Global Settings

This chapter has the following sections:

Transaction Settings

To set up the transactions:

Step 1 Go to **Global Settings** > **Transaction Settings**.

Step 2 Specify the **Out-of-Sync Commit** behavior to control the Check Sync feature. See Synchronizing Configuration for details about the synchronizing configuration using the Config Sync feature. Choose one of the following:

Choose:

- Accept— Check sync feature in network inventory will be disabled.
- Reject— Check sync feature in network inventory will be enabled.

Step 3 Enable/disable Device South Bound Lock—Device southbound lock is enabled by default. When VTS has a redundant pair or group, it is possible for a transaction to succeed even when one or more of the redundant members are down, as long as one device is up. When the transaction comes, VTS checks the connectivity to the redundant devices and if it can not reach one of the devices, the admin state of the device will be changed to southbound-locked and the transaction configuration will only be pushed to the active devices. In order for the southbound lock feature to work, you must create a umap and provide the credentials that NSO will use, in the authgroup "vts-default" . This feature currently supports the following redundant groups:

- VPC Pair
- ESI Group

- Static Multi-Homed devices
- DCI
- VTSR

Step 4 Click **Save**.

Modifying Login Banners

The Login Banners page lets you modify the text that appears on the VTS login page and Home page.

To modify login banners:

Step 1 Go to **Administration** > **Login Banners**. The Login Banners page appears.
Step 2 Modify the text in the Before login Text text box, to update the text that appears on the VTS login screen.
Step 3 Modify the text in the After login Text text box, to update the text that appears on the Home page after you log in.
Step 4 Click **Submit**.

Managing Users

You can create users to define the role that the users have when they log in to Cisco VTS. There are two default roles available:

- Administrator
- Operator
- ncsadmin—Has the same permissions as Administrator.
- ncsoper—Has the same permissions as Operator.

To create users:

Step 1 Click **Administration** > **User Management**. The Administration / User Management window appears.
Step 2 Click **Add (+)** icon. The Add New User popup window appears.
Step 3 Enter the **User Name** and **Passphrase**, and then select the desired role from the Role drop down list.
Step 4 Click **Save**.

The user details get added to the Users table.

Note To edit the user name, check the User Name check box, click **Edit** icon.

To delete the user name, check the User Name check box, click **Delete (X)** icon.

Step 5 You must add the user to the Authentication group. To do this go to **Inventory** > **Authentication Group**, and add the user.

Step 6 Log out and log in again with the new user.

Enabling External Authentication and Authorization

Cisco VTS allows you to integrate with a remote authentication and authorization server for user authentication and authorization. In this release, Cisco VTS supports external authentication and authorization via TACACS+ servers and LDAP servers.

Note Cisco VTS does not support Accounting via LDAP servers.

You can add multiple TACACS+ servers and LDAP servers. The authentication servers are chosen from the list of configured servers based on the priority that you set when you configure external authentication.

See the TACACS+ documentation for installing and configuring the TACACS+ server on the IPv4/IPv6 network.

Cisco VTS supports OpenLDAP and MS-ActiveDirectory implementations of LDAP. See the respective documentation for details about installing and configuring the LDAP servers.

For a user logging into VTS to be able to authenticate via TACACS+ server or LDAP server, the VTS admin needs to set up the external authorization servers.

For TACACS + servers, a TACACS+ user has to be added to the user group and that user group has to be mapped to a VTS user role, which is the administrator and operator. To do this, you need to modify the TACACS+ configuration file and add users and groups to map with the VTS user role. The user group names that you need to use while you create users in TACACS+ server are:

- Administrator
- Operator

On LDAP Server, users should be mapped to "Administrator / Operator " role for VTS to authorize the users. This can be done by making the memberUid attribute of Administrator / Operator group, the uid of the user.

See Setting up Remote Authentication Server, on page 4 for details.

Important Notes:

- If the same username is present in the local (Cisco VTS) database and the TACACS+/LDAP server, then the user will be first authenticated using the local server. If the username is not present in the local database, or if local authentication fails due to a password mismatch, then the system tries to authenticate the user from the TACACS+/LDAP server.
- Cisco VTS users and groups should be consistent across all the participating TACACS+/LDAP servers.
- If the same username is configured in both local and TACACS+/LDAP server, you need to make sure the roles assigned are identical at both the places. We recommend that you have unique users in the local database and TACACS+/LDAP servers.

- If an AAA user is not assigned to any of the Cisco VTS groups in TACACS+/LDAP server, the user authentication will fail.
- AAA users, even AAA admin users, will not be able to disable AAA, but still will be able to add/delete AAA configuration.
- AAA username with special characters are not supported.
- We recommend that you use the *vts-default* authorization group while adding devices into network inventory. This is a system defined authorization group, available in Cisco VTS. If you are not using the *vts-default* authorization group, you need to ensure that you create an auth group which has AAA user added as the VTC Admin User Name.

The servers are contacted for authentication, based on the priority you set while you configure the servers. If a TACACS+/LDAP server is unavailable, then the next server is contacted for authentication and so on till all the servers are exhausted. This process is repeated thrice. If the user cannot be authenticated or authorized all the three times, then the authentication for the external user fails.

Setting up Remote Authentication Server

To enable remote user authentication, you must configure the system to use an external authentication server.

Before you begin

Review the Enabling External Authentication and Authorization, on page 3 section.

Step 1 Go to **Global Settings** > **Remote Authentication Settings**.
The Remote Authentication Settings page appears.

Step 2 Set the Global Time Out. This is to set the connection timeout with the external authentication server. The default is 15 seconds. The number of retries for a connection is set to three.

Step 3 Use the **Enable Protocol** slider to enable the desired protocol. You must add at least one server for the selected protocol. TACACS+ and LDAP are supported.

To enable TACACS+, use the TACACS + slider.

a) Click **Add (+)**. The Configure TACACS + popup window appears.
b) Enter the IP Address/Host Name, and the port details.
c) Enter the secret key in the Key field. This can have 128 characters.
d) Enter the secret key in the Key field. This can have 128 characters.
e) Click **Logging** toggle button to enable the accounting.

For details about accounting and logging, see Setting up Accounting and Enabling Accounting and Logging.

To delete a TACACS+ server, select the check box corresponding to the server, click delete **(X)**, and then click **Save**.

To enable LDAP, use the LDAP slider.

a) Click **Add (+)**.
b) Enter the IP Address/Hostname. This is the IP adddress or Hostname of the LDAP server.
c) Enter the Root Domain Name. This is the Base DN of the LDAP server. This is a comma-separated list.
d) Enter the User Search Base. This is the LDAP directory used to search for the user identity.
e) Enter the Group Search Base. This is to determine the organizational unit that contains the groups.

Note Multiple entries for USER SEARCH BASE is not supported. For example,

```
ou=DevUsers,dc=arun,dc=net or
ou=ProdUsers,dc=arun,dc=net or
ou=Users,ou=DevUsers,dc=arun,dc=net”
```

f) Enter the Group Search Filter. This is to determine the ObjectClass of the group.
g) Enter the Port of the LDAP server. By default, this is 389.
h) Enter the User Search Filter.
i) Enter the Group Membership Attribute
j) Check the SSL checkbox to enable SSL.
k) Click **Save**.

Step 4 Specify the priority with which Cisco VTS should contact the external authentication servers.

Enabling Accounting and Logging

The admin can select one of the TACACS+ Server as a logging server. Audit logs are sent to that server. In addition to that server, the audit logs will also be logged to the local log file (present in Cisco VTS).

On the TACACS+ server where you have enabled logging, you can find the log files at */var/log/tac_plus.acct*.

The Cisco VTS location where you can find the log file is */opt/vts/log/nso/vts-accounting.log*. Logs are collected every 120 seconds (default setting).

Following are the fields that can be found in the log:

- Client IP—Client IP from where the request was made
- Server IP—VTS server IP
- User Name—User who performs the transaction
- Message—The model change in the transaction or the REST API url
- Date/Time—The time when the change was made
- Application Name—VTS (static value)
- Operation Type—Derived from the change, could be CREATE, UPDATE or DELETE
- Status—Success or Error (static value)

Setting up Accounting

To set up accounting, you must add one of the TACACS+ servers that are registered with Cisco VTS as the logging server. You can do this while you add the remote authorization servers. If you have already added remote authentication servers, you can select a server and edit it to make it the logging server.

Note You can have only one TACACS+ server as the logging server at a time.

Step 1 Go to **Administration** > **Remote Authentication Settings**.
The Remote Authentication Settings page appears.

Step 2 Use the **Enable Protocol** toggle button to enable the desired protocol. You must add at least one configuration instance for the selected protocol. Currently only TACACS+ is supported.

Step 3 Click **Add (+)**. The Configure TACACS+ popup window appears.

Step 4 Enter the IP Address/Host Name, and the port details.

Note Cisco VTS supports IPv4 and IPv6 addresses.

Step 5 Enter the secret key in the Key field. This can have 128 characters.

Step 6 Click **Logging** toggle button to enable the accounting.

Step 7 Click **Add**.

Step 8 Click **Save**.
The logs get saved in the local VTS server and TACACS server.

In Cisco VTS, you can see all the logs in vts-accounting.log, which has details like the Username, Date/Time, Application Name, Operation Type, Status, Sever IP, Client IP address, and the exact message about the transaction. Similarly, in the TACACS server also you can see all the logs for the transactions.

Logs are collected every 120 seconds (default setting), and pushed to TACACS+ accounting server (for example, tac_plus.acct) and to VTC (vts-accounting.log).

The log file will be rotated once it reaches 100 MB in size. The backup exists for 10 rotations, then gets deleted.

Creating Authentication Groups

Authentication Group is used by Cisco VTS to authenticate or to log in to the device.

You can create authentication groups and assign devices you import into Cisco VTS, to these groups. Authentication groups are used to group devices with the same credentials (that is, usernames and passphrases). Once the authentication groups are created, all the devices under these groups may be accessed without specifying the credentials every time they are accessed.

If the same credential are used for accessing all devices, one authentication group can be used. If the credentials are different for different devices, multiple authentication-groups (as many as username/passphrase pairs used by devices) need to be created.

When you do a manual import of devices, the CSV file that is used to import inventory details links the authentication group with a specific device. The applicable authentication group should be used for corresponding device entry in the CSV file.

Note Changing the VTS UI password on first time log in does not update the vts-default authgroup password. To sync vts-default password with VTS UI, change the password of vts-default authgroup after you change the password for VTS UI initially. You must do this before you import devices into the inventory, using the vts-default authgroup.

To create an authentication group:

Step 1 Go to **Global Settings** > **Authentication Group**.

Step 2 Click **Add (+)** icon. The Add Authentication Group popup window appears.

Enter the following details, and click **Save**:

- Authentication Group Name—The authorization group name.
- VTC Admin User Name—This is the VTC administrative user name.
- Device User Name—This is the login user name for the device.
- Passphrase—This is the login passphrase for the device.

The authentication group gets added to the Groups table.

To edit an authentication group, select the desired Authenticationth Group Name check box and click the **Edit** icon.

To delete an authentication group, select the desired Authentication Group Name check box and click the **Delete (X)** icon.

Viewing HA Status

The High Availability page lets you view the status of nodes part of the high availability setup.

Go to **Administration** > **High Availabiity**.

You can view the role of Policy Plane, VTC and Control Plane, VTSR.

Note You can only view the table here without performing any action.

The VTC table displays the following details:

- Node ID
- Current Role
- Time Stamp
- Configured Role

The VTSR table displays the following details:

- Node ID
- Current Role
- Time Stamp

Enabling Auto Southbound Lock

Cisco VTS automatically southbound locks all the devices after a period of inactivity.

Note

- The auto southbound lock is enabled by default with 15 minute default period of inactivity.
- This feature is only about southbound lock. You must manually unlock the devices, if required.
- The period of inactivity is not checked on a device level. Upon hitting the inactivity period timer, all the devices are southbound locked.

To enable/disable auto southbound lock:

Step 1 Go to **Global Settings** > **Device Settings**. The Device Settings page appears.

Step 2 Use the **Auto Southbound Lock** toggle button to enable or disable the auto southbound lock feature. It is enabled by default.

Step 3 Enter the desired period of inactivity in the **Period of inactivity (in minutes)** field. This can be an integer between 15 and 60. The default is 15 minutes.