Configuring the System

The following sections describe how to configure ECDS system parameters:

- Configuring AAA, page 9-1
- Changing a Password, page 9-8
- Configuring System Settings, page 9-9
- Where to Go Next, page 9-17

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 ECDS 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 an ECDS 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 covers login authentication and authorization for the CDSM. For information about device login authentication and authorization, see the “Login Access Control” section on page 5-69 and the “Authentication” section on page 5-76.

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.

**Note**
User Name, TACACS User Name, Roles Name, and Domain Name should contain Lower case (a-z) and Upper case (A-Z) characters, Numbers (0-9), space, and special characters - _ / only.

## 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 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:

- 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:

- 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:

**Step 1**  Choose **System > AAA > Users**. The User Table page is displayed.  
*Table 9-1* describes the icons for the User Table page.

**Table 9-1  User Table Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Create New]</td>
<td>Creates a new entry.</td>
</tr>
<tr>
<td>![Edit]</td>
<td>Edits an entry.</td>
</tr>
<tr>
<td>![Filter]</td>
<td>Creates a filtered table. Filter the table based on the field values.</td>
</tr>
<tr>
<td>![View]</td>
<td>Views all table entries. Click this icon to view all entries after you have created a filtered table.</td>
</tr>
<tr>
<td>![Refresh]</td>
<td>Refreshes the table.</td>
</tr>
<tr>
<td>![Print]</td>
<td>Prints the current window.</td>
</tr>
</tbody>
</table>

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

![Creating New User Account]

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.

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.

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, click **Role Management**. The Role Management Table page is displayed.

   Table 9-1 describes the icons for the Role Management page.

### Table 9-2  Role Management Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Creates a new entry.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>Edits an entry.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon" /></td>
<td>Creates a filtered table. Filter the table based on the field values.</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon" /></td>
<td>Views all table entries. Click this icon to view all entries after you have created a filtered table.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Icon" /></td>
<td>Refreshes the table.</td>
</tr>
<tr>
<td><img src="image6.png" alt="Icon" /></td>
<td>Assigns all roles.</td>
</tr>
<tr>
<td><img src="image7.png" alt="Icon" /></td>
<td>Removes all roles.</td>
</tr>
</tbody>
</table>
Table 9-2  Role Management Icons (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>![View icon]</td>
<td>Views read-only items.</td>
</tr>
<tr>
<td>![Checkmark icon]</td>
<td>Indicates that the current transaction was successfully completed.</td>
</tr>
</tbody>
</table>

To add roles, see the “Creating, Editing, and Deleting Roles” section on page 9-6.
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 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, click Domain Management. The Domain Management Table page is displayed.
To add domains, see the “Creating, Editing, and Deleting Domains” section on page 9-7.
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 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 ECDS 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:

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

Figure 9-3 Roles Table Page

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 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 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 ECDS network entities or objects that make up the ECDS network. Whereas a role defines which services a user can perform in the ECDS 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:

**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.

**Figure 9-4Creating New Domain**
Changing a Password

If you are a user without admin privileges and you are logged in to the CDSM, 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.

⚠️ 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 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:

Step 1  Choose System > Password. The Password page is displayed.
Step 2  In the New Password field, enter the changed password.
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, page 9-9
- Configuring Fast SE Offline Detection, page 9-10
- Configuring Distribution QoS, page 9-11
- Configuring System Status Alarm, page 9-13
- WMT Live QoS Support Across WAN, page 9-14
- Configuring Service Routing, page 9-14

System Properties

To modify the system properties:

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 9-3 describes the system properties.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdsn.session.timeout</td>
<td>Length of a Content Distribution Manager session (in minutes). The default is 10. The range is from 5 to 120.</td>
</tr>
<tr>
<td>DeviceGroup.overlap</td>
<td>SE feature overlapping (true or false).</td>
</tr>
<tr>
<td>System.CmsUnsProgram.Sync.Interval</td>
<td>Interval by which CMS synchronizes program import UNS objects (in minutes). The default is 1440 minutes. The range is from 1 to 43200.</td>
</tr>
<tr>
<td>System.datafeed.pollRate</td>
<td>Poll rate between the SE or the SR and the CDSM (in seconds). The default is 300. The range is from 30 to 1800.</td>
</tr>
<tr>
<td>System.device.recovery.key</td>
<td>Device identity recovery key. This property enables a device to be replaced by another node in the ECDS network.</td>
</tr>
<tr>
<td>System.healthmonitor.collectRate</td>
<td>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.</td>
</tr>
<tr>
<td>System.Icm.enable</td>
<td>Local and CDSM feature (true or false). This property allows settings that are configured using the local device CLI or the CDSM to be stored as part of the ECDS network configuration data.</td>
</tr>
<tr>
<td>System.monitoring.collectRate</td>
<td>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.</td>
</tr>
<tr>
<td>System.monitoring.dailyConsolidationHour</td>
<td>Hour at which the CDSM consolidates hourly and daily monitoring records. The default is 1. The range is from 0 to 23.</td>
</tr>
</tbody>
</table>
Configuring System Settings

Chapter 9 Configuring the System

Configuring System Settings

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

### Configuring Fast SE Offline Detection

You can detect offline SEs more quickly if you enable the Fast Detection of Offline SEs feature.

If Fast Detection of Offline SEs is not enabled, the CDSM waits for at least two “System.datafeed.pollRate” polling periods before declaring the SE offline.

If Fast Detection of Offline SEs is enabled, the CDSM waits until the value displayed in the Maximum Offline Detection Time field, located on the Configure Fast SE Offline Detection page, is exceeded.

Communication between the SE and CDSM using User Datagram Protocol (UDP) allows faster detection of SEs that have gone offline. UDP heartbeat packets are sent at a specified interval from each SE to the primary CDSM in an ECDS 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 nonresponsive SEs as offline. Because UDP heartbeats require less processing than a getUpdate request, they can be transmitted more frequently, and the CDSM can detect offline SEs much faster.

An SE is declared offline when it has failed to contact the CDSM for a getUpdate request (get configuration poll) for at least two polling periods.

**Note**

In ECDS 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.

---

**Table 9-3 System Properties Fields (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System.monitoring.enable</td>
<td>SE statistics monitoring (true or false).</td>
</tr>
<tr>
<td>System.monitoring.monthly</td>
<td>Frequency (in days) with which the CDSM consolidates daily</td>
</tr>
<tr>
<td>ConsolidationFrequency</td>
<td>monitoring records into monthly records. The default is 14. The range is</td>
</tr>
<tr>
<td></td>
<td>from 1 to 30.</td>
</tr>
<tr>
<td>System.monitoring.record LimitDays</td>
<td>Maximum number of days of monitoring data to maintain in the system.</td>
</tr>
<tr>
<td></td>
<td>The default is 1825. The range is from 0 to 7300.</td>
</tr>
<tr>
<td>System.repstatus.update Enabled</td>
<td>Replication status periodic calculations on an SE (enable or disable).</td>
</tr>
<tr>
<td>System.repstatus.updateRate</td>
<td>Rate of replication status periodic updates calculated on an SE (in minutes).</td>
</tr>
<tr>
<td>Sec</td>
<td>The default is 10. The range is from 5 to 1440.</td>
</tr>
<tr>
<td>System.repstatus.updateRate Sync</td>
<td>Rate of replication status periodic updates calculated on an SE (in</td>
</tr>
<tr>
<td>Sec</td>
<td>seconds). The default is 600 seconds. Setting this rate overrides the</td>
</tr>
<tr>
<td></td>
<td>update rate set in minutes. The ranges is from 30 to 86400.</td>
</tr>
<tr>
<td>System.repstatus.updateSync</td>
<td>Sending summary replication status with requested detailed status (true</td>
</tr>
<tr>
<td>Enabled</td>
<td>or false).</td>
</tr>
</tbody>
</table>

---

Cisco ECDS 2.6 Software Configuration Guide
To configure Fast Detection of Offline SEs:

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

*Note* The Fast Detection of Offline SEs feature is in effect only when the CDSM receives the first UDP heartbeat packet and a getUpdate request from an SE.

**Step 2** Check the **Enable** check box to enable the CDSM to detect the offline status of SEs quickly.

*Note* SEs can have their software upgraded without any errors in the status being displayed in the CDSM if you disable Fast Detection of Offline SEs.

**Step 3** In the **Heartbeat Rate** field, specify how often, in seconds, the SEs should transmit a UDP heartbeat packet to the CDSM. The default is 30. The range is from 30 to 3600.

**Step 4** 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 1. The range is from 1 to 100.

**Step 5** 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:

\[
\text{Maximum Offline Detection Time} = \text{Failed heartbeat count} \times \text{Heartbeat rate}
\]

If Fast Detection of Offline SEs is enabled, the CDSM detects SEs that are in network segments that do not support UDP and uses a getUpdate request (get configuration poll) to detect offline SEs.

If the CDSM does not receive regular keep-alive communication from an SE, the CDSM displays the SE as offline after a time period of \(2 \times (\text{Heartbeat rate}) \times (\text{Failed heartbeat count})\).

**Step 6** 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 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:
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 next section, “Setting DSCP Values for QoS Packets,” for 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 8-12 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 **QoS 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 ECDS 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 9-4**.)

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description and Value</th>
</tr>
</thead>
</table>
| 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). |
Chapter 9  Configuring the System

Configuring System Settings

Configuring System Status Alarm

To configure system status alarm settings:

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

**Figure 9-5  System Status Alarm Page**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description and Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>af32</td>
<td>Sets packets with AF32 DSCP (011100).</td>
</tr>
<tr>
<td>af33</td>
<td>Sets packets with AF33 DSCP (011110).</td>
</tr>
<tr>
<td>af41</td>
<td>Sets packets with AF41 DSCP (100010).</td>
</tr>
<tr>
<td>af42</td>
<td>Sets packets with AF42 DSCP (100100).</td>
</tr>
<tr>
<td>af43</td>
<td>Sets packets with AF43 DSCP (100110).</td>
</tr>
<tr>
<td>cs1</td>
<td>Sets packets with CS1 (precedence 1) DSCP (001000).</td>
</tr>
<tr>
<td>cs2</td>
<td>Sets packets with CS2 (precedence 2) DSCP (010000).</td>
</tr>
<tr>
<td>cs3</td>
<td>Sets packets with CS3 (precedence 3) DSCP (011000).</td>
</tr>
<tr>
<td>cs4</td>
<td>Sets packets with CS4 (precedence 4) DSCP (100000).</td>
</tr>
<tr>
<td>cs5</td>
<td>Sets packets with CS5 (precedence 5) DSCP (101000).</td>
</tr>
<tr>
<td>cs6</td>
<td>Sets packets with CS6 (precedence 6) DSCP (110000).</td>
</tr>
<tr>
<td>cs7</td>
<td>Sets packets with CS7 (precedence 7) DSCP (111000).</td>
</tr>
<tr>
<td>default</td>
<td>Sets packets with default DSCP (000000).</td>
</tr>
<tr>
<td>ef</td>
<td>Sets packets with EF DSCP (101110).</td>
</tr>
</tbody>
</table>

**Step 2** Check the **System Status Alarm** check box to enable the system status alarm. If you do not want the system status alarm to be displayed in the GUI page, disable it from the CDSM page. By default, the check box is disabled.
Step 3  Click **Submit** to save the settings.

---

**WMT Live QoS Support Across WAN**

In previous releases, QoS (DSCP markings) support for Live WMT traffic was between the Service Engine (SE) and client on the remote site LAN. With this new feature in Release 2.6.2, customers can now extend the QoS DSCP marking as well across the WAN for RTSP and HTTP live traffic.

Live streaming support for QoS across the WAN is important as enterprise customers need and desire more control across their WAN infrastructure where the bandwidth may be limited and/or expensive.

The DSCP configuration setting in the "QoS value for content delivery" on the "Creating New Delivery Service" page in CDSM has been been extended in its usage for WMT. Instead of just Service Engine to Client on LAN, it now also applies between Service Engines/Content Acquirers and Service Engines across the WAN.

![Figure 9-6 Delivery Service Page](image)

**Note**  When configuring Delivery Services to be used on the same origin server, the QoS settings will only take effect for the first configured Delivery Service. All subsequent Delivery Services will not contain the QoS value for WMT streams between Service Engines. QoS values will be maintained between the Service Engine and Client for all Delivery Services.

---

**Configuring Service Routing**

The Service Routing menu options consist of the following:

- **Coverage Zone File Registration**, page 9-15
- **Configuring Global Routing**, page 9-16
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 following sections in this guide:

- “Coverage Zone File”
- “Creating Coverage Zone Files”

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 ECDS 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 CDSM 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 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 ECDS 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:

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, FTP, or CIFS 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 9-5 describes the upload method fields. Table 9-6 describes the import method fields.

<table>
<thead>
<tr>
<th>Table 9-5</th>
<th>Upload Method for Coverage Zone Files</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Coverage Zone File Upload</td>
<td>Local directory path to the Coverage Zone file. To locate the file, use the <strong>Browse</strong> button. Click the <strong>Validate</strong> button to validate the Coverage Zone file.</td>
</tr>
<tr>
<td>Destination Filename</td>
<td>Name of the Coverage Zone file. This field is filled in automatically with the filename from the local directory path.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 9-6</th>
<th>Import Method for Coverage Zone Files</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Property</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Coverage Zone File URL</td>
<td>The URL where the Coverage Zone file is located, including path and filename. Click the <strong>Validate</strong> button to validate the Coverage Zone file.</td>
</tr>
<tr>
<td>Destination File Name</td>
<td>Name of the Coverage Zone file.</td>
</tr>
<tr>
<td>Update Interval (minutes)</td>
<td>Frequency with which the CDSM looks for changes to the Coverage Zone file. The default value is 10 minutes.</td>
</tr>
<tr>
<td>Username</td>
<td>Name of the user to be authenticated when fetching the Coverage Zone file.</td>
</tr>
<tr>
<td>Password</td>
<td>User password for fetching the Coverage Zone file.</td>
</tr>
<tr>
<td>NTLM user Domain</td>
<td>NT LAN Manager (NTLM) user domain name for NTLM authentication.</td>
</tr>
<tr>
<td>Disable Basic Authentication</td>
<td>When checked, NTLM headers cannot be stripped off to allow fallback to the basic authentication method. If you leave this check box unchecked, NTLM authentication headers can be stripped to allow fallback to the basic authentication method, and the username and password information can be passed to the origin server in clear text with a basic authentication header.</td>
</tr>
</tbody>
</table>

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:

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 60. The default is 60 seconds.

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

---

**Tip**  To apply a Coverage Zone file to an individual SR for local coverage zone configuration, see the “Configuring Service Router Settings” section on page 5-115.

---

**Where to Go Next**

See the following support documentation:

- For information about system output logs, see the “System Audit Logs” section on page 10-7.
- For information on upgrading the ECDS software, see the “Upgrading Software” section on page 11-1.
- For information on the ports used by the ECDS, see the “System Port Numbers” section on page 10-8.