTP, SCP, and **HTTP** are the possible protocols used to get the software file from the server used to store it. **Local Image** is selected when the software image file was downloaded to the VDS servers that are being upgraded.

Step 3 In the **Image Location** field, enter the location of the software file. For FTP, SCP, and HTTP, the format is I*P_address*::*/absolute_path/*::*filename*. For Local Image, the format is */absolute_path/*::*filename.*

The Deployment Type field is informational only and displays the environment (ISA or RTSP) of the VDS.

Step 4 From the **Select Servers to Upgrade** drop-down list, select **All** or the server group of the VDS servers you want to upgrade.

Note Only the server groups (Vault Group, Cache Group, Stream Group, and SSV Group) of the VDS servers that were offloaded are listed.

The Off Load Servers List is populated with the VDS servers that were offloaded and are part of the group selected in the **Select Servers to Upgrade**.

Step 5 To select a VDS server for software upgrade, click the VDS server and click the **right-arrow** button. To select multiple VDS servers, hold down the **Shift** key while selecting each VDS server. To select all VDS servers, click the **double right-arrow.**

To deselect a VDS Server, click the VDS server in the Servers to Upgrade list and click the **left-arrow** button. To deselect multiple VDS servers, hold down the **Shift** key while selecting each VDS server. To deselect all VDS servers, click the **double left-arrow**.

Step 6 Click **Next**. A Username and Password is listed for each VDS server IP address.

Step 7 Enter the Username and Password for each VDS server that has “root” login credentials.

If more than one VDS server is being upgraded the **Use the Same Credentials for all Servers** check box is displayed. If all the VDS servers have the same login credentials, you can check the **Use the Same Credentials for all Servers** check box.

Step 8 Click **Start Upgrade**.

Software Upgrade Status

To view the status of the software upgrade or to cancel a software upgrade, do the following:

Step 1 Choose **Maintain > Servers > Software Upgrade Status**. The Software Upgrade Status page is displayed listing all the VDS servers that have been scheduled for a software upgrade.

The Status column displays the current status of the software upgrade for each VDS server. If the status is red, move the mouse pointer over the red box to get more information about the failure.

Step 2 If the status is Scheduled or Failure, the option to cancel the upgrade is available. To cancel a scheduled or failed software upgrade for a VDS server, check the **Cancel** check box and click **Cancel Upgrade**. To cancel all scheduled software upgrades, click the **Check ALL** check box and click **Cancel Upgrade**.

Step 3 If the status is a green box, the software upgrade was successful. After upgrading the software on the VDS server, restart the server (**Maintain > Servers > Server Restart**) and set the server to online (**Maintain > Servers > Server Offload**).

Setting System Thresholds

The System Thresholds page allows you to set thresholds for loss and usage of the VDS resources, as well as enable or disable monitoring of the VDS services. The Performance Parameters section of the page has threshold values; the System Services section of the page enables or disables monitoring of the specific services. To view the system services monitored, see Services Monitor, page 5-43. Table 7-6 lists each threshold in the Performance Parameters section, and where each threshold is monitored.

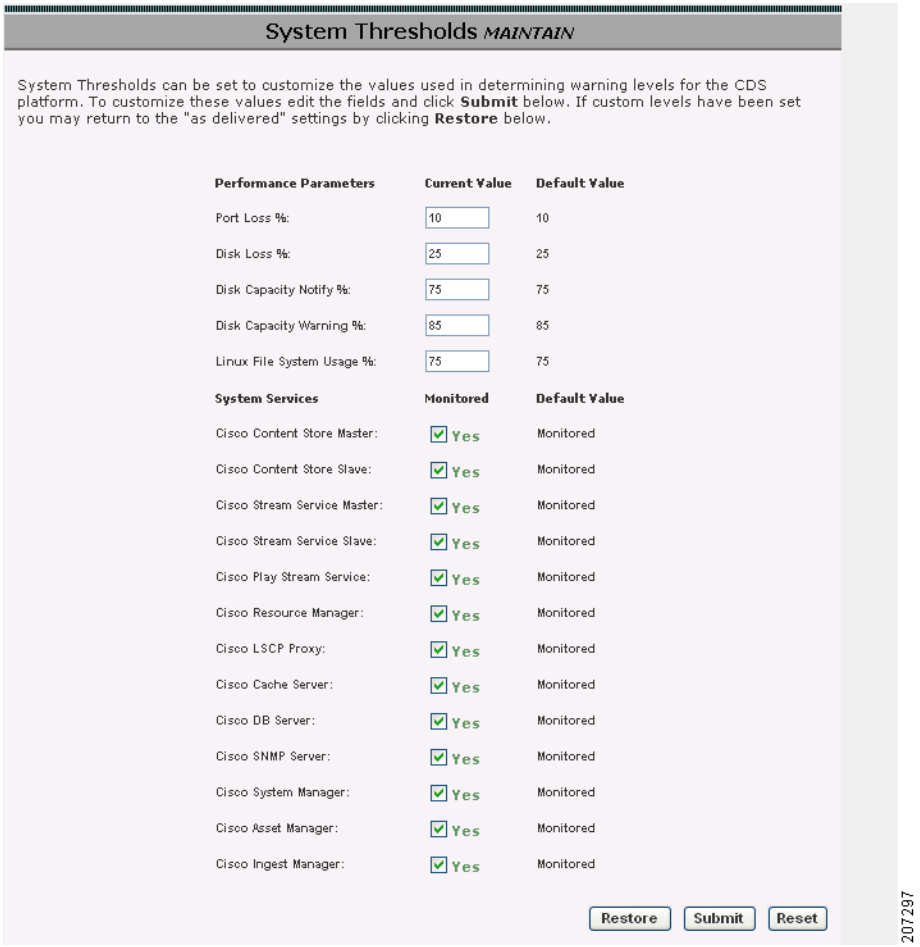
Table 7-6 Performance Thresholds

Threshold	Monitoring Page
Port Loss	The Network indicator box on System Health, page 5-3
Disk Loss	The Disk indicator box on System Health, page 5-3
Disk Capacity Notify	Disk Monitor, page 5-36
Disk Capacity Warning	Disk Monitor, page 5-36
Linux File System Usage	Disk Monitor, page 5-36

To set the system thresholds and enable or disable the system services, do the following:

Step 1 Choose **Maintain > Servers > System Thresholds.** The System Thresholds page is displayed (Figure 7-2).

Figure 7-2 System Thresholds Page



Step 2 Enter the threshold settings and enable or disable the services as appropriate.

Step 3 Click **Submit** to save the settings.

To clear the fields and start over, click **Reset**.

To restore the default settings, click **Restore**. The default values are shown in a separate column on the page.

Restarting the Services

Each server runs services that allow the server to function with other components in the VDS. Services are not automatically restarted each time there is a configuration change. If you need to restart a service, the Services Restart page provides this option. This action does not power cycle the unit. Table 7-7 describes the different services.

Table 7-7 Restart Services Options

Service	Description
Reload Service Groups	Any time there are changes (adding, editing, or deleting) to the QAM Gateway or Headend Setup configuration, it is necessary to reload the service groups. If the Content Storage feature is enabled, the Reload Service Group option is not available. It is not necessary to reload the service groups if the Content Storage feature is enabled.
ISA/OpenStream	Any time there are changes to the Streamer BMS or Vault BMS pages, it is necessary to restart the ISA/OpenStream service. If the Content Storage feature is enabled, it is not necessary to reload the ISA/OpenStream service, and therefore the option is not available.
SNMP	Any time there are changes to the SNMP configuration, it is necessary to restart the SNMP service.

To restart a service, do the following:

Step 1 Choose **Maintain > Services**. The Services Restart page is displayed.

Step 2 From the **Server IP/Name** drop-down list, choose the IP address or nickname of the server and click **Display**. The server type and ID, as well as the array ID, are displayed.

Step 3 Select the check box next to each service you want to restart and click **Submit**.

To clear the fields and start over, click **Reset**.

Content Manager

The Content Manager page allows deletion of multiple content objects.

Note The Content Manager page is part of the TV Playout feature and is displayed only if TV Playout feature is enabled. For more information, see Playout Scheduler, page F-13.

To delete multiple content objects, do the following:

Step 1 Choose **Maintain > Services > Content Manager**. The Content Manager page is displayed with the 100 most recent ingests listed.

The first text box and **Display** button provide access to the details of a completed ingest object and takes you to the **Monitor > System Level > Completed Ingests** page. Enter the first character of the content object name in the text box. A drop-down list of content objects is displayed. If there are more than 25

content objects that start with that first character you entered, you are prompted to continue entering the next character of the content object name or click **Display**. After you click **Display**, the Completed Ingest page is displayed with the details of the selected content object.

Step 2 To display a list of content objects, use one of the following methods:

- In the Browse Content box, click one of the characters. A list of content objects that begin with that character is displayed.
- In the Quick Lists box, the following options are offered:
  - **Most Recent Ingests (max 100)**—Lists the 100 most recent completed ingests sorted by ingest date.
  - **List All Contents**—Lists all completed ingests sorted by content name. This option is available only if the number of completed ingests is less than 100.
  - **Content Status (Damaged Only)**—Lists status information only for damaged completed ingests.

After you perform one of these methods, a list is displayed. The list of content objects can span several pages. To view the next page, click the page number. The content name, file size, duration, and date the object was ingested are displayed.

Step 3 Check the Delete check box next to each content object you want to delete, and click **Delete**.

Note It takes approximately four seconds to ensure the content is deleted from the entire system and the CDSM GUI displays the change before the next delete task is triggered. If a large number of content objects are selected for deletion, the time to complete the operation increases.

Software Maintenance

The Software Maintenance pages provides the ability to view the VDS software, upload an electronic program guide (EPG) file, generate server IDs and group IDs for Video Virtualization Infrastructure (VVI), and perform a clean-up on the system. This section covers the following topics:

Viewing the Software Version and Server Information

To view the VDS software version and server information, choose **Maintain > Software > Software Version**. The Software Version page is displayed. From the **Server IP** drop-down list, choose a server IP address or nickname and click **Display**. The following information is displayed:

- Server type (Vault, Streamer SSV (ISV))
- Software version
- Server ID
- Array ID
- Product ID (PID)—CDE model (for example, CDE220)
- Version ID (VID)—Hardware version (for example, V01)
- Serial number—Serial number of the CDE
- Additional string—Model variation (for example, 4A-C)

Configuring the TV Playout Application

The Application Configuration page allows you to choose the Streamers participating in streaming content for the TV Playout application, and to choose how the Streamers participate. The following applications are configurable:

- Barker Stream/Playlists
- Playout Scheduler

Note The Application Configuration page is part of the TV Playout feature and is displayed only if TV Playout feature is enabled. For more information, see Playout Scheduler, page F-13.

The Streamers, or ISVs, chosen for the TV Playout application participate in an **active-standby** relationship, or an **active-active** relationship.

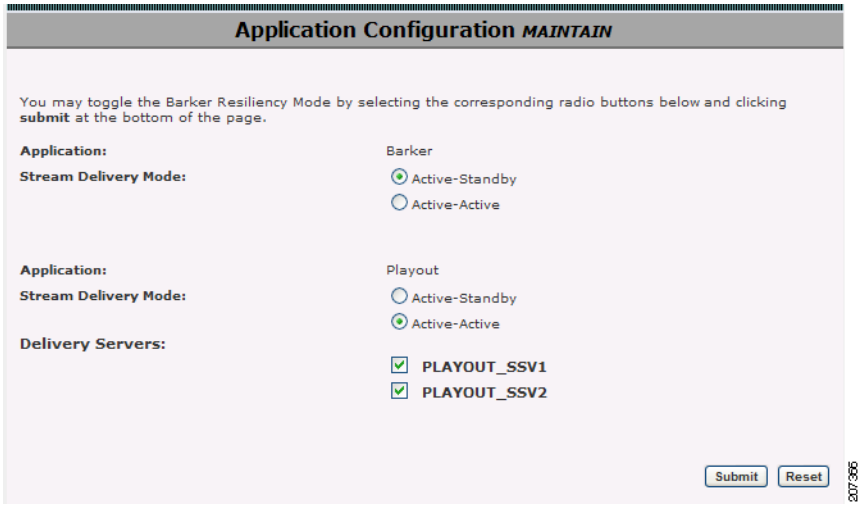
In an **active-standby** relationship, one server acts as the authority and all streams initiate from this server. The other servers participating in streaming for the TV Playout application only take over when the active server goes offline.

In an **active-active** relationship, all servers participating in the TV Playout application, stream the content at the same time.

To configure the Barker Stream and Playout Schedule applications, do the following:

Step 1 Choose **Maintain > Software > Application Configuration**. The Application Configuration page is displayed (Figure 7-3).

Figure 7-3 Application Configuration Page



Step 2 Choose the **Stream Delivery Mode**.

Active-Standby—All streams initiate from one server (active). The other servers (standby) only take over when the active server goes offline.

Active-Active —All servers stream the content at the same time.

Note Stream Failover must be disabled if the **Stream Delivery Mode** is set to **Active-Active**. Stream Failover must be enabled if the **Stream Delivery Mode** is set to **Active-Standby**. For more information on setting Stream Failover, see Stream Failover Support, page F-3.

Step 3 For **Active-Active**, check the check box next to each server participating in each application.

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

To clear the fields and start over, click **Reset**.

Importing a TV Playout Schedule

The Playout Importer page can be used to upload a Playout file, containing the Playout Scheduler data from another VDS, into the Playout Scheduler of this VDS. The Playout file is an XML file.

Note The Playout Importer page is part of the TV Playout feature and is displayed only if the TV Playout feature is enabled. For more information, see Playout Scheduler, page F-13.

To import a Playout file, do the following:

Step 1 Choose **Maintain > Software > Playout Importer**. The Playout Importer page is displayed.

Step 2 In the **Playout Export Location** text box, enter the full path and filename, or click **Browse** to locate the file using the Browse window.

Step 3 When importing a Playout file, each channel is checked for an existing playout schedule, if there are conflicts, the setting in the **Action on Import** field is used to decide how to handle the conflict.

Select **Preserve existing schedules**, to preserve the existing playout schedule when a conflict is identified. Select **Overwrite existing schedules**, to overwrite the existing playout schedule.

Step 4 Click **Import**.

To clear the fields and start over, click **Reset**.

Upgrade Status of the TV Playout Application

When upgrading the VDS-VR (formerly CDS-TV) software from Release 1.5.4.6, there are some steps that must be followed before any configuration changes can occur. The Playout Upgrade Status page tracks the status of these steps. Clicking the Status of each step takes the user to the page that needs to be modified. (For the link to work on the first one, the user needs to have Engineering-level access.)

Additionally, the Alarms table displays an alarm stating the playout upgrade is incomplete.

Note The Playout Upgrade Status page is part of the TV Playout feature and is displayed only if the TV Playout feature is enabled. For more information, see Playout Scheduler, page F-13.

Uploading an EPG File

The EPG File Upload page can be used to upload an electronic program guide (EPG) file into the VDS for use with the Media Scheduler. The EPG file is an XML file.

Note The EPG File Upload page is part of the Media Scheduler feature. For more information, see Media Scheduler, page F-12.

Before you can upload an EPG file, you need to enter the channel information. See Configuring Input Channels, page 4-26 for more information.

To upload an EPG file, do the following:

Step 1 Choose **Maintain > Software > EPG Upload**. The EPG File Upload page is displayed.

Step 2 Enter the full path and filename in the **EPG File Location** field, or click **Browse** to locate the file using the Browse window.

Step 3 After the full path and filename of the EPG File is entered, click **Upload**.

To clear the fields and start over, click **Reset**.

Identifying Server IDs and Group IDs for VVI with Split-Domain Management

When using CCP Streamers in a VVI with split-domain management, it is mandatory that all group IDs and server IDs be unique for each server in the system. To assure this, the VVIM manages all the identifiers, and the Stream Managers get a range of group IDs and server IDs from the VVIM and uses them for the Streamers it manages.

Table 7-8 lists the CDSM GUI ID names and maps them to the CServer names in the setupfile and .arroyorc files.

Table 7-8 ID Names in the CDSM GUI and CServer Files

CDSM GUI ID Name	CServer Files ID Name
Array ID on the Array Name page	groupid
Group ID on the Server-Level pages	groupid
Stream Group ID on the Server Setup page	arrayid
Cache Group ID on the Server Setup page	arrayid
Vault Group ID on the Server Setup page	arrayid
Stream Group ID on the Configuration Generator page	arrayid

Generating Server IDs and Group IDs from the VVIM

The Configuration Generator page is used to generate group IDs and server IDs for the Stream Managers. When the Stream Manager contacts the VVIM during the initial configuration using the cdsconfig script, the VVIM generates the IDs, sends them to the Stream Manager, and populates the table on the Configuration Generator page. This is done by an HTTP GET request over port 80.

If the Stream Manager is unable to contact the VVIM during the initial configuration, the cdsconfig script prompts the Stream Manager administrator to contact the VVIM administrator for the server ID. The VVIM administrator would then go to the Configuration Generator page to generate the IDs for the Stream Manager.

For HTTP streamers, if the Stream Manager is unable to reach the VVIM, either because port 80 is not open for communication or because of some other connectivity reason, the Stream Manager administrator can contact the VVIM administrator for the needed information. This information consists of the following:

- Stream Group IDs
- Cache Group information

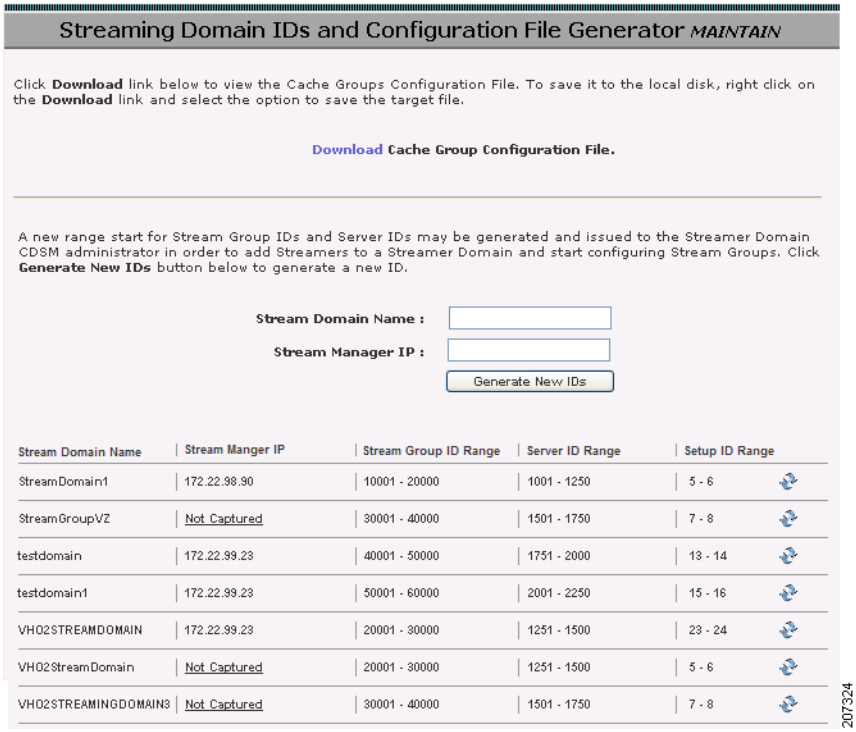
Using the Configuration Generator page, the VVIM administrator can look up the group ID and server ID ranges, and if necessary generate them. The VVIM administrator can provide the beginning group ID for the Stream Groups, which the Stream Manager administrator enters on the Stream Groups Setup page, if prompted to do so.

The Cache Group information is contained in an XML file, called CacheGroupsConfig.xml. The VVIM administrator can click the **Download** link to view the CacheGroupsConfig.xml file, and right-click the **Download** link to save the XML file locally. This XML file can be sent to the Stream Manager administrator and the Stream Manager can upload it through the Cache Group Locator page.

To generate new IDs or view the existing IDs, do the following:

Step 1 Choose **Maintain > Software > Configuration Generator.** The Configuration Generator page is displayed (Figure 7-4).

Figure 7-4 Configuration Generator Page



Step 2 In the **Stream Domain Name** field, enter the name of the Stream Manager that you are generating IDs for.

Step 3 In the **Stream Manager IP** field, enter the IP address of the Stream Manager that you are generating IDs for.

Step 4 Click **Generate New IDs**.

Configuration Generator Table

The table on the Configuration Generator page lists the Stream Domain Name, Stream Manager IP address, and the ID ranges assigned for each Stream Manager.

Stream Group ID Range and Server ID Range

Sometimes the group IDs and Server IDs show as "not generated" in the table. To generate the IDs, click the **Not Generated** text in the Stream Group ID Range column. A dialog box is displayed asking if you want to generate the IDs now. Click **OK**.

Stream Manager IP Address

The IP address of the Stream Manager is not included in the table on the Configuration Generator page until the Stream Manager is configured using the CDSM Setup page. It is possible that the Stream Manager IP address failed to be captured, in which case the entry is displayed as "Not Captured." Click the **Not Captured** link to enter the IP address manually. A text box is displayed with an Update icon (plus sign) and a Cancel icon (X).

Setup ID Range

Setup IDs are only used in RTSP environments that have split-domain management and are using CCP Streamers. The VVIM only generates two setup IDs for each Stream Domain. A setup ID is used to identify the Setup server in a Stream Group. The Setup and Control servers are configured for each Stream Group on the Control/Setup IP page. See Configuring the Control and Setup IPs, page 4-50 for more information. If the Stream Manager uses the two allotted setup IDs, it contacts the VVIM for a new set of setup IDs. If the connection between the Stream Manager and VVIM fails, the Stream Manager administrator contacts the VVIM administrator for the IDs. The new setup IDs can be generated by clicking the **Generate new Setup ID** range icon in the Setup ID Range column.

Note CCP Streamers are not supported in a VVI split-domain management for RTSP environments.

Generating a Server ID from the Stream Manager

The Server ID Generator page is used to generate a server ID for a Streamer that is being added to the VVI, but is unable to communicate with the Stream Manager. During the initial configuration, the Streamer contacts the Stream Manager and requests a server ID. If the Streamer is unable to contact the Stream Manager, the cdsconfig script displays a prompt to contact the Stream Manager administrator for a server ID. The Stream Manager administrator would then go to the Server ID Generator page to generate a server ID for the Streamer.

Note The Server ID Generator page is available only on the Stream Manager when VVI and Content Storage are enabled in an ISA environment. For more information, see Content Storage, page F-11 and Virtual Video Infrastructure, page F-8.

There is a range of server IDs, 1 to 1000, that are reserved for Vaults and Caching Nodes. It is the responsibility of the VVIM administrator to make sure the server IDs are unique among all Vaults and Caching Nodes in the VVI. The VVIM reserves a group of 250 server IDs for each Stream Domain (for example, 1001-1250, 1251-1500, and so on).

To generate a server ID for a Streamer, do the following:

Step 1 Choose **Maintain > Software > ID Management.** The Server ID Generator page is displayed; including the System ID Settings, which consist of the following:

- Group ID Range Start—Beginning ID for the Stream Groups, Vault Groups, and Cache Groups
- Server ID Range Start—Beginning ID for the VDS servers in the system

- Setup ID Range Start—Beginning ID for the Streamer Setup server

Step 2 Click **Generate New ID**. The new server ID is displayed in the Server ID field.

System Cleanup

The System Cleanup page allows you to clean up any errors that may have accumulated on your system. When errors occur, they are added to the Alarms table. See Alarms Table, page 5-2 for more information and other alarms and alerts that link to other CDSM pages.

The following errors and situations are monitored and registered in the Alarms table if found and linked to the System Cleanup page:

- Orphaned server IDs
- Multiple or duplicate Cache Locate IP addresses
- Out of range Group IDs
- ServerMap and StatMap inconsistencies
- Extra or incorrect SERVERMAP15 entries

The System Cleanup page displays a **Fix All** option if there are no errors found for the Cache Locate IP addresses (either Multiple or Duplicate). If Multiple or Duplicate Cache Locate IP addresses errors are found, then the **Fix All** option is not displayed until these are resolved, because they require user input as to which entry to keep and which entry to remove.

Orphaned Server IDs

Orphaned Server IDs occur when servers are removed from the CDSM without first removing them from the groups they belong to (for example, Vault Group or Stream Group). This leaves a reference in the groupmap table to the server ID that is no longer valid, which means the group can no longer be edited through the CDSM GUI.

Multiple or Duplicate Cache Locate IP Addresses

The CDSM GUI checks and validates user input to prevent multiple locate entries in the VDS server setupfile files; this is an additional check for multiple or duplicate Locate IP addresses. The Locate IP address is used in VVIM systems with HTTP as the cache-fill protocol. The procedures are different between multiple and duplicate Locate IP addresses:

- Duplicate Locate IP Addressees—Two or more identical entries in the control IP map table for a single Cache Group, having the same group ID, locate IP, and locate subnet IP. If this has occurred, select any one of the entries for removal, and the CDSM automatically reduces the number of entries to one.
- Multiple Locate IP Addresses—More than the required single-entry for a Cache Group, and the entries are not identical in that they have differing IP addresses or subnets. If this has occurred, select the entries you want removed.

Out of Range Group IDs

Sometimes the CDSM is configured as a legacy system with Stream Groups and Vault Groups, only later to find that it was incorrectly configured and needs to be changed to a VVIM or Stream Manager. This creates Stream Group map table entries that use the incorrect group ID range with no method of removing them from the CDSM GUI because the configuration pages for groups correctly filters out the incorrect group IDs from the drop-down lists. The Out of Range Group IDs check cleans up these groups.

SERVERMAP and STATMAP Inconsistencies

When adding a large number of VDS servers to a CDSM, mistakes can be made with regard to the .arroyorc file found on each VDS server (for example, incorrect group ID [array ID] or IP address). This can lead to incorrect entries in the server STATMAP table. Additionally, servers that are not removed correctly can also leave an incorrect entry in the server STATMAP table. The server STATMAP table is used to generate the System Monitor content and errors in it can lead to display issues and incorrect states being displayed.

Extra or Incorrect SERVERMAP Entries

If the CDSM is reconfigured or reinstalled for a different type of VDS (legacy or VVI) and the CDSM is not properly wiped clean, there could be residual entries in the SERVERMAP15 table and STATMAP table that do not apply to the current configuration.

Manuals

To view the manual, choose **Maintain > Manuals**. The Manual page is displayed. Click the link to the manual. The manual is displayed by means of the Acrobat Reader plug-in for your browser.

Tip To download the manual to your computer, right-click the link of the manual and save the manual to a location on your hard drive for later viewing.