CHAPTER 5

Configuring the System

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

For information on logs, see the "System Audit Logs" section on page 6-6. For information on upgrading the VDS-SB software, see the "Software Upgrade" section on page 7-1. For information on the ports used by the VDS-SB, see the "System Port Numbers" section on page 6-6.

Configuring AAA

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

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

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

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

In the VDS-SB network, login authentication and authorization are used to control user access and configuration rights to the VDSM and SBs There are two levels of login authentication and authorization:

- Device
- VDSM

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.

This section covers login authentication and authorization for the VDSM. For information about device login authentication and authorization, see the "Login Access Control" section on page 3-6 and the "Authentication" section on page 3-14.

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

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

Creating, Editing, and Deleting Users

Note This section is addressed to users with administrator-level privileges (admin users) only.

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

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

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

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

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

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

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

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

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

Table 5-1 describes the icons for the User Table page.

Table 5-1 User Table Icons

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 8 In the **Branding String** field, enter a name or phrase that you want to appear in the VDSM banner, when this user logs in.

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

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

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

Table 5-1 describes the icons for the Role Management page.

Table 5-2 Role Management Icons

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

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

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

Step 12 Click the **Assign** icon (blue cross mark) next to each role name you want to assign to the user account. To remove the role from the user account, click the **Assign** icon again.

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

Step 13 Click **Submit** to save the settings.

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

Step 14 From the left-panel menu, click **Domain Management**. The Domain Management Table page is displayed.

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

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

Step 15 Click the **Assign** icon next to each domain name you want to assign to the user account.

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

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

Step 16 Click **Submit** to save the settings.

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

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

Creating, Editing, and Deleting Roles

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

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

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

To create or edit a role, do the following:

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

Table 5-1 describes the icons for the Role Management page.

Table 5-3 Role Management Icons

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

Table 5-3 Role Management Icons (continued)

Icon	Function
	Views all table entries. Click this icon to view all entries after you have created a filtered table.
	Refreshes the table.
	Assigns all roles.
	Removes all roles.
	Views read-only items.
	Indicates that the current transaction was successfully completed.

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

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

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

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

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

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

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

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

Creating, Editing, and Deleting Domains

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

When you configure a domain, you can choose to include Service Broker in the domain.

To create or edit a domain, do the following:

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

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

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

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

Step 4 From the **Entity Type** drop-down list, choose Service Brokers.

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

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

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

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

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

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

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

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

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

Changing a Password

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

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

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

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

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

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

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

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

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

Configuring System Settings

This section covers the following topics:

System Properties

To modify the system properties, do the following:

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

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

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

Table 5-4 describes the system properties.

Table 5-4 System Properties Fields

Field	Description
System.datafeed.pollRate	The poll rate of devices to VDSM (in seconds). The default setting is 30 seconds
System.device.recovery.key	Device Identity Recovery Key.This property enables a device to be replaced by another node in the VDS-SB network.
System.gui.rowCount	Default row count for all pages containing a table. The default setting is 10.
System.gui.session.timeout	Length of a VDSM session (in minutes). The default value is 100 minutes.
System.healthmonitor.collectRate	Sets the collect and send rate in seconds for the CMS device health (or status) monitor. The default is 120 seconds. The range is from 5 to 3600.
System.lcm.enable	Local and VDSM feature. This property allows settings that are configured using the local device CLI or the VDSM to be stored as part of the VDS-SB network configuration data. The default value is true.
System.security.minPasswordLength	Minimum number of characters required for a user password. The default is 6. The range is from 6 to 31.
System.security.minUserNameLength	Minimum number of characters required for a user name. The default is 4. The range is from 1 to 32.

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

Configuring Device Offline Detection

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

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

To configure Device Offline Detection, do the following:

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

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

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

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

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

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

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

Maximum Offline Detection Time =Heartbeat Rate * Heartbeat Fail Count

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

Service Broker Policy Files

The Service Broker Policy Files menu options consist of the following:

- Configuring Service Broker Policy File
- Configuring BFQDN Policy File
- Configuring CDN Selection Policy File
- Configuring CDN Adaptation Policy File

Configuring Service Broker Policy File

Service Broker Policy File can be used as a global file to encompass all 3 sub files (BFQN policy file, CDN Selection Policy File and CDN Adaptation Policy File) into one large Javascript file for simplicity in smaller applications.

To register a Service Broker Policy File, do the following:

Step 1 Choose **System > Configuration > Service Broker Policy Files > Service Broker Policy File Registration**. The Service Broker Policy File Registration page is displayed.

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

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

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

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

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

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

Table 5-5 Upload Method for Service Broker Policy File Registration

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

Table 5-6 Import Method for Service Broker Policy File Registration

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

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

Configuring BFQDN Policy File

To register a BFQDN Policy File, do the following:

Step 1 Choose **System > Configuration > Service Broker Policy Files > BFQDN Policy File Registration**. The BFQDN Policy File Registration page is displayed.

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

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

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

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

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

Step 4 Enter the fields as appropriate. Table 5-7 describes the upload method fields. Table 5-8 describes the import method fields.

Table 5-7 Upload Method for BFQDN Policy File Registration

Property	Description
Namespace	Unique namespace for the BFQDN Policy file
Source File Upload	Local directory path to the BFQDN policy file. To locate the file, use the **Browse** button. Click the **Validate** button to validate the BFQDN Policy file.
Destination Filename	Name of the BFQDN policy file. This field is filled in automatically with the filename from the local directory path.

Table 5-8 Import Method for BFQDN Policy File Registration

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

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

Configuring CDN Selection Policy File

To register a CDN Selection Policy File, do the following:

Step 1 Choose **System > Configuration > Service Broker Policy Files > CDN Selection Policy File Registration**. The CDN Selection Policy File Registration page is displayed.

Step 2 To set a global Service Broker Policy file, Click on the radio button next to the Service Broker Policy File URL.

Step 3 Click **Set Global File** button to save the settings. To clear the global Service Broker Policy file, click **Clear Global File** button**.**

Step 4 To create a new Service Broker Policy File , Click the **Create New** icon in the task bar. The CDN Selection Policy File Registration page is displayed.

To edit a CDN Selection Policy file registration, click the **Edit** icon next to the registration you want to edit.

Step 5 Choose a file import method from the **File Import Method** drop-down list:

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

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

Step 6 Enter the fields as appropriate. Table 5-9 describes the upload method fields. Table 5-10 describes the import method fields.

Table 5-9 Upload Method for CDN Selection Policy File Registration

Property	Description
Namespace	Unique namespace for the CDN Selection Policy file
Source File Upload	Local directory path to the CDN Selection Policy file. To locate the file, use the **Browse** button. Click the **Validate** button to validate the CDN Selection Policy file.
Destination Filename	Name of the CDN Selection policy file. This field is filled in automatically with the filename from the local directory path.

Table 5-10 Import Method for CDN Selection Policy File Registration

Property	Description
Namespace	Unique namespace for the CDN Selection Policy file
Source File URL	The URL where the CDN Selection Policy file is located, including path and filename. Click the **Validate** button to validate the CDN Selection Policy file.
Destination File Name	Name of the CDN Selection Policy file.
Update Interval (minutes)	Frequency with which the VDSM looks for changes to the CDN Selection policy file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the CDN Selection policy file.
Password	User password for fetching the CDN Selection policy file.

Step 7 To save the settings, click **Submit**.

Configuring CDN Adaptation Policy File

To register a CDN Adaptation Policy File, do the following:

Step 1 Choose **System > Configuration > Service Broker Policy Files > CDN Adaptation Policy File Registration**. The CDN Adaptation Policy File Registration page is displayed.

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

To edit a CDN Adaptation Policy file registration, click the **Edit** icon next to the registration you want to edit.

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

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

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

Step 4 Enter the fields as appropriate. Table 5-11 describes the upload method fields. Table 5-12 describes the import method fields.

Table 5-11 Upload Method for CDN Adaptation Policy File Registration

Property	Description
Namespace	Unique namespace for the CDN Adaptation Policy file
Source File Upload	Local directory path to the CDN Adaptation policy file. To locate the file, use the **Browse** button. Click the **Validate** button to validate the CDN Adaptation Policy file.
Destination Filename	Name of the CDN Adaptation policy file. This field is filled in automatically with the filename from the local directory path.

Table 5-12 Import Method for CDN Adaptation Policy File Registration

Property	Description
Namespace	Unique namespace for the CDN Adaptation Policy file
Source File URL	The URL where the CDN Adaptation Policy file is located, including path and filename. Click the **Validate** button to validate the CDN Adaptation Policy file.
Destination File Name	Name of the CDN Adaptation Policy file.
Update Interval (minutes)	Frequency with which the VDSM looks for changes to the CDN Adaptation policy file. The default value is 10 minutes.
Username	Name of the user to be authenticated when fetching the CDN Adaptation policy file.
Password	User password for fetching the CDN Adaptation policy file.

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

Configuring CDN IP Network File

On-net/Off-net designation of IP subnets is done via coverage zone xml file. Up to 50,000 subnet entries are supported in this file.

To configure a CDN IP Network File, do the following:

Step 1 Choose **System > Configuration > CDN IP Network File Registration**. The CDN IP Network File Registration page is displayed.

Step 2 To set a global CDN IP Network file, Click on the radio button next to the CDN IP Network File URL.

Step 3 Click **Set Global File** button to save the settings. To clear the global CDN IP Network file, click **Clear Global File** button**.**

Step 4 To upload a new CDN IP Network file, Click the **Create New** icon in the task bar. The CDN IP Network File Registration page is displayed.

To edit a CDN IP Network file registration, click the **Edit** icon next to the registration you want to edit.

Step 5 Choose a file import method from the **File Import Method** drop-down list:

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

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

Step 6 Enter the fields as appropriate. Table 5-13 describes the upload method fields. Table 5-14 describes the import method fields.

Table 5-13 Upload Method for CDN IP Network File Registration

Property	Description
Source File Upload	Local directory path to the CDN Adaptation policy file. To locate the file, use the **Browse** button. Click the **Validate** button to validate the CDN IP Network file.
Destination Filename	Name of the CDN IP Network file. This field is filled in automatically with the filename from the local directory path.

Table 5-14 Import Method for CDN IP Network File Registration

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

Step 7 To save the settings, click **Submit**.

Configuring the VDSM to Communicate with an External System

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

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

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

- VDSM configuration settings to allow communication with Prime Central
- Registration of the VDSM on Prime Central

- Sending SNMP traps to Prime Central

Registering and De-Registering with Prime Central

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

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

Note VDSM should be de-registered from the Prime Central before deleting the configuration settings of Prime Central.

To configure the settings for an external system (Prime Central), do the following:

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

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

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

Step 3 Enter the settings as appropriate. See Table 5-15 for a description of the fields.

Table 5-15 External System Parameters

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

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

Viewing or Downloading XML Schema Files

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

- CDNNetwork.xsd—CDN-IP Network Configuration file is used to customize the networks and geographic regions each SB services.

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

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

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

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