Configuring Devices

This chapter discusses configuring locations and devices, and detailed instructions on configuring the different types of devices–VDSMs, SBs. This chapter presents the following major topics:

Configuring Locations

Locations are set up in the VDSM to organize and group SBs into virtual networks for routing content to appropriate CDNs.

Locations need to be configured before you can activate SBs and bring them online in the VDS-SB network. Table 3-1 describes the icons for the Locations Table page.

Table 3-1 Location Icons

Icon	Function
	Create a new location.
	Create a filtered table.
	View all locations.
	Refresh the table.
	Print the current window.
	Edit a location.

To create a new location or edit an existing one, do the following:

Step 1 Choose **Devices > Locations**. The Locations Table page is displayed.

The table is sortable by clicking the column headings.

Step 2 In the task bar, click the **Create New Location** icon. The Creating New Location page is displayed.

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

Step 3 Enter the settings as appropriate. See Table 3-2 for a description of the fields.

Table 3-2 Location Fields

Field	Description
Name	Name of the location.
Parent Location	Choose a location from the drop-down list. A location with no parent, None, is level 1. The location level is displayed after you choose a parent location.
Comments	Enter any information about the location.

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

To delete a location, from the Locations Table page, click the **Edit** icon next to the location you want to delete, and click the **Delete** icon in the task bar.

To view the location tree, click the **Location Trees** icon in the task bar. The location tree represents the network topology you configured when you assigned a parent to each location.

Configuring the Service Broker

This section walks you through the different configuration pages available for a Service Broker. The main configuration groups are described as follows:

- Broker Settings—Routing settings for Service Broker
- General Settings—Settings for access control of the device, maintenance, network connectivity, and monitoring

Activating a Service Broker

Activating a device (Service Broker) can be done through the Device Activation page.

To activate a device from the Device Activation page, do the following:

Step 1 Choose **Devices > Devices**. The Devices Table page is displayed.

Step 2 Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.

Step 3 Click **Show All** to display the top-level menu options, and click **Device Activation**. The Device Activation page is displayed.

Step 4 Enter the settings as appropriate. See Table 3-3 for a description of the fields.

Table 3-3 Device Activation Fields

Field	Description
Name	Name of the device.
Location	Lists all the locations configured for the VDS-SB.
Status	Status of the Service Broker. It can have the following values: • Online • Offline • Inactive • Pending • Offloading
Activate	To activate or deactivate the device, check or uncheck the **Activate** check box.
Server Offload	To offload this device for maintenance or a software upgrade, check the **Server Offload** check box. When checked, SB stops processing client requests.
DNS TTL	The time period (in seconds) for caching DNS replies. the range is from 0 to 60 seconds and the default is 60 seconds.
CDN IP Network File	CDN IP network file configured at SB level. The network file should be fist registered through System->Configuration->CDN IP Network File Registration. If not configured, global CDN IP Network File, if any, will take effect.
Use SB's primary IP address	Enables the VDSM to use the IP address on the primary interface of the SB for management communications. **Note** If the **Use SBs primary IP Address for Management Communication** check box is checked and the Management Communication Address and Port are configured, the VDSM uses the SB's primary IP address for communication.
Management Communication Address	Manually configures a management IP address for the VDSM to communicate with the SB. Manual configuration of the management IP address and port are used when using port channel configuration to separate management and streaming traffic. For more information about port channel configuration see the "Configuring Port Channel and Load Balancing Settings" section on page 3-25
Management Communication Port	Port number to enable communication between the VDSM and the SB.
Comments	Information about the settings.

Note To make sure the SB is binding to the primary interface (or management IP address if configured) as the source IP address when sending management traffic to the VDSM, create a static route from the SB to the VDSM. To configure a static IPv4 route from the SB, see the "Configuring Static IPv4 Routes" section on page 3-35 section. Alternatively, you can use the **ip route** command on the VDS-SB device.

Note Service Broker uses Primary interface IP for binding DNS to that interface. Primary designation denotes which interface will have DNS/HTTP bound to it for client requests to ensure proper routing. In prior release, primary interface was configured to management/internal network. Now, primary interface must be client facing since DNS/HTTP is bound there.

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

Broker Settings

Enabling Geo Location Service for Service Broker

Service Broker supports querying a collocated server running Neustar (previously was referred to as Quova prior to Neustar's puchase) GDS v6 for retrieving geo location parameters. The time taken to retrieve this information increases the total latency to redirect a request as compared to when geo-location information not used. SB does caching of the information retrieved per IP address, and thus it will not incur this for following requests. The Geo location query C-API interface with GDS utilizes TCP sessions destined to port 7000. The weekly updates from GDS will be over HTTP (port 80).To enable routing settings for a Service Broker, do the following:

Step 1 Choose **Devices > Devices**, and click the **Edit** icon next to the device you want to assign.

Step 2 Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.

Step 3 Click **Show All** to display the top-level menu options, and click **Broker Settings > Request Broker Settings > General Settings**. The Routing Settings page is displayed.

Step 4 Enter the settings as appropriate. See Table 3-4 for a description of the fields.

Table 3-4 Routing Settings for Service Broker

Field	Description
Enable Geo Location Service	To enable or disable the Geo Location service, check or uncheck the Enable Geo Location Service checkbox
Geo Location cache Timeout	The timeout value in seconds of Geo Location Cache. The range is from 0 to 864000 seconds and default is 0 seconds
Geo Location Cache Max Entries	The maximum number of entries that can be entered in Geo-Location cache. The range is from 10000 to 100000 entries. The default is 10000 entries
Primary Geo-Location Server IP Address	IP address of the Primary Geo-Location Server
Port	Port number at which the Primary Geo-Location Server is listening to.

Table 3-4 Routing Settings for Service Broker

Field	Description
Secondary Geo-Location Server IP Address	IP address of the Secondary Geo-Location Server
Port	Port Number at which the Secondary Geo Location Server is listening to.

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

Access Policy Settings for Service Broker

To enable access policy settings for a Service Broker, do the following:

Step 1 Choose **Devices > Devices**, and click the **Edit** icon next to the device you want to assign.

Step 2 Click the **Edit** icon next to the device you want to configure. The Devices home page is displayed.

Step 3 Click **Show All** to display the top-level menu options, and click **Broker Settings > Request Broker Settings > Access Policy**. The Access Policy Settings page is displayed.

Step 4 To enable Access Policy for a Service Broker, check the **Enable Access Policy** checkbox.

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

General Settings

The General Settings pages provide settings for access control of the device, maintenance, network connectivity, and monitoring. The configuring of general settings consists of the following procedures:

- Login Access Control
- Authentication
- Setting Storage Handling
- Network Settings
- Configuring Notification and Tracking
- Configuring Troubleshooting

Login Access Control

Login authentication and authorization are used to control user access and configuration rights to VDSMs and SBs. Login authentication is the process by which the devices verify whether the person who is attempting to log in to the device 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 an authentication, authorization, and accounting (AAA) database, and the devices must be configured to access the particular authentication server (or servers) where the AAA database is kept.

In a VDS-SB network, user accounts can be created for access to the VDSM and, independently, for access to the SBs that are registered to the VDSM. For user accounts that access the VDSM, see the "Configuring AAA" section on page 5-1.

Login Authentication

Login authentication provides the configuration for independent logins; in other words, login access to the device only.

Login authentication can also be used to log in to the VDSM GUI. When logging in to the VDSM GUI with an external user account (RADIUS or TACACS+), the user is authenticated by the external database. After the external user is authenticated, its role depends on the privilege configured in the external database (zero [0] means a normal user and 15 means a super user). The privilege level of 0 or 15 is mapped to the read-only or admin user role in the VDSM GUI. No VDSM local user is created in the VDSM database for the external user that logs in, so the external user cannot be managed by the VDSM GUI.

Note If you plan to use a RADIUS server or a TACACS+ server for authentication, you must configure the server settings before you configure and submit these settings. See the "Configuring RADIUS Server Settings" section on page 3-13 and the "Configuring TACACS+ Server Settings" section on page 3-14 for more information.

When the primary login server and the primary enable server are set to local, usernames and passwords are local to each device. Local authentication and authorization uses locally configured login and passwords to authenticate login attempts.

Note If the **Enable Failover Server Unreachable** option is enabled, it applies to both the login authorization methods and the exec authentication methods.

If you are going to use different servers for login authentication and enable authentication (for example, local for login authentication and RADIUS for the enable authentication), then the username and password must be the same for both servers.

By default, local login authentication is enabled. You can disable local login authentication only after enabling one or more of the other login authentication servers. However, when local login authentication is disabled, if you disable all other login authentication methods, a warning message is displayed stating "At least one authentication method is required to select for login."

Caution Make sure that RADIUS or TACACS+ authentication is configured and operating correctly before disabling local authentication and authorization. If you disable local authentication and RADIUS or TACACS+ is not configured correctly, or if the RADIUS or TACACS+ server is not online, you may be unable to log in to the device.

To configure the login authentication and enable authentication schemes for the device, do the following:

Step 1 Choose **Devices > Devices > General Settings > Login Access Control > Login Authentication**. The Login Authentication page is displayed.

Step 2 Enter the settings as appropriate. See Table 3-5 for a description of the fields.

Table 3-5 Login Authentication Fields

Field	Description
Login Authentication Settings	
Enable Failover Server Unreachable	If **Enable Failover Server Unreachable** is enabled, the following applies: • Only two login authentication schemes (a primary and secondary scheme) are allowed on the device. • Device fails over from the primary authentication scheme to the secondary authentication scheme only if all specified authentication servers of the primary authentication scheme are unreachable. Conversely, if the **Enable Failover Server Unreachable** option is disabled, the device contacts the secondary authentication database, regardless of the reason the authentication failed with the primary authentication database. **Note** To use this option, you must set TACACS+ or RADIUS as the primary authentication method and local as the secondary authentication method.
Authentication Login Servers	When enabled, login authentication servers are used to authenticate user logins and whether the user has access permissions to the device. Check this option and set one or more Login servers for login authentication. By unchecking this option, local authentication is used by default. Three servers can be configured. **Note** If local is selected for any of the Login servers, the password in the username is used to authenticate the user. See the "Creating, Editing, and Deleting Users—Usernames" section on page 3-12
Primary Login Server	Choose local, RADIUS, or TACACS+.
Secondary Login Server	Choose local, RADIUS, or TACACS+.
Tertiary Login Server	Choose local, RADIUS, or TACACS+.
Enable Authentication Settings	
Primary Enable Server	The enable server is used to allow normal users to enter the privileged EXEC mode.Choose local, RADIUS, or TACACS+.
Secondary Enable Server	Choose local, RADIUS, or TACACS+.
Tertiary Enable Server	Choose local, RADIUS, or TACACS+.
Local Enable Password	Set the local enable password for normal users to log in to the Enable server and have privileged EXEC mode. If multiple authorization methods are configured, the SB tries to authenticate the enable password by way of each configured method until one of them is successful.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Exec Authorization

Exec authorization provides the configuration for determining the services allowed for each user that logs in to the device.

Exec authorization can also be used to determine the services the user has for the VDSM GUI. When logging in to the VDSM GUI with an external user account (RADIUS or TACACS+), the user is authenticated by the external database. After the external user is authenticated, its role depends on the privilege configured in the external database (zero [0] means a normal user and 15 means a super user). The privilege level of 0 or 15 is mapped to the read-only or admin user role in the VDSM GUI. No VDSM local user is created in the VDSM database for the external user that logs in, so the external user cannot be managed by the VDSM GUI.

Note If you plan to use a TACACS+ server for authorization, you must configure the server settings before you configure and submit these settings. See the "Configuring RADIUS Server Settings" section on page 3-13 and the "Configuring TACACS+ Server Settings" section on page 3-14 for more information.

When the primary authorization server is set to local, usernames and passwords are local to each device. Local authorization uses locally configured login and passwords to authorize services for the user.

Note If the **Enable Failover Server Unreachable** option is enabled, it applies to both the login authorization methods and the exec authentication methods.

If you are going to use different servers for login authentication and enable authentication (for example, local for login authentication and RADIUS for the enable authentication), then the username and password must be the same for both servers.

Caution Make sure that RADIUS or TACACS+ authentication is configured and operating correctly before disabling local authentication and authorization. If you disable local authentication and RADIUS or TACACS+ is not configured correctly, or if the RADIUS or TACACS+ server is not online, you may be unable to log in to the device.

To configure the exec authorization schemes for the device, do the following:

Step 1 Choose **Devices > Devices > General Settings > Login Access Control > Exec Authorization**. The Exec Authorization page is displayed.

Step 2 Enter the settings as appropriate. See Table 3-6 for a description of the fields.

Table 3-6 Exec Authorization Fields

Field	Description
Authorization Exec Servers	When enabled, authorization exec servers are used to authorize services for logged in users. Check this option and set one or more servers for exec authorization. By unchecking this option, local authentication is used by default. Three servers can be configured. **Note** If a user encounters failure during EXEC shell) startup authorization, the user fails to log in to the SB even if the user passed the login authentication.
Primary Exec Server	Choose local, RADIUS, or TACACS+.
Secondary Exec Server	Choose local, RADIUS, or TACACS+.
Tertiary Exec Server	Choose local, RADIUS, or TACACS+.
Primary Enable Server	The enable server determines if the normal user can enter the privileged EXEC mode. Choose local, RADIUS, or TACACS+.
Normal User Commands	Choose **Enable** or **Enable if Authenticated**. The **Enable if Authenticated** option turns off authorization on the TACACS+ server and authorization is granted to any Normal user who is authenticated.
Super User Commands	Choose **Enable** or **Enable if Authenticated**. The **Enable if Authenticated** option turns off authorization on the TACACS+ server and authorization is granted to any Super user who is authenticated.
Enable Config Commands	Check the **Enable Config Commands** check box to enable authorization of the configuration mode commands. By default, this option is disabled, which means all configuration commands issued are allowed.
Enable Console Config	Check the **Enable Console Commands** check box to enable authorization of all commands issued on a console TTY connection. By default, this option is disabled, which means commands issued through a console TTY connection always succeed.

Note The following commands bypass authorization and accounting: CTRL+C, CTRL+Z, **exit**, **end**, and all of configuration commands for entering submode (for example, **interface 10 Gigabit Ethernet 1/0**).

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Configuring SSH

Secure Shell (SSH) consists of a server and a client program. Like Telnet, you can use the client program to remotely log in to a machine that is running the SSH server. However, unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

The SSH page allows you to specify the key length and login grace time.

To enable the SSH daemon, do the following:

Step 1 Choose **Devices > Devices > General Settings > Login Access Control > SSH**. The SSH page is displayed.

Step 2 Check **Enable** to enable the SSH feature. SSH enables login access to the device through a secure and encrypted channel.

Step 3 In the **Length of Key** field, specify the number of bits needed to create an SSH key. The default is 2048.

Step 4 In the **Login Grace Time** field, specify the number of seconds the server waits for the user to successfully log in before it ends the connection. The authentication procedure must be completed within this time limit. The default is 300 seconds.

Note When changing the **Login Grace Time**, you need to first uncheck the **Enable** check box and click **Submit**. Enter the new **Login Grace Time**, check **Enable**, and click **Submit**.

Step 5 Select the SSH version.

a. To allow clients to connect using SSH protocol version 1, check the **Enable SSHv1** check box.

b. To allow clients to connect using SSH protocol version 2, check the **Enable SSHv2** check box.

Note You can enable both SSHv1 and SSHv2, or you can enable one version and not the other. You cannot disable both versions of SSH unless you disable the SSH feature by unchecking the **Enable** check box.

Step 6 Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Enabling Telnet

To enable the Telnet service, do the following:

Step 1 Choose **Devices > Devices > General Settings > Login Access Control > Telnet**. The Telnet page is displayed.

Step 2 Check **Telnet Enable** to enable the terminal emulation protocol for remote terminal connections.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Setting the Message of the Day

The Message of the Day (MOTD) feature enables you to provide information bits to the users when they log in to a device. There are three types of messages that you can set up:

- MOTD banner
- EXEC process creation banner
- Login banner

To configure the Message of the Day settings, do the following:

Step 1 Choose **Devices > Devices > General Settings > Login Access Control > Message of the Day**. The MOTD page is displayed.

Step 2 Check **Enable** to enable the MOTD settings. The Message of the Day (MOTD) banner, EXEC process creation banner, and Login banner fields become enabled.

Step 3 In the **Message of the Day (MOTD) Banner** field, enter a string that you want to display as the MOTD banner when a user attempts to log in to the device.

Note In the Message of the Day (MOTD) Banner, EXEC Process Creation Banner, and Login Banner fields, you can enter a maximum of 980 characters. A new line character (or **Enter**) is counted as two characters, as it is interpreted as \n by the system. You cannot use special characters such as `, % ,^ , and " in the MOTD text.

Step 4 In the **EXEC Process Creation Banner** field, enter a string to be displayed as the EXEC process creation banner when a user enters into the EXEC shell of the device.

Step 5 In the **Login Banner** field, enter a string to be displayed after the MOTD banner when a user attempts to log in to the device.

Step 6 Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Changing the CLI Session Time

To change the CLI session time, do the following:

Step 1 Choose **Devices > Devices > General Settings > Login Access Control > CLI Session Time**. The CLI Session Time page is displayed.

Step 2 In the **CLI Session Time** field, enter the time (in minutes) that the device waits for a response before ending the session.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Changing Users—Admin Password

Every device (VDSM, SB) has a built-in user account. The username is *admin* and the default password is *default*. This account allows access to all services and entities in the VDS-SB. Any user that can access the Admin Password page in the VDSM can configure a new password for the administrator user account on individual SBs

To change the Admin password, do the following:

Step 1 Choose **Devices > Devices > General Settings > Login Access Control > Users > Admin Password**. The Admin Password page is displayed.

Step 2 In the **Password** field, enter a new password.

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

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

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Creating, Editing, and Deleting Users—Usernames

You can create, edit, and delete user accounts for login access to individual devices.A privilege profile must be assigned to each new user account. The Usernames page uses privilege profiles to determine which tasks a user can perform and the level of access provided. Users with administrative privileges can add, delete, or modify user accounts through the VDSM or the device CLI.

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

Step 1 Choose **Devices > Devices > General Settings > Login Access Control > Users > Usernames**. The User Table page is displayed.

The table is sortable by clicking the column headings.

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

To edit a local user, click the **Edit** icon next to the name you want to edit.

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

Table 3-7 Local User Fields

Field	Description
Username	Name of user.
Password	User password.

Table 3-7 Local User Fields (continued)

Field	Description
Confirm Password	Re-enter user password.
Privilege	There are two types of predefined privilege profiles: • Normal user—User has read access and can see some of the SB or VDSM settings. • Superuser—User has administrative privileges such as creating new users and modifying the SB or VDSM settings.

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

To delete a user, click the **Edit** icon for the user, then click the **Delete** icon in the task bar.

Authentication

User authentication and authorization (configuration rights) data can be maintained in any combination of these three databases:

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

The Login Authentication page allows you to choose an external access server or the internal (local) device-based authentication, authorization, and accounting (AAA) system for user access management. You can choose one method or a combination of the three methods. The default is to use the local database for authentication.

Configuring RADIUS Server Settings

Note The VDSM does not cache user authentication information. Therefore, the user is reauthenticated against the Remote Authentication Dial In User Service (RADIUS) server for every request. To prevent performance degradation caused by many authentication requests, install the VDSM in the same location as the RADIUS server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To configure the RADIUS server settings, do the following:

Step 1 Choose **Devices > Devices > General Settings > Authentication > RADIUS Server**. The RADIUS Server Settings page is displayed.

Step 2 Enter the settings as appropriate. See Table 3-8 for a description of the fields.

Table 3-8 RADIUS Server Settings Fields

Field	Description
Enable Radius Authentication	Enables RADIUS authentication.
Time to wait	Number of seconds to wait for a response before timing out on a connection to a RADIUS server. The range is from 1 to 20. The default is 5.
Number of retransmits	Number of attempts allowed to connect to a RADIUS server. The default is 2.
Enable redirect	Redirects an authentication response to a different authentication server if an authentication request using the RADIUS server fails.
Redirect Message [1-3]	Message sent to the user if redirection occurs. **Note** If the redirect message has a space, it must be in quotes (" ").
Location [1-3]	Sets an HTML page location. This is the URL destination of the redirect message that is sent when authentication fails.
Shared Encryption Key	Encryption key shared with the RADIUS server. The maximum number of characters allowed is 15.
Server Name [1-5]	IP address or hostname of the RADIUS server.
Server Port [1-5]	Port number on which the RADIUS server is listening. The default is 1645.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

To use RADIUS for login authentication and authorization, see the "Login Authentication" section on page 3-6.

Configuring TACACS+ Server Settings

Note The VDSM does not cache user authentication information. Therefore, the user is reauthenticated against the Terminal Access Controller Access Control System Plus (TACACS+) server for every request. To prevent performance degradation caused by many authentication requests, install the VDSM in the same location as the TACACS+ server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To configure the TACACS+ server settings, do the following:

Step 1 Choose **Devices > Devices > General Settings > Authentication > TACACS+ Server**. The TACACS+ Server Settings page is displayed.

Step 2 Enter the settings as appropriate. See Table 3-9 for a description of the fields.

Table 3-9 TACACS+ Server Settings Fields

Field	Description
Enable TACACS+ Servers	Enables TACACS+ authentication.
Use ASCII Password Authentication	Changes the default password type from Password Authentication Protocol (PAP) to ASCII clear text format.
Time to wait	Number of seconds to wait for a response before timing out on a connection to a TACACS+ server. The range is from 1 to 20. The default is 5.
Number of retransmits	Number of attempts allowed to connect to a TACACS+ server. The default is 2.
Security Word	Encryption key shared with the TACACS+ server. The range is from 1 to 99. An empty string is the default.
Primary Server	IP address or hostname of the primary TACACS+ server.
Secondary Server Tertiary Server	IP address or hostname of the backup TACACS+ server. Up to two backup servers are allowed.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

To use TACACS+ for login authentication and authorization, see the "Login Authentication" section on page 3-6.

Configuring AAA Accounting

Accounting tracks all user actions and when the action occurred. It can be used for an audit trail or for billing for connection time or resources used (bytes transferred).

The VDS-SB accounting feature uses TACACS+ server logging. Accounting information is sent to the TACACS+ server only, not to the console or any other device. The syslog file on the SB logs accounting events locally. The format of events stored in the syslog is different from the format of accounting messages.

The TACACS+ protocol allows effective communication of AAA information between SBs and a central TACACS+ server. It uses TCP for reliable connections between clients and servers. SBs send authentication and authorization requests, as well as accounting information to the TACACS+ server.

Note Before you can configure the AAA accounting settings for a device, you must first configure a TACACS+ server for the device. See the "Configuring TACACS+ Server Settings" section on page 3-14.

Note The VDSM does not cache user authentication information. Therefore, the user is reauthenticated against the Terminal Access Controller Access Control System Plus (TACACS+) server for every request. To prevent performance degradation caused by many authentication requests, install the VDSM in the same location as the TACACS+ server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To configure the AAA accounting settings, do the following:

Step 1 Choose **Devices > Devices > General Settings > Authentication > AAA Accounting**. The AAA Accounting Settings page is displayed.

Step 2 Enter the settings as appropriate. See Table 3-9 for a description of the fields.

Table 3-10 AAA Accounting Settings Fields

Field	Description
System Events	Enables accounting records on the TACACS+ server about system events; such as system reboot, interface up or down states, and accounting configuration enabled or disabled. From the **System Events** drop-down list choose **start-stop** or **stop-only.** The **start-stop** option records events when they start and when they stop. The **stop-only** option records events when they stop.
Exec Shell Events	Enables accounting records on the TACACS+ server about user EXEC terminal sessions, including username, date, and start and stop times. From the **Exec Shell Events** drop-down list choose **start-stop** or **stop-only.** The **start-stop** option records events when they start and when they stop. The **stop-only** option records events when they stop.
Normal User Commands	Enables accounting records on the TACACS+ server for Normal users using commands in the EXEC mode. From the **Normal User Commands** drop-down list choose **start-stop** or **stop-only.** The **start-stop** option records events when they start and when they stop. The **stop-only** option records events when they stop.
Super User Commands	Enables accounting records on the TACACS+ server for Super users using commands in the EXEC mode. From the **Super User Commands** drop-down list choose **start-stop** or **stop-only.** The **start-stop** option records events when they start and when they stop. The **stop-only** option records events when they stop.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Configuring an Access Control List

To configure an access control list (ACL) for group authorization, do the following:

Step 1 Choose **Devices > Devices > General Settings > Authentication > Access Control List > Configure Access Control List**. The Access Control List Table page is displayed.

The table is sortable by clicking the column headings.

Step 2 Click the **Create New** icon in the task bar. The Configure Access Control List page is displayed.

To edit a group, click the **Edit** icon next to the name you want to edit.

Step 3 Enter the settings as appropriate. See Table 3-11 for a description of the fields.

Table 3-11 Access Control List Fields

Field	Description
Action	Whether to permit or deny access for this group.
Group Name	If this action is for all groups, choose **Any Group Name**. If this action is for a specific group, choose **Enter Group Name** and enter the group name in the field.
Change Position	To change the order of this group in the access control list, which is displayed in the Access Control List Table page, click **Change Position**.

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

To delete a group, click the **Edit** icon for the group, then click the **Delete** icon in the task bar.

Step 5 From the left-panel menu, choose **Enable Access Control List**. The Enable Access Control List page is displayed.

Step 6 Check the **Enable Access Control List** check box and click **Submit**.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

To move a group up or down in the Access Control List table, click the Up arrow or Down arrow in the Move column.

The ACL can be applied from the device or from a device group. The source of the currently applied settings is shown in the Access Control List Table page.

Setting Storage Handling

The Storage option offers disk error-handling settings.

Enabling Disk Error Handling

The Disk Error Handling page allows you to configure how disk errors are handled, and to define disk error-handling thresholds for bad sectors and disk errors (I/O errors).

The **Threshold for Bad Sectors** and the **Threshold for Disk Errors** counts only apply to bad sectors and disk errors detected since the last reboot of the device. These counts do not persist across a device reboot (reload).

If the **Enable Disk Error Handling Reload** option is enabled and a SYSTEM disk drive is marked bad because the disk error-handling threshold (bad sectors or disk errors) was reached, the device is automatically reloaded. Following the device reload, the bad sector and disk error threshold counts are reset, and a syslog message and an SNMP trap are generated.

If a critical disk drive is marked bad, the redundancy of the system disks for this device is affected. Critical disks are disks with SYSTEM partitions. However, drives with SYSTEM partitions use RAID1. With the RAID system, if the critical primary disk fails, the other mirrored disk (mirroring only occurs for SYSTEM partitions) seamlessly continues operation. There is a separate alarm for bad RAID. The SMART statistics that are returned by the **show disks SMART-info detail** command include sector errors directly reported by the drive itself.

Note We do not recommend enabling the **Enable Disk Error Handling Reload** option, because the software state may be lost when the device is reloaded.

To configure a disk error-handling method, do the following:

Step 1 Choose **Devices > Devices > General Settings > Storage > Disk Error Handling**. The Disk Error Handling Settings page is displayed.

Step 2 Check the **Enable** check box.

Step 3 Check the **Enable Disk Error Handling Reload** check box if you want the device to reload when a critical disk (SYSTEM) has problems.

Step 4 Check the **Enable Disk Error Handling Threshold** check box if you want to set the number of disk errors allowed before the disk is marked bad, and enter the following:

a. In the **Threshold for Bad Sectors** field, enter the number of allowed bad sectors before marking the disk bad. This threshold only applies to bad sectors detected since the last reboot of the device. The range is 0 to 100. The default threshold is 30

b. In the **Threshold for Disk Errors** field, enter the number of allowed disk errors (I/O errors) before marking the disk bad. This threshold only applies to disk and sector errors detected since the last reboot of the device. The range is from 0 to 100,000. The default is 500.

Note When both **Threshold for Bad Sectors** and **Threshold for Disk Errors** are set to 0, it means never mark the disk bad when it detects bad sectors or disk errors, and the disk_failure alarm is not raised. A disk with SYSTEM partitions uses RAID1. There is a separate alarm for bad RAID.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

When a sector I/O error is detected, a "badsector" alarm is raised against the corresponding disk, which occurs during the lifetime of a disk. A "badsector" alarm is raised when the number of bad sectors for a specific disk exceeds the "badsector" alarm threshold. The default threshold for bad sector alarms is set to 15 errored sectors. See the *Cisco VDS Service Broker 1.0.1 Command Reference* for information on setting the threshold for bad sector alarms and remapped sector alarms, by using the following commands:

```
(config)# disk error-handling threshold alarm-bad-sectors <threshValue>
(config)# disk error-handling threshold alarm-remapped-sectors <threshValue>
(config)# disk error-handling bad-sectors-mon-period <minutes>
```

The **Disk Failure Percentage Threshold** field on the Service Monitor page sets the overall percentage of CDNFS disk failures. When the percentage of failed disks (default is 75) exceeds this threshold, no further requests are sent to this device. The **Disk Failure Threshold** setting is only for the CDNFS disks. For more information, see the "Setting Service Monitor Thresholds" section on page 3-38.

Network Settings

The Network pages provide settings for network connectivity. Configuring network settings consist of the following procedures:

- Enabling FTP Services
- Enabling DNS
- Enabling RCP
- Configuring NTP
- Setting the Time Zone
- Viewing Network Interfaces
- Configuring External IP Addresses
- Configuring Port Channel and Load Balancing Settings
- Configuring IP General Settings
- Configuring IP ACL for IPv4
- Configuring Static IPv4 Routes
- Configuring DSR VIP

Enabling FTP Services

To enable FTP services to listen for connection requests, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > FTP**. The FTP Settings page is displayed.

Step 2 Check the **Enable FTP Services** check box.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Enabling DNS

DNS Settings are required on all SBs, and VDSMs. The SBs need to be able to resolve the BFQDNS, and be able to communicate with the DNS servers, and the VDSMs need to resolve host names.

To configure Domain Name System (DNS) servers, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > DNS**. The DNS Settings page is displayed.

Step 2 Enter the settings as appropriate. See Table 3-12 for a description of the fields.

Table 3-12 DNS Settings Fields

Field	Description
Enable	Enables Domain Name System (DNS) on the device.
List of DNS Servers	Space-delimited list of IP addresses for up to eight name servers for name and address resolution.
Domain Names	A space-delimited list of up to three default domain names. A default domain name allows the system to resolve any unqualified hostnames. Any IP hostname that does not contain a domain name will have the configured domain name appended to it. This appended name is resolved by the DNS server and then added to the host table. A DNS server must be configured on the system for hostname resolution to work correctly. To do this, use the List of DNS Servers field.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Enabling RCP

Remote Copy Protocol (RCP) lets you download, upload, and copy configuration files between remote hosts and a switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection oriented. This service listens for requests on TCP port 514.

To enable RCP services, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > RCP**. The RCP page is displayed.

Step 2 Check the **RCP Enable** check box to have the RCP services listen for RCP requests.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Configuring NTP

To configure the device to synchronize its clock with an NTP server, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > NTP**. The NTP page is displayed.

Step 2 Check **Enable** to enable NTP.

Step 3 In the **NTP Server** field, enter the IP address or hostname of up to four NTP servers. Use a space to separate the entries.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Setting the Time Zone

If you have an outside source on your network that provides time services, such as an NTP server, you do not need to set the system clock manually. When manually setting the clock, enter the local time. The device calculates Coordinated Universal Time (UTC) based on the time zone set.

Note Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at startup to initialize the software clock.

Caution We highly recommend that you use NTP servers to synchronize the devices in your VDS-SB network. If you change the local time on the device, you must change the BIOS clock time as well; otherwise, the timestamps on the error logs are not synchronized. Changing the BIOS clock is required because the kernel does not handle time zones.

To manually configure the time zone, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > Time Zone**. The Time Zone page is displayed with the default settings of UTC (offset = 0) and no daylight savings time configured.

Step 2 To configure a standard time zone, do the following:

a. Click the **Standard Time Zone** radio button.

The standard convention for time zones uses a *Location/Area* format in which *Location* is a continent or a geographic region of the world and *Area* is a time zone region within that location. For a list of standard time zones that can be configured and their UTC offsets, see Table 3-13 on page 3-23.

b. From the **Standard Time Zone** drop-down list, choose a location for the time zone. The page refreshes, displaying all area time zones for the chosen location in the second drop-down list.

c. Choose an area for the time zone.

The UTC offset (hours and minutes ahead or behind UTC) for the corresponding time zone is displayed. During summer time savings, the offset may differ and is displayed accordingly.

Note Some of the standard time zones (mostly time zones within the United States) have daylight savings time zones configured automatically.

Step 3 To configure a customized time zone, do the following:

a. Click the **Customized Time Zone** radio button.

b. In the **Customized Time Zone** field, enter a name to for the time zone. The time zone entry is case sensitive and can contain up to 40 characters. Spaces are not allowed. If you specify any of the standard time zone names, an error message is displayed when you click **Submit**.

c. For UTC offset, choose **+** or **–** from the **UTC Offset** drop-down list to indicate whether the configured time zone is ahead or behind UTC. Also, choose the number of hours (0 to 23) and minutes (0 to 59) offset from UTC for the customized time zone. The range for the UTC offset is from –23:59 to 23:59, and the default is 0:0.

Step 4 To configure customized summer time savings, do the following:

Note Customized summer time can be specified for both standard and customized time zones.

The start and end dates for summer time can be configured in two ways: absolute dates or recurring dates. Absolute dates apply once and must be reset every year. Recurring dates apply every year.

a. Click the **Absolute Dates** radio button to configure summer settings once.

b. In the **Start Date** and **End Date** fields, specify the month, day, and year that the summer time savings starts and ends in mm/dd/yyyy format.

Alternatively, click the **Calendar** icon and select a date. The chosen date is highlighted in blue. Click **Apply**.

c. Click the **Recurring Dates** radio button to configure a recurring summer setting.

d. Using the drop-down lists, choose the start day, week, and month when the summer time savings starts. For example, if the summer time savings begins the first Sunday in March, you would select Sunday, 1st, March from the drop-down lists.

e. Using the drop-down lists, choose the start day, week, and month when the summer time savings ends.

Step 5 Using the **Start Time** drop-down lists and the **End Time** drop-down lists, choose the hour (0 to 23) and minute (0 to 59) at which daylight savings time starts and ends.

Start Time and End Time fields for summer time are the times of the day when the clock is changed to reflect summer time. By default, both start and end times are set at 00:00.

Step 6 In the Offset field, specify the minutes offset from UTC (0 to 1439). (See Table 3-13 on page 3-23.)

The summer time offset specifies the number of minutes that the system clock moves forward at the specified start time and backward at the end time.

Step 7 To not specify a summer or daylight savings time for the corresponding time zone, click the **No Customized Summer Time Configured** radio button.

Step 8 Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Table 3-13 lists the UTC offsets for the different locations around the world.

Table 3-13 Time Zone—Offset from UTC

Time Zone	Offset from UTC (in hours)	Time Zone	Offset from UTC (in hours)
Africa/Algiers	+1	Asia/Vladivostok	+10
Africa/Cairo	+2	Asia/Yekaterinburg	+5
Africa/Casablanca	0	Asia/Yakutsk	+9
Africa/Harare	+2	Australia/Adelaide	+9.30
Africa/Johannesburg	+2	Australia/Brisbane	+10
Africa/Nairobi	+3	Australia/Darwin	+9.30
America/Buenos_Aires	–3	Australia/Hobart	+10
America/Caracas	–4	Australia/Perth	+8
America/Mexico_City	–6	Australia/Sydney	+10
America/Lima	–5	Canada/Atlantic	–4
America/Santiago	–4	Canada/Newfoundland	–3.30
Atlantic/Azores	–1	Canada/Saskatchewan	–6
Atlantic/Cape_Verde	–1	Europe/Athens	+2
Asia/Almaty	+6	Europe/Berlin	+1
Asia/Baghdad	+3	Europe/Bucharest	+2
Asia/Baku	+4	Europe/Helsinki	+2
Asia/Bangkok	+7	Europe/London	0
Asia/Colombo	+6	Europe/Moscow	+3
Asia/Dacca	+6	Europe/Paris	+1
Asia/Hong_Kong	+8	Europe/Prague	+1
Asia/Irkutsk	+8	Europe/Warsaw	+1

Table 3-13 Time Zone—Offset from UTC (continued)

Time Zone	Offset from UTC (in hours)	Time Zone	Offset from UTC (in hours)
Asia/Jerusalem	+2	Japan	+9
Asia/Kabul	+4.30	Pacific/Auckland	+12
Asia/Karachi	+5	Pacific/Fiji	+12
Asia/Katmandu	+5.45	Pacific/Guam	+10
Asia/Krasnoyarsk	+7	Pacific/Kwajalein	–12
Asia/Magadan	+11	Pacific/Samoa	–11
Asia/Muscat	+4	US/Alaska	–9
Asia/New Delhi	+5.30	US/Central	–6
Asia/Rangoon	+6.30	US/Eastern	–5
Asia/Riyadh	+3	US/East–Indiana	–5
Asia/Seoul	+9	US/Hawaii	–10
Asia/Singapore	+8	US/Mountain	–7
Asia/Taipei	+8	US/Pacific	–8
Asia/Tehran	+3.30		

The offset time (number of hours ahead or behind UTC) as displayed in the table is in effect during winter time. During summer time or daylight savings time, the offset may be different from the values in the table and is calculated and displayed accordingly by the system clock.

Viewing Network Interfaces

The Network Interfaces page is informational only. To view this information, choose **Devices > Devices > General Settings > Network > Network Interfaces**. Information about the network interfaces configured for the device is displayed.

Configuring External IP Addresses

The External IP page allows you to configure up to eight Network Address Translation (NAT) IP addresses. This allows a router to translate up to eight internal addresses to registered unique addresses and translate external registered addresses to addresses that are unique to the private network.

To configure NAT IP addresses, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > External IP**. The External IP Settings page is displayed.

Step 2 Check the **Enable** check box.

Step 3 In the External IP Address fields (1–8), enter up to eight IP addresses.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Configuring Port Channel and Load Balancing Settings

To configure load balancing on port channels, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > Port Channel Settings**. The Port Channel Settings page is displayed.

Step 2 From the **Load Balancing Method** drop-down list, choose one of the following load balancing methods:

- **dst-ip**—Destination IP address
- **dst-mac**—Destination MAC address
- **dst-mixed-ip-port**—Destination IP address and TCP/UDP port
- **dst-port**—Destination port
- **round robin**—Each interface in the channel group
- **src-dst-ip**—Source and destination IP address
- **src-dst-mac**—Source and destination MAC address
- **src-dst-mixed-ip-port**—Source destination IP address and source destination port
- **src-dst-port**—Source and destination port
- **src-mixed-ip-port**—Source IP address and source destination port
- **src-port**—Source port

Round robin allows traffic to be distributed evenly among all interfaces in the channel group. The other balancing options give you the flexibility to choose specific interfaces (by IP address, MAC address, port) when sending an Ethernet frame.

The source and destination options mean that while calculating the outgoing interface, take into account both the source and destination (MAC address or port).

Note Round-robin load-balancing mode is not supported when Link Aggregation Control Protocol (LACP) is enabled on the port channel.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Configuring IP General Settings

The Path Maximum Transmission Unit (MTU) Discovery discovers the largest IP packet size allowable between the various links along the forwarding path and automatically sets the correct value for the packet size. By using the largest MTU the links can support, the sending device can minimize the number of packets it must send.

Note The Path MTU Discovery is a process initiated by the sending device. If a server does not support IP Path MTU Discovery, the receiving device has no mechanism available to avoid fragmenting datagrams generated by the server.

To enable Path MTU Discovery, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > IP General Settings**. The IP General Settings page is displayed.

Step 2 Check **Enable Path MTU Discovery**.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Configuring IP ACL for IPv4

Access control lists (ACLs) provide a means to filter packets by allowing a user to permit or deny IP packets from crossing specified interfaces. Packet filtering helps to control packet movement through the network. Such control can help limit network traffic and restrict network use by certain users or devices.

You can also apply ACLs to management services such as SNMP, SSH, HTTPS, Telnet, and FTP. ACLs can be used to control the traffic that these applications provide by restricting the type of traffic that the applications handle.

In a managed VDS-SB network environment, administrators need to be able to prevent unauthorized access to various devices and services. VDS-SB supports standard and extended ACLs that allow administrators to restrict access to or through a VDS-SB network device, such as the SB. Administrators can use ACLs to reduce the infiltration of hackers, worms, and viruses that can harm the network.

ACLs provide controls that allow various services to be tied to a particular interface. For example, the administrator can use IP ACLs to define a public interface on the Service Broker for content serving and a private interface for management services (for example, Telnet, SSH, SNMP, HTTPS, and software upgrades). A device attempting to access one of the services must be on a list of trusted devices before it is allowed access. The implementation of ACLs for incoming traffic on certain ports for a particular protocol type is similar to the ACL support for the Cisco Global Site Selector and Cisco routers.

To use ACLs, the system administrator must first configure ACLs and then apply them to specific services. The following are some examples of how IP ACLs can be used in various enterprise deployments:

- Application layer proxy firewall with a hardened outside interface has no ports exposed. (*Hardened* means that the interface carefully restricts which ports are available for access primarily for security reasons. Because the interface is outside, many types of attacks are possible.) The device's outside address is globally accessible from the Internet, while its inside address is private. The inside interface has an ACL to limit Telnet, SSH, and VDSM traffic.
- Device is deployed anywhere within the enterprise. Like routers and switches, the administrator wants to limit Telnet, SSH, and VDSM access to the IT source subnets.
- Device is deployed as a reverse proxy in an untrusted environment, and the administrator wishes to allow only port 80 inbound traffic on the outside interface and outbound connections on the back-end interface.

Note IP ACLs are defined for individual devices only.

When you create an IP ACL, you should note the following constraints:

- IP ACL names must be unique within the device.
- IP ACL names must be limited to 30 characters and contain no spaces or special characters.
- VDSM can manage up to 50 IP ACLs and a total of 500 conditions per device.
- When the IP ACL name is numeric, numbers 1 through 99 denote standard IP ACLs and numbers 100 through 199 denote extended IP ACLs. IP ACL names that begin with a number cannot contain nonnumeric characters.
- Extended IP ACLs cannot be used with SNMP applications.

Creating a New IP ACL

To create a new IP ACL, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > IP ACL** for IPv4 addressing. The IP ACL Table page is displayed.

The table is sortable by clicking the column headings.

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

To edit an ACL, click the **Edit** icon next to the name you want to edit.

Step 3 In the **Name** field, enter a name, observing the naming rules for IP ACLs.

Step 4 From the **ACL Type** drop-down list, choose an IP ACL type (**Standard** or **Extended**). The default is **Standard**.

Step 5 Click **Submit**. The page refreshes and the Modifying IP ACL page for a newly created IP ACL is displayed.

Note Clicking **Submit** at this point merely saves the IP ACL; IP ACLs without any conditions defined do not appear on the individual devices.

Adding Conditions to an IP ACL

To add conditions to an IP ACL, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > IP ACL** for IPv4 addressing. C The IP ACL Table page is displayed.

Step 2 Click the **Edit** icon next to the name of the IP ACL you want to add a condition to. The Modifying IP ACL page is displayed.

Step 3 Click the **Create New** icon in the task bar. The Condition page is displayed.

To edit a condition, click the **Edit** icon next to the name you want to edit.

Note The number of available fields for creating IP ACL conditions depends on the whether the IP ACL type is standard or extended.

Step 4 Enter values for the properties that are enabled for the type of IP ACL that you are creating.

- To create a standard IP ACL, go to Step 5.
- To create an extended IP ACL, go to Step 6.

Step 5 To set up conditions for a standard IP ACL, do the following:

a. From the **Purpose** drop-down list, choose a purpose (**Permit** or **Deny**).

b. In the **Source IP** field, enter the source IP address.

c. In the **Source IP Wildcard** field, enter a source IP wildcard address.

d. Click **Submit**. The Modifying IP ACL page is displayed showing the new condition and its configuration.

e. To add another condition to the IP ACL, repeat the steps.

f. To reorder your list of conditions in the Modifying IP ACL page, use the Up arrow or Down arrow in the **Order** column, or click a column heading to sort by any configured parameter.

Note The order of the conditions listed becomes the order in which IP ACLs are applied to the device.

g. When you have finished adding conditions to the IP ACL, and you are satisfied with all your entries and the order in which the conditions are listed, click **Submit** in the Modifying IP ACL page to commit the IP ACL to the device database.

A green "Change submitted" indicator appears in the lower right corner of the Modifying IP ACL page to indicate that the IP ACL is being submitted to the device database.

Table 3-14 describes the fields in a standard IP ACL.

Table 3-14 Standard IP ACL Conditions

Field	Default Value	Description
Purpose[1]	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Source IP[1]	0.0.0.0	IP address of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format. for IPv4.
Source IP[1] Wildcard Source Prefix	255.255.255.255 0	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.

1. Required field.

Step 6 To set up conditions for an extended IP ACL, do the following:

a. From the **Purpose** drop-down list, choose a purpose (**Permit** or **Deny**).

b. From the **Extended Type** drop-down list, choose **Generic**, **TCP**, **UDP**, or **ICMP**.

After you choose a type of extended IP ACL, various options become available depending on what type you choose.

c. Enter the settings as appropriate. See Table 3-15 for descriptions of the extended IP ACL fields.

d. Click **Submit**. The Modifying IP ACL page is displayed showing the new condition and its configuration.

e. To add another condition to the IP ACL, repeat the steps.

f. To reorder your list of conditions from the Modifying IP ACL page, use the Up arrow or Down arrow in the **Order** column, or click a column heading to sort by any configured parameter.

Note The order of the conditions listed becomes the order in which IP ACLs are applied to the device.

g. When you have finished adding conditions to the IP ACL, and you are satisfied with all your entries and the order in which the conditions are listed, click **Submit** in the Modifying IP ACL page to commit the IP ACL to the device database.

A green "Change submitted" indicator appears in the lower-left corner of the Modifying IP ACL page to indicate that the IP ACL is being submitted to the device database.

Table 3-15 Extended IP ACL Conditions

Field	Default Value	Description	Extended Type
Purpose[1]	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).	Generic, TCP, UDP, ICMP
Protocol	ip	Internet protocol (**gre**, **icmp**, **ip**, **tcp**, or **udp**). To match any Internet protocol, use the **ip** keyword.	Generic
Established	Unchecked (false)	When checked, a match with the ACL condition occurs if the TCP datagram has the ACK or RST bits set, indicating an established connection. Initial TCP datagrams used to form a connection are not matched.	TCP
Source IP[1]	0.0.0.0	IP address of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4.	Generic, TCP, UDP, ICMP
Source IP Wildcard[1] Source Prefix	255.255.255.255 0	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.	Generic, TCP, UDP, ICMP

Table 3-15 Extended IP ACL Conditions (continued)

Field	Default Value	Description	Extended Type
Source Port 1	0	Decimal number or name of a port. Valid port numbers are 0 to 65535. See Table 3-16 and Table 3-17 for port name descriptions and associated port numbers. Valid TCP port names are as follows: • domain • exec • ftp • ftp-data • https • nfs • rtsp • ssh • telnet • www Valid UDP port names are as follows: • bootpc • bootps • domain • netbios-dgm • netbios-ns • netbios-ss • nfs • ntp • snmp • snmptrap	TCP, UDP
Source Operator	range	Specifies how to compare the source ports against incoming packets. Choices are **<**, **>**, **==**, **!=**, or **range**.	TCP, UDP
Source Port 2	65535	Decimal number or name of a port. See Source Port 1.	TCP, UDP
Destination IP	0.0.0.0	IP address of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4.	Generic, TCP, UDP, ICMP
Destination IP Wildcard Destination Prefix	255.255.255.255 0	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format for IPv4. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.	Generic, TCP, UDP, ICMP

Table 3-15 Extended IP ACL Conditions (continued)

Field	Default Value	Description	Extended Type
Destination Port 1	0	Decimal number or name of a port. Valid port numbers are 0 to 65535. See Table 3-16 and Table 3-17 for port name descriptions and associated port numbers. Valid TCP port names are as follows: • domain • exec • ftp • ftp-data • https • nfs • rtsp • ssh • telnet • www Valid UDP port names are as follows: • bootpc • bootps • domain • netbios-dgm • netbios-ns • netbios-ss • nfs • ntp • snmp • snmptrap	TCP, UDP
Destination Operator	range	Specifies how to compare the destination ports against incoming packets. Choices are **<**, **>**, **==**, **!=**, or **range**.	TCP, UDP
Destination Port 2	65535	Decimal number or name of a port. See Destination Port 1.	TCP, UDP
ICMP Param Type[1] ICMPv6 Param Type	None	Choices are **None**, **Type/Code**, or **Msg**. • **None**—Disables the ICMP Type, Code, and Message fields. • **Type/Code**—Allows ICMP messages to be filtered by ICMP message type and code. Also enables the ability to set an ICMP message code number. • **Msg**—Allows a combination of type and code to be specified using a keyword. Activates the ICMP Message drop-down list. Disables the ICMP Type field.	ICMP
ICMP Message[1] ICMPv6 Message	administratively-prohibited	Allows a combination of ICMP type and code to be specified using a keyword chosen from the drop-down list. See Table 3-18 for descriptions of the ICMP messages.	ICMP
ICMP Type[1] ICMPv6 Type	0	Number from 0 to 255. This field is enabled when you choose **Type/Code**.	ICMP
Use ICMP Code[1] Use ICMPv6 Code	Unchecked	When checked, enables the ICMP Code field.	ICMP
ICMP Code[1] ICMPv6 Code	0	Number from 0 to 255. Message code option that allows ICMP messages of a particular type to be further filtered by an ICMP message code.	ICMP

1. Required field.

Table 3-16 lists the UDP keywords that you can use with extended access control lists.

Table 3-16 UDP Keywords and Port Numbers

Port Name	Description	UDP Port Number
bootpc	Bootstrap Protocol (BOOTP) client service	68
bootps	Bootstrap Protocol (BOOTP) server service	67
domain	Domain Name System (DNS) service	53
netbios-dgm	NetBIOS datagram service	138
netbios-ns	NetBIOS name resolution service	137
netbios-ss	NetBIOS session service	139
nfs	Network File System service	2049
ntp	Network Time Protocol settings	123
snmp	Simple Network Management Protocol service	161
snmptrap	SNMP traps	162

Table 3-17 lists the TCP keywords that you can use with extended access control lists.

Table 3-17 TCP Keywords and Port Numbers

Port Name	Description	TCP Port Number
domain	Domain Name System service	53
exec	Remote process execution	512
ftp	File Transfer Protocol service	21
ftp-data	FTP data connections (used infrequently)	20
https	Secure HTTP service	443
nfs	Network File System service applications	2049
rtsp	Real-Time Streaming Protocol applications	554
ssh	Secure Shell login	22
telnet	Remote login using Telnet	23
www	World Wide Web (HTTP) service	80

Table 3-18 lists the keywords that you can use to match specific ICMP message types and codes.

Table 3-18 Keywords for ICMP Message Type and Code

Message	Description
administratively-prohibited	Messages that are administratively prohibited from being allowed access.
alternate-address	Messages that specify alternate IP addresses.
conversion-error	Messages that denote a datagram conversion error.
dod-host-prohibited	Messages that signify a Department of Defense (DoD) protocol Internet host denial.

Table 3-18 Keywords for ICMP Message Type and Code (continued)

Message	Description
dod-net-prohibited	Messages that specify a DoD protocol network denial.
echo	Messages that are used to send echo packets to test basic network connectivity.
echo-reply	Messages that are used to send echo reply packets.
general-parameter-problem	Messages that report general parameter problems.
host-isolated	Messages that indicate that the host is isolated.
host-precedence-unreachable	Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable). This is the most common response. Large numbers of this datagram type on the network are indicative of network difficulties or may be indicative of hostile actions.
host-redirect	Messages that specify redirection to a host.
host-tos-redirect	Messages that specify redirection to a host for type of service-based (ToS) routing.
host-tos-unreachable	Messages that denote that the host is unreachable for ToS-based routing.
host-unknown	Messages that specify that the host or source is unknown.
host-unreachable	Messages that specify that the host is unreachable.
information-reply	Messages that contain domain name replies.
information-request	Messages that contain domain name requests.
mask-reply	Messages that contain subnet mask replies.
mask-request	Messages that contain subnet mask requests.
mobile-redirect	Messages that specify redirection to a mobile host.
net-redirect	Messages that are used for redirection to a different network.
net-tos-redirect	Messages that are used for redirection to a different network for ToS-based routing.
net-tos-unreachable	Messages that specify that the network is unreachable for the ToS-based routing.
net-unreachable	Messages that specify that the network is unreachable.
network-unknown	Messages that denote that the network is unknown.
no-room-for-option	Messages that specify the requirement of a parameter, but that no room is available for it.
option-missing	Messages that specify the requirement of a parameter, but that parameter is not available.
packet-too-big	Messages that specify that the ICMP packet requires fragmentation but the Do Not Fragment (DF) bit is set.
parameter-problem	Messages that signify parameter-related problems.
port-unreachable	Messages that specify that the port is unreachable.
precedence-unreachable	Messages that specify that host precedence is not available.

Table 3-18 Keywords for ICMP Message Type and Code (continued)

Message	Description
protocol-unreachable	Messages that specify that the protocol is unreachable.
reassembly-timeout	Messages that specify a timeout during reassembling of packets.
redirect	Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect). ICMP redirect messages are used by routers to notify the hosts on the data link that a better route is available for a particular destination.
router-advertisement	Messages that contain ICMP router discovery messages called router advertisements.
router-solicitation	Messages that are multicast to ask for immediate updates on neighboring router interface states.
source-quench	Messages that have been received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench). This datagram may be used in network management to provide congestion control. A source quench packet is issued when a router is beginning to lose packets due to the transmission rate of a source. The source quench is a request to the source to reduce the rate of a datagram transmission.
source-route-failed	Messages that specify the failure of a source route.
time-exceeded	Messages that specify information about all instances when specified times were exceeded.
timestamp-reply	Messages that contain timestamp replies.
timestamp-request	Messages that contain timestamp requests.
traceroute	Messages that specify the entire route to a network host from the source.
ttl-exceeded	Messages that specify that ICMP packets have exceeded the time-to-live configuration.
unreachable	Messages that are sent when packets are denied by an access control list; these packets are not dropped in the hardware but generate the ICMP-unreachable message.

Applying an IP ACL to an Interface

The IP ACLs can be applied to a particular interface (such as management services to a private IP address) so that the device can have one interface in a public IP address space that serves content and another interface in a private IP address space that the administrator uses for management purposes. This feature ensures that clients can access the Service Broker only in the public IP address space for serving content and not access it for management purposes. A device attempting to access one of these applications that is associated with an IP ACL must be on the list of trusted devices to be allowed access.

To apply an IP ACL to an interface from the CLI, use the following interface configuration command:

interface {**10 Gigabit Ethernet** | **Portchannel** | **Standby** | **10 Gigabit Ethernet**} *slot/port* [**ip**] **access-group** {*accesslistnumber* | *accesslistname*} {**in** | **out**}

Deleting an IP ACL

You can delete an IP ACL, including all conditions and associations with network interfaces, or you can delete only the IP ACL conditions. Deleting all conditions allows you to change the IP ACL type if you choose to do so. The IP ACL entry continues to appear in the IP ACL listing; however, it is in effect nonexistent.

To delete an IP ACL, do the following:

Step 1 Choose **Devices > Devices**. > **General Settings > Network > IP ACL** for IPv4 addressing. The IP ACL Table page is displayed.

Step 2 Click the **Edit** icon next to the name of the IP ACL that you want to delete. The Modifying IP ACL page is displayed. If you created conditions for the IP ACL, you have three options for deletion:

- **Delete ACL**—This option removes the IP ACL, including all conditions and associations with network interfaces and applications.
- **Delete All Conditions**—This option removes all the conditions, while preserving the IP ACL name.
- **Delete IP ACL Condition**—This option removes one condition from the ACL.

Step 3 To delete the entire IP ACL, click **Delete ACL** in the task bar. You are prompted to confirm your action. Click **OK**. The record is deleted.

Step 4 To delete only the conditions, click **Delete All Conditions** in the task bar. You are prompted to confirm your action. Click **OK**. The window refreshes, conditions are deleted, and the ACL Type field becomes available.

Step 5 To delete one condition, do the following:

a. Click the **Edit** icon next to the condition. The condition settings are displayed.

b. Click the **Delete IP ACL Condition** icon in the task bar. The IP ACL table is displayed.

c. Click **Submit** to save the IP ACL table to the database.

Configuring Static IPv4 Routes

The Static IP Routes page allows you to configure a static IPv4 route for a network or host. Any IP packet designated for the specified destination uses the configured route.

To configure a static IP route, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > Static IP Routes**. The IP Route Table page is displayed.

The table is sortable by clicking the column headings.

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

To edit a static route, click the **Edit** icon next to the name you want to edit.

Step 3 In the **Destination Network Address** field, enter the destination network IP address.

Step 4 In the **Netmask** field, enter the destination host netmask.

Step 5 In the **Gateway's IP Address** field, enter the IP address of the gateway interface.

Step 6 Click **Submit** to save the settings.

To delete a route, click the **Edit** icon for the route, then click the **Delete** icon in the task bar.

Configuring DSR VIP

The VDS-SB supports Virtual IP (VIP) configuration for Direct Server Return (DSR) when working with networks that use load balancers. DSR bypasses the load balancer for all server responses to client requests by using MAC Address Translation (MAT).

The VDS-SB allows for the configuration of up to four VIPs (on loopback interfaces).

Client requests are sent to the load balancer and the load balancer sends the requests on to the Service Broker. If DSR VIP is configured on the VDS-SB (and supported on the load balancer), all VDS-SB responses to the client are sent directly to the client, bypassing the load balancer.

To configure a DSR VIP, do the following:

Step 1 Choose **Devices > Devices > General Settings > Network > DSR VIP**. The DSR VIP page is displayed.

Step 2 In the **Direct Server Return VIP 1** field, enter the IPv4 and IPv6 address of the Direct Server Return VIP.

Step 3 Enter any additional DSR VIPs in the remaining fields (Direct Server Return VIP 2 to 4).

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Configuring Notification and Tracking

The Notification and Tracking pages provide settings for alarms, thresholds, SNMP connectivity, and device monitoring. Configuring notification and tracking consists of the following procedures:

- Enabling Alarm Overload Detection
- Setting Service Monitor Thresholds
- Configuring SNMP
- Enabling System Logs
- Configuring Transaction Logs for the Service Broker

Alarm Settings

The Alarm Settings page covers the following configuration settings;

- Enabling Alarm Overload Detection
- Alarms for Admin Shutdown Interface

Enabling Alarm Overload Detection

The device tracks the rate of incoming alarms from the Node Health Manager. If the rate of incoming alarms exceeds the high-water mark (HWM) threshold, the device enters an alarm overload state. This condition occurs when multiple applications raise alarms at the same time. When a device is in an alarm overload state, the following events occur:

- Traps for the raise alarm-overload alarm and clear alarm-overload alarm are sent. SNMP traps for subsequent alarm raise-and-clear operations are suspended.
- Traps for alarm operations that occur between the raise-alarm-overload alarm and the clear-alarm-overload alarm operations are suspended, but individual device alarm information is still collected and available using the CLI.
- Device remains in an alarm overload state until the rate of incoming alarms decreases to less than the low-water mark (LWM).
- If the incoming alarm rate falls below the LWM, the device comes out of the alarm overload state and begins to report the alarm counts to the SNMP servers and the VDSM.

Alarms that have been raised on a device can be listed by using the CLI commands shown in Table 3-19. These CLI commands allow you to systematically drill down to the source of an alarm.

Table 3-19 Viewing Device Alarms

Command	Syntax	Description
show alarms		Displays a list of all currently raised alarms (critical, major, and minor alarms) on the device.
	show alarms critical	Displays a list of only currently raised critical alarms on the device.
	show alarms major	Displays a list of only currently raised major alarms on the device.
	show alarms minor	Displays a list of only currently raised minor alarms on the device.
	show alarms detail	Displays detailed information about the currently raised alarms.
	show alarms history	Displays a history of alarms that have been raised and cleared on the device. The CLI retains the last 100 alarm raise and clear events only.
	show alarms status	Displays the counts for the currently raised alarms on the device. Also lists the alarm-overload state and the alarm-overload settings.

To configure the alarm overload detection, do the following:

Step 1 Choose **Devices > Devices > General Settings > Notification and Tracking > Alarm Settings**. The Alarm Settings page is displayed.

Step 2 Uncheck the **Enable Alarm Overload Detection** check box if you do not want to configure the device to suspend alarm raise and clear operations when multiple applications report error conditions. Alarm overload detection is enabled by default.

Step 3 In the **Alarm Overload Low Water Mark** field, enter the number of alarms per second for the clear alarm overload threshold. The low water mark is the level to which the number of alarms must drop below before alarm traps can be sent. The default value is 1.

Step 4 In the **Alarm Overload High Water Mark** field, enter the number of alarms per second for the raise alarm-overload threshold. The high-water mark is the level the number of alarms must exceed before alarms are suspended. The default value is 10.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Alarms for Admin Shutdown Interface

When the **Alarms for Admin Shutdown Interface** check box is checked, the interface alarm is shutdown. If there is already an alarm raised when the setting is submitted, unchecking the option and submitting the change does not clear the outstanding alarm. There are two ways to avoid this situation:

1. Clear the outstanding alarm first before disabling this option.
2. Disable this option and reboot. The alarm is cleared during reboot.

Note The **Alarms for Admin Shutdown Interface** option should be enabled before any of the above for the alarm to take affect.

To enable the **Alarms for Admin Shutdown Interface** option, do the following:

Step 1 Choose **Devices > Devices > General Settings > Notification and Tracking > Alarm Settings**. The Alarm Settings page is displayed.

Step 2 Check the **Alarms for Admin Shutdown Interface** check box to enable this option.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Setting Service Monitor Thresholds

The Service Monitor page is where you configure workload thresholds for the device.

To configure workload thresholds, do the following:

Step 1 Choose **Devices > Devices > General Settings > Notification and Tracking > Service Monitor**. The Service Monitor page is displayed.

Step 2 Enter the settings as appropriate. See Table 3-20 for a description of the fields.

Table 3-20 Service Monitor Fields

Field	Description
CPU Settings	
Enable	Allows the SB to collect CPU load information from the device.
Threshold	Value (as a percentage) that determines when the device is overloaded. The threshold determines the extent of CPU usage allowed. The range is from 1 to 100. The default is 80.

Table 3-20 Service Monitor Fields (continued)

Field	Description
Sample Period	Time interval (in seconds) between two consecutive samples. The sample period is the time during which the device and the SB exchange keep-alive messages that contain the device load information. The range is from 1 to 60. The default is 1.
Number of Samples	Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.
Disk Settings	
Enable	Allows the SB to collect disk transaction information from the device.
Threshold	The threshold, as a percentage, determines the extent of disk I/O load allowed. The disk threshold is a disk I/O load threshold setting. It is not used to monitor disk usage, it is calculated using the kernel's diskstats status. This represents how much disk I/O capacity the device is using. It is calculated across all disks on the device. The range is from 1 to 100. The default is 80.
Sample Period	Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.
Number of Samples	Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.
Memory Settings	
Enable	Allows the SB to collect memory usage information from the device.
Threshold	The threshold (in percent) determines the extent of memory usage allowed. The range is from 1 to 100. The default is 80.
Sample Period	Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.
Number of Samples	Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.
KMemory Settings	
Threshold	The threshold (in percent) determines the extent of kernel memory usage allowed. The range is from 1 to 100. The default is 50.
Sample Period	Time interval (in seconds) between two consecutive samples. The range is from 1 to 60. The default is 1.
Number of Samples	Number of most recently sampled values used when calculating the average. The range is from 1 to 120. The default is 2.
Augmentation Alarms	
Enable	Enables augmentation alarms. For more information, see the "Augmentation Alarms" section on page 3-40.

Table 3-20 Service Monitor Fields (continued)

Field	Description
Threshold	The augmentation alarms threshold is a percentage, that applies to the CPU, memory, kernel memory, disk, disk fail count, and NIC usages. By default it is set to 80 percent. The threshold value range is 1–100. As an example of an augmentation alarm, if the threshold configured for CPU usage is 80 percent, and the augmentation threshold is set to 80 percent, then the augmentation alarm for CPU usage is raised when the CPU usage crosses 64 percent. If "A" represents the Service Monitor threshold configured, and "B" represents the augmentation threshold configured, then the threshold for raising an augmentation alarm = (A * B) / 100 percent.
Transaction Logging	
Enable	Enables Service Monitoring transaction logging. For more information, see the "Service Monitor Transaction Logs" section on page 6-19.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Augmentation Alarms

Augmentation alarms are soft alarms that send alerts before the threshold is reached. These alarms are applicable to all devices—Service Brokers, Service Brokers and VDSMs. Augmentation thresholds apply to device parameters.

A different augmentation alarm is supported for each of the device-level thresholds. Based on the device parameters monitored by Service Monitor, the following minor alarms could be raised for device-level thresholds:

- CpuAugThreshold—Service Monitor CPU augmentation alarm.
- MemAugThreshold—Service Monitor memory augmentation alarm.
- KmemAugThreshold—Service Monitor kernel memory augmentation alarm.
- DiskAugThreshold—Service Monitor disk augmentation alarm.
- DiskFailCntAugThreshold—Service Monitor disk failure count augmentation alarm.

Check the augmentation threshold, device-level threshold, and average load for the above alarm instance. Add more devices if necessary. A useful command is the **show service-monitor** command. The augmentation alarms raised are displayed in the **show alarms detail** command. The alarms are cleared when the load goes below the augmentation threshold.

Note For system disks (disks that contain SYSTEM partitions), only when all system disks are bad is the diskfailure augmentation and threshold alarms raised. The diskfailcnt threshold does not apply to system disks. The threshold only applies to CDNFS disks, which is also the case for the augmentation thresholds. This is because the system disks use RAID1. There is a separate alarm for bad RAID. With the RAID system, if the critical primary disk fails, the other mirrored disk (mirroring only occurs for SYSTEM partitions) seamlessly continues operation. However, if the disk drive that is marked bad is a critical disk drive, the redundancy of the system disks for this device is affected. For more information

on disk error handling and threshold recommendations, see the "Enabling Disk Error Handling" section on page 3-18.

As the **show disk details** command output reports, if disks have both SYSTEM and CDNFS partitions, they are treated as only system disks, which means they are not included in the accounting of the CDNFS disk calculation.

Configuring SNMP

The Cisco VDS-SB supports the following versions of SNMP:

- Version 1 (SNMPv1)—A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
- Version 2 (SNMPv2c)—The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.
- Version 3 (SNMPv3)—An interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are:
  - Message integrity—Ensuring that a packet has not been tampered with in-transit.
  - Authentication—Determining the message is from a valid source.
  - Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

  SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

Table 3-21 identifies what the combinations of security models and levels mean.

Table 3-21 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Process
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

The SNMPv3 agent can be used in the following modes:

- noAuthNoPriv mode (that is, no security mechanisms turned on for packets)
- AuthNoPriv mode (for packets that do not need to be encrypted using the privacy algorithm [DES 56])
- AuthPriv mode (for packets that must be encrypted; privacy requires that authentication be performed on the packet)

Using SNMPv3, users can securely collect management information from their SNMP agents without worrying that the data has been tampered with. Also, confidential information, such as SNMP set packets that change a Content Engine's configuration, can be encrypted to prevent their contents from being exposed on the wire. Also, the group-based administrative model allows different users to access the same SNMP agent with varying access privileges.

Note the following about SNMPv3 objects:

- Each user belongs to a group.
- Group defines the access policy for a set of users.
- Access policy is what SNMP objects can be accessed for reading, writing, and creating.
- Group determines the list of notifications its users can receive.
- Group also defines the security model and security level for its users.

To configure the SNMP settings, do the following:

Step 1 Choose **Devices > Devices > General Settings > Notification and Tracking > SNMP > General Settings**. The SNMP General Settings page is displayed.

Step 2 Enable the settings as appropriate. See Table 3-22 for a description of the fields.

Table 3-22 SNMP General Settings Fields

Field	Description
Traps	
Enable SNMP Settings	Enables the SNMP agent to transmit traps to the SNMP server.
Service Engine	Enables the Disk Fail trap, which is the disk failure error trap.
SNMP	Enables SNMP-specific traps: • Authentication—Enables authentication trap. • Cold Start—Enables cold start trap.
SB Alarm	Enables alarm traps: • Raise Critical—Enables raise-critical alarm trap. • Clear Critical—Enables clear-critical alarm trap. • Raise Major—Enables raise-major alarm trap. • Clear Major—Enables clear-major alarm trap. • Raise Minor—Enables raise-minor alarm trap. • Clear Minor—Enables clear-minor alarm trap.
Entity	Enables SNMP entity traps.

Table 3-22 SNMP General Settings Fields (continued)

Field	Description
Config	Enables CiscoConfigManEvent error traps.
Miscellaneous Settings	
Notify Inform	Enables the SNMP notify inform request.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Step 4 From the left-panel menu, click **Community**. The SNMP Community Table page is displayed.

The table is sortable by clicking the column headings. The maximum number of community strings that can be created is ten.

Step 5 Click the **Create New** icon in the task bar. The SNMP Community page is displayed.

Click the **Edit** icon next to the community name to edit a community setting.

Note Each community is associated with a group. Each group has a view and users are assigned to a group. If the group does not have a view associated with it, then users associated that group cannot access any MIB entry.

Step 6 Enter the settings as appropriate. See Table 3-23 for a description of the fields.

Table 3-23 SNMP Community Fields

Field	Description
Community	Community string used as a password for authentication when you access the SNMP agent of the device using SNMPv1 or SNMPv2. The “Community Name” field of any SNMP message sent to the device must match the community string defined here to be authenticated. You can enter a maximum of 64 characters in this field.
Group name/rw	Group to which the community string belongs. The **Read/Write** option allows a read or write group to be associated with this community string. The **Read/Write** option permits access to only a portion of the MIB subtree. Choose one of the following three options from the drop-down list: • **None**—Choose this option if you do not want to specify a group name to be associated with the community string. • **Read/Write**—Choose this option if you want to allow read-write access to the group associated with this community string. • **Group**—Choose this option if you want to specify a group name.
Group Name	Name of the group to which the community string belongs. You can enter a maximum of 64 characters in this field. This field is available only if you have chosen the **Group** option in the Group name/rw field.

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

To delete an SNMP community, click the **Edit** icon for the community, then click the **Delete** icon in the task bar.

Step 8 From the left-panel menu, click **Group**. The SNMP Group Table page is displayed.

The table is sortable by clicking the column headings. The maximum number of groups that can be created is ten.

Step 9 Click the **Create New** icon in the task bar. The SNMP Group page is displayed.

Click the **Edit** icon next to the Group Name to edit a group.

Step 10 Enter the settings as appropriate. See Table 3-24 for a description of the fields.

Table 3-24 SNMP Group Fields

Field	Description
Name	Name of the SNMP group. You can enter a maximum of 256 characters. A group defines a set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define what SNMP objects can be read, written to, or created. In addition, the group defines what notifications a user is allowed to receive. An SNMP group is a collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of the attributes defined by the group.
Sec Model	Security model for the group. Choose one of the following options from the drop-down list: • **v1**—Version 1 security model (SNMP Version 1 [noAuthNoPriv]). • **v2c**—Version 2c security model (SNMP Version 2 [noAuthNoPriv]). • **v3-auth**—User security level SNMP Version 3 (AuthNoPriv). • **v3-noauth**—User security level SNMP Version 3 (noAuthNoPriv). • **v3-priv**— User security level SNMP Version 3 (AuthPriv). The **Sec Model** you choose determines which of the following three security algorithms is used on each SNMP packet: • noAuthNoPriv—Authenticates a packet by a string match of the username. • AuthNoPriv—Authenticates a packet by using either the HMAC MD5 or SHA algorithms. • AuthPriv—Authenticates a packet by using either the HMAC MD5 or SHA algorithms and encrypts the packet using the CBC-DES (DES-56) algorithm.
Read View	Name of the view (a maximum of 64 characters) that enables you only to view the contents of the agent. By default, no view is defined. To provide read access to users of the group, a view must be specified. A read view defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the group.

Table 3-24 SNMP Group Fields (continued)

Field	Description
Write View	Name of the view (a maximum of 64 characters) that enables you to enter data and configure the contents of the agent. By default, no view is defined. A write view defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.
Notify View	Name of the view (a maximum of 64 characters) that enables you to specify a notify, inform, or trap. By default, no view is defined. A notify view defines the list of notifications that can be sent to each user in the group.

Step 11 Click **Submit** to save the settings.

To delete an SNMP group, click the **Edit** icon for the group, then click the **Delete** icon in the task bar.

Step 12 From the left-panel menu, click **User**. The SNMP User Table page is displayed.

The table is sortable by clicking the column headings. The maximum number of users that can be created is ten.

Step 13 Click the **Create New** icon in the task bar. The SNMP User page is displayed.

Click the **Edit** icon next to the username to edit a user.

Step 14 Enter the settings as appropriate. See Table 3-25 for a description of the fields.

Table 3-25 SNMP User Fields

Field	Description
Name	String representing the name of the user (256 characters maximum) who can access the device. An SNMP user is a person for which an SNMP management operation is performed.
Group	Name of the group (256 characters maximum) to which the user belongs.
Remote SNMP ID	Globally unique identifier for a remote SNMP entity. To send an SNMPv3 message to the device, at least one user with a remote SNMP ID must be configured on the device. The SNMP ID must be entered in octet string format. For example, if the IP address of a remote SNMP entity is 192.147.142.129, then the octet string would be 00:00:63:00:00:00:a1:c0:93:8e:81.
Authentication Algorithm	Authentication algorithm that ensures the integrity of SNMP packets during transmission. Choose one of the following three options from the drop-down list: • **No-auth**—Requires no security mechanism to be turned on for SNMP packets. • **MD5**—Provides authentication based on the hash-based Message Authentication Code Message Digest 5 (HMAC-MD5) algorithm. • **SHA**—Provides authentication based on the hash-based Message Authentication Code Secure Hash (HMAC-SHA) algorithm.

Table 3-25 SNMP User Fields (continued)

Field	Description
Authentication Password	String (256 characters maximum) that configures the user authentication (HMAC-MD5 or HMAC-SHA) password. The number of characters is adjusted to fit the display area if it exceeds the limit for display. This field is optional if the **no-auth** option is chosen for the authentication algorithm. Otherwise, this field must contain a value.
Confirmation Password	Authentication password for confirmation. The re-entered password must be the same as the one entered in the Authentication Password field.
Private Password	String (256 characters maximum) that configures the authentication (HMAC-MD5 or HMAC-SHA) parameters to enable the SNMP agent to receive packets from the SNMP host. The number of characters is adjusted to fit the display area if it exceeds the limit for display.
Confirmation Password	Private password for confirmation. The re-entered password must be the same as the one entered in the Private Password field.

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

To delete an SNMP user, click the **Edit** icon for the user, then click the **Delete** icon in the task bar.

Step 16 To define a SNMPv2 MIB view, click **View** from the left-panel menu. The SNMP View Table page is displayed.

The table is sortable by clicking the column headings. The maximum number of SNMPv2 views that can be created is ten.

SNMP view—A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.

Step 17 Click the **Create New** icon in the task bar. The SNMP View page is displayed.

Click the **Edit** icon next to the username to edit a view.

Step 18 Enter the settings as appropriate. See Table 3-26 for a description of the fields.

Table 3-26 SNMP View Fields

Field	Description
Name	String representing the name of this family of view subtrees (256 characters maximum). The family name must be a valid MIB name such as ENTITY-MIB.
Family	Object identifier (256 characters maximum) that identifies a subtree of the MIB.
View Type	View option that determines the inclusion or exclusion of the MIB family from the view. Choose one of the following two options from the drop-down list: • **Included**—The MIB family is included in the view. • **Excluded**—The MIB family is excluded from the view. **Note** When configuring an SNMP View with Excluded, the specified MIB that is excluded is not accessible for the community associated with the group that has that view.

Step 19 Click **Submit** to save the settings.

To delete an SNMP view, click the **Edit** icon for the view, then click the **Delete** icon in the task bar.

Step 20 From the left-panel menu, click **Host**. The SNMP Host Table page is displayed.

The table is sortable by clicking the column headings. The maximum number of hosts that can be created is four.

Step 21 Click the **Create New** icon in the task bar. The SNMP Host page is displayed.

Click the **Edit** icon next to the hostname to edit a host.

Step 22 Enter the settings as appropriate. See Table 3-27 for a description of the fields.

Table 3-27 SNMP Host Fields

Field	Description
Trap Host	Hostname or IP address an SNMP entity to which notifications (traps and informs) are to be sent.
Community/User	Name of the SNMP community or user (256 characters maximum) that is sent in SNMP trap messages from the device.
Authentication	Security model to use for sending notification to the recipient of an SNMP trap operation. Choose one of the following options from the drop-down list: • **No-auth**—Sends notification without any security mechanism. • **v2c**—Sends notification using Version 2c security. • **Model v3-auth**—Sends notification using SNMP Version 3 (AuthNoPriv). • **Security Level v3-noauth**—Sends notification using SNMP Version 3 (NoAuthNoPriv security). • **Level v3-priv**—Sends notification using SNMP Version 3 (AuthPriv security).
Retry	Number of retries (1 to 10) allowed for the inform request. The default is 2.
Timeout	Timeout for the inform request in seconds (1 to 1000). The default is 15.

Step 23 Click **Submit** to save the settings.

To delete an SNMP host, click the **Edit** icon for the host, then click the **Delete** icon in the task bar.

Step 24 From the left-panel menu, click **Asset Tag**. The SNMP Asset Tag page is displayed.

Step 25 In the **Asset Tag Name** field, enter a name for the asset tag and click **Submit**.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Step 26 From the left-panel menu, click **Contact**. The SNMP Contact page is displayed.

Step 27 In the **Contact** field, enter a name of the contact person for this device.

Step 28 In the **Location** field, enter a location of the contact person for this device.

Step 29 Click **Submit** to save the settings.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Supported MIBs

The SNMP agent supports the following MIBs:

- ENTITY-MIB (RFC 2037 Revision 199610310000Z))
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790, hrSWInstalled and hrPrinterTable subgroups are not supported)
- BGP-4-MIB (RFC-4274)
- UCD-SNMP-MIB
- CISCO-ENTITY-ASSET-MIB
- CISCO-CONFIG-MAN-MIB (Revision 9511280000Z)
- CISCO_VDS_SERVICE_BROKER_MIB

ENTITY-MIB, MIB-II, HOST-RESOURCES-MIB, BGP-4-MIB, and UCD-SNMP-MIB are public-available MIBs.

To download a copy of the CISCO_VDS_SERVICE_BROKER_MIB, do the following:

Step 1 Choose **System > Files > SNMP MIB.** The CISCO_VDS_SERVICE_BROKER_MIB.my is listed.

Step 2 Click one of the following links;

- **CISCO_VDS_SERVICE_BROKER_MIB.my**

Your browser program displays a dialog box asking if you want to open or save the file.

Step 3 Choose the appropriate option; either open or save the file.

For each 64-bit counter MIB object in the CISCO_VDS_SERVICE_BROKER_MIB, a 32-bit counter MIB object is implemented so that SNMP clients using SNMPv1 can retrieve data associated with 64-bit counter MIB objects. The MIB objects of each of these groups are read-only.

The CISCO_VDS_SERVICE_BROKER_MIB.my provides some object identifiers (OIDs) for Service Broker statistics. All the OIDs in the MIB are only for querying purposes; no traps have been added to this MIB. The Service Broker MIB provides two groups, vdssbStatsGroup and vdssbServiceMonitorGroup, which contain OIDs for the statistics from the **show statistics service-broker all/summary/bfqdn/cdn/geolocation/history/javascript/** command

Use the following link to access the CISCO-ENTITY-ASSET-MIB and the CISCO-CONFIG-MAN-MIB:

ftp://ftp.cisco.com/pub/mibs/v2/

Note If your browser is located behind a firewall or you are connecting to the Internet with a DSL modem and you are unable to access this file folder, you must change your web browser compatibility settings. In the Internet Explorer (IE) web browser, choose **Tools > Internet Options > Advanced**, and check the **Use Passive FTP** check box.

Enabling System Logs

Use the System Logs page to set specific parameters for the system log file (syslog). This file contains authentication entries, privilege level settings, and administrative details. System logging is always enabled. By default, the system log file is stored as /local1/syslog.txt.

To enable system logging, do the following:

Step 1 Choose **Devices > Devices > General Settings > Notification and Tracking > System Logs**. The System Log Settings page is displayed.

Step 2 Enter the settings as appropriate. See Table 3-28 for a description of the fields.

Table 3-28 System Logs Settings Fields

Field	Description
System Logs	
Enable	Enables system logs.
Facility	Facility where the system log is sent.
Console Settings	
Enable	Enable sending the system log to the console.
Priority	Severity level of the message that should be sent to the specified remote syslog host. The default priority is warning. The priorities are: Emergency—System is unusable. Alert—Immediate action needed. Critical—Critical condition. Error—Error conditions. Warning—Warning conditions. Notice—Normal but significant conditions. Information—Informational messages. Debug—Debugging messages.
Disk Settings	
Enable	Enables saving the system logs to disk.
File Name	Path and filename where the system log file is stored on the disk. The default is /local1/syslog.txt.
Priority	Severity level of the message that should be sent to the specified remote syslog host.
Recycle	The maximum size of the system log file before it is recycled. The default is 10000000 bytes.
Host Settings	
Enable	Enables sending the system log file to a host. You can configure up to four hosts.
Hostname	A hostname or IP address of a remote syslog host.

Table 3-28 System Logs Settings Fields (continued)

Field	Description
Priority	Severity level of the message that should be sent to the specified remote syslog host.
Port	The destination port on the remote host. The default is 514.
Rate Limit	The message rate per second. To limit bandwidth and other resource consumption, messages can be rate limited. If this limit is exceeded, the remote host drops the messages. There is no default rate limit, and by default all system log messages are sent to all syslog hosts.

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

Multiple Hosts for System Logging

Each syslog host can receive different priority levels of syslog messages. Therefore, you can configure different syslog hosts with a different syslog message priority code to enable the device to send varying levels of syslog messages to the four external syslog hosts.

However, if you want to achieve syslog host redundancy or failover to a different syslog host, you must configure multiple syslog hosts on the device and assign the same priority code to each configured syslog host.

Configuring Transaction Logs for the Service Broker

Transaction logs allow administrators to view the traffic that has passed through the SB. The fields in the transaction log are the client's IP address, the date and time when a request was made, the URL that was requested, the SB selected to serve the content, the protocol, and the status of the redirect. The SB transaction log file uses the W3C Common Log file format. For more information about transaction logs and their formats, see the "Service Broker Transaction Log Fields" section on page 6-17.

To enable transaction logging for the SB, do the following:

Step 1 Choose **Devices > Devices > General Settings > Notification and Tracking > Transaction Logging**. The Transaction Log Settings page is displayed.

Step 2 Enter the settings as appropriate. See Table 3-29 for a description of the fields.

Table 3-29 Transaction Log Settings Fields

Field	Description
General Settings	
Transaction Log Enable	Enables transaction logging.
Compress Files before Export	When this check box is checked, archived log files are compressed into gzip format before being exported to external FTP servers
Archive Settings	
Max size of Archive File	Maximum size (in kilobytes) of the archive file to be maintained on the local disk. The range is from 1,000 to 2,000,000. The default is 500,000.

Table 3-29 Transaction Log Settings Fields (continued)

Field	Description
Max number of files to be archived	Maximum number of files to be maintained on the local disk. The range is from 1 to 10,000. The default is 10.
Archive occurs	How often the working log is archived and the data is cleared from the working log. Choose one of the following: • Choose **every** to archive every so many seconds, and enter the number of seconds for the interval. The range is from 120 to 604800. • Choose **every hour** to archive using intervals of one hour or less, and choose one of the following: – **at**—Specifies the minute in which each hourly archive occurs – **every**—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30) • Choose **every day** to archive using intervals of one day or less, and choose one of the following: – **at**—Specifies the hour in which each daily archive occurs – **every**—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24) • Choose **every week on** to archive at intervals of one or more times a week, choose the days of the week, and choose what time each day.
Export Settings	
Enable Export	Enables exporting of the transaction log to an FTP server.
Export occurs	How often the working log is sent to the FTP server and the data is cleared from the working log. Choose one of the following: • Choose **every** to export every so many minutes, and enter the number of minutes for the interval. The range is from 1 to 100800. • Choose **every hour** to export using intervals of one hour or less, and choose one of the following: – **at**—Specifies the minute in which each hourly export occurs – **every**—Specifies the number of minutes for the interval (2, 5, 10, 15, 20, or 30) • Choose **every day** to export using intervals of one day or less, and choose one of the following: – **at**—Specifies the hour in which each daily export occurs – **every**—Specifies the number of hours for the interval (1, 2, 3, 4, 6, 8, 12, 24) • Choose **every week on** to export using intervals of one or more times a week, choose the days of the week, and what time each day.
FTP Export Server	IP address or hostname of the FTP server.
Name	Name of the user.

Table 3-29 Transaction Log Settings Fields (continued)

Field	Description
Password	Password for the user.
Confirm Password	Confirms the password for the user.
Directory	Name of the directory used to store the transaction logs on the FTP server.
SFTP	Check the **SFTP** check box, if you are using an SFTP server.

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

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

Configuring Troubleshooting

The Kernel Debugger troubleshooting page allows you to enable or disable access to the kernel debugger. Once enabled, the kernel debugger is automatically activated when kernel problems occur.

Note The "hardware watchdog" is enabled by default and automatically reboots a device that has stopped responding for over ten minutes. Enabling the kernel debugger disables the "hardware watchdog."

If the device runs out of memory and kernel debugger (KDB) is enabled, the KDB is activated and dump information. If the KDB is disabled and the device runs out of memory, the syslog reports only dump information and reboots the device.

Enabling the Kernel Debugger

To enable the kernel debugger, do the following:

Step 1 Choose **Devices > Devices > General Settings > Troubleshooting > Kernel Debugger**. The Kernel Debugger window appears.

Step 2 To enable the kernel debugger, check the **Enable** check box, and click **Submit**.

To apply the factory default settings for the device, click the **Apply Defaults** icon in the task bar.

To remove the settings from the device, click the **Remove Settings** icon in the task bar.

For information about monitoring the SBs, see the "Device Monitoring" section on page 6-7.

Configuring URL Signing

The URL Signing page allows you to see the list of URL Signing keys configured in the Service Broker.

To create a new URL Signature key, do the following:

Step 1 Choose **Devices > SB Device> General Settings> URL Signing.** The URL Signing Table page is displayed.

Step 2 Click the **Create New** icon in the task bar. The Creating New URL Signature Key page is displayed.

To edit a URL Signing Key, click the **Edit** icon next to the URL Signing Key.

Step 3 Enter the settings as appropriate. See Table 3-30 for a description of the fields.

Table 3-30 URL Signing Key Fields

Field	Description
Cryptographic Algorithm	Specifies the cryptographic algorithm. From the **Cryptographic Algorithm** drop-down list choose **Symmetric** or **Asymmetric**
Key ID Owner	Specifies the owner ID of the owner of the encryption key. Valid values are 1-8
Key ID Number	Specifies the encryption Key ID number. Valid values are 1-8
Key	This field is applicable only if **Symmetric Key** is chosen in the **Cryptographic Algorithm** drop-down list. Specifies a unique URL signature key with up to 64 characters (excluding double quotes at the beginning and end of the string). Valid values are 7-bit printable ASCII characters (alphabetic, numerics, and others) and does not support a space or the following special characters: question mark (?), and double quotes ("). Quoted and unquoted strings are allowed. Double quotes (") are allowed at the beginning and end of the string only. If you do not surround the key string with double quotes, quotes are added when you click **Submit.**
Public Key URL	This field is applicable only if **Asymmetric Key** is chosen in the **Cryptographic Algorithm** drop-down list. Specifies the location of the public key file. Only HTTP, HTTPS, or FTP addresses are supported. The public/private key pair is stored in Privacy Enhanced Mail (PEM) format.

Table 3-30 URL Signing Key Fields (continued)

Field	Description
Private Key URL	This field is applicable only if **Asymmetric Key** is chosen in the **Cryptographic Algorithm** drop-down list. Specifies the location of the private key file. Only HTTP, HTTPS, or FTP addresses are supported. The public/private key pair is stored in Privacy Enhanced Mail (PEM) format.
Symmetric Key	This field is applicable only if **Asymmetric Key** is chosen in the **Cryptographic Algorithm** drop-down list. Specifies the 64 bytes symmetric key Valid values are 7-bit printable ASCII characters (alphabetic, numerics, and others) and does not support a space or the following special characters: question mark (?), and double quotes ("). Quoted and unquoted strings are allowed. Double quotes (") are allowed at the beginning and end of the string only. If you do not surround the key string with double quotes, quotes are added when you click **Submit.**

Step 4 Click **Submit** to save the URL Signing key details.

Configuring the VDSM

Configuring a VDSM consists of the General Settings menu items. For information on configuring general settings, see the "General Settings" section on page 3-5.

Device activation is accomplished during installation and initialization of the VDS-SB devices.

The Device Activation page for the VDSM displays information about the management IP address and the role of the VDSM. To change the name of the VDSM, enter a new name in the **Name** field and click **Submit**.

For information about primary and standby VDSMs, see the "Configuring Primary and Standby VDSMs" section on page 2-7.