Authentication & Authorization (CVP)

Authentication determines if the provided user credentials (username/password) are correct. If authentication succeeds, the user is logged in.

Authorization determines what operations the user can perform after login. Authorization can be for no access, read access, or read and write access.

In the Access Control page, the type of Authentication and Authorization can be defined. AAA servers are defined in this page.

This module guides account management administrators to manage AAA servers, user accounts, and user roles. It provides the functionality required to manage all aspects of user accounts.

Note

Only account management administrators have the permissions to manage accounts.

Sections in this chapter include:

- Access to the Access Control Page on page 290
- Managing AAA Servers on page 292
- About Users and Roles on page 297
- Managing User Accounts on page 298
- Managing User Roles on page 301
- Viewing Activity Logs on page 304
- Access Requirements for Image Bundle Upgrades on page 306
14.1 Access to the Access Control Page

Step 1  Click the gear icon on the home page.

Figure 14-1: Gear Icon

Step 2  Click Access Control in the left menu.

The system displays the initial Access Control Page. See Figure 14-2.

Figure 14-2: Initial Access Control Page

The system displays the Servers section when either RADIUS or TACACS is selected as Authentication source. See Figure 14-3.

Figure 14-3: AAA Access Control Page

- If the authentication is local, the authorization must be done locally.
If the authentication is done externally, the authorization can be done locally or externally.

### Table 14-1 Server Authentication and Authorization

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Local</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td>RADIUS</td>
</tr>
<tr>
<td>TACACS</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td>TACACS</td>
</tr>
</tbody>
</table>

**Note**

External servers supported by CloudVision are RADIUS and TACACS.

**Related topics:**
- Managing AAA Servers on page 292
- Managing User Accounts on page 298
- Managing User Roles on page 301
- Access Requirements for Image Bundle Upgrades on page 306
14.2 Managing AAA Servers

The system uses the following functionalities to manage AAA servers:

- Adding AAA Servers
- Modifying AAA Servers
- Removing AAA Servers

14.2.1 Adding AAA Servers

Step 1 Navigate to the Access Control Page.

Step 2 Click the Authentication source drop-down menu and select either RADIUS or TACACS. The Access Control page lists all current servers. See Figure 14-3.

Step 3 Click + New Server at the upper right corner of the Servers section. See Figure 14-4.

Figure 14-4: + New Server in Access Control Page

Figure 14-5: New Server Pop-Up Window

Step 4 Provide the required Information in corresponding fields.

Step 5 If required, click Test for testing the new configuration. Else, skip to step 8.

Step 6 Enter your credentials when the Test Server pop-up prompts for it. See Figure 14-6.
Figure 14-6: Test Server Pop-Up Window

![Test Server Pop-Up Window](image)

**Step 7** Click **Run Test**.

The system displays test results. If required, modify the configuration based on the test result.

**Step 8** Click **Save**.

The server is added to the list of servers in the AAA grid.

**Related topics:**
- Access to the Access Control Page on page 290
- Modifying AAA Servers on page 293
- Removing AAA Servers on page 296

### 14.2.2 Modifying AAA Servers

**Step 1** Navigate to the **Access Control** Page.

**Step 2** Select desired modes from **Authentication source** and **Authorization source** drop-down menus.

The system lists all registered servers of the selected AAA server type. See **Figure 14-3**.

**Step 3** Click the edit icon available next to IP address of the corresponding server.

The system pops-up the **Edit Server** window. See **Figure 14-7**.

**Figure 14-7: Edit Server Pop-Up Window**

![Edit Server Pop-Up Window](image)

**Step 4** Modify the required information.
Step 5  If required, click **Test** to verify latest changes.

Step 6  Click **Save**.

**Note**
To apply external authentication, there should be at least one enabled server listed in the page.

### 14.2.2.1 Adding Vendor Specific Codes to AAA Servers

You can add vendor specific codes to AAA servers for the following:

- **RADIUS**
- **TACACS+**
- **CISCO ACS on page 295**

#### RADIUS

Arista Vendor Specific Code: add it to the RADIUS dictionary.

```
VENDOR Arista 30065
BEGIN-VENDOR Arista
ATTRIBUTE Arista-AVPair 1 string
END-VENDOR Arista
```

To specify role for a user

```
"bob"  Cleartext-Password := "Pa$sW04d"
    Arista-AVPair = "shell:cvp-roles=network-admin",
    Service-Type = NAS-Prompt-User
```

#### TACACS+

For TACACS+ there is no vendor specific code, just different strings.

**Note**
CloudVision support for TACACS+ servers can be affected with the setting of the “service” parameter. Some TACACS servers may require “service = shell” instead of “service = exec” in the TACACS+ configuration (**tacacs.conf**).

This example configures user “bob” in the admin group and specifies certain attributes. It specifies a "cvp-roles" attribute for the CloudVision role name (it can also be a list of roles).

```
A. tacacs.conf
    group = admingroup {
        default service = deny
        service = exec {
            default attribute = permit
            priv-lvl = 15
            cvp-roles = network-admin
        }
        enable = nopassword
    }
    user = bob {
        login = cleartext "secret"
        member = admingroup
    }

B. CVP AAA settings
C. Switch AAA configlet
```
CISCO ACS

To ensure that authentication and authorization work properly, complete the following procedures.

- Creating Identity Groups and Users
- Creating a Shell Profile using ACS on page 295
- Creating and Modifying Access Policy on page 295

Creating Identity Groups and Users

Step 1 Select Users and Identity Stores, and then select Identity Groups.
Step 2 Make sure a group named <user-group> exists. If this group does not exist, add it.
Step 3 Add new users under the group named <user-group>.

Creating a Shell Profile using ACS

Step 1 Go to the Policy Elements page.
Step 2 Select Device Administration > Shell Profiles.
Step 3 Click the Create button to create a new shell profile.
Step 4 Select the Custom Attributes tab, and then add a new mandatory attribute named “cvp-roles”.
Step 5 Specify one or more of the following values to the new “cvp-roles” attribute:
  - network-admin
  - network-operator

Note
If you have created custom role(s) under CVP Account Management, you can use them.

Step 6 Check to make sure that under the “Common Tasks Attributes” table, “Assigned Privilege Level” and “Max Privilege Level” are added by default with and the specified value is 15. Also, verify that requirement is set “Mandatory.”

Creating and Modifying Access Policy

Step 1 Go to the Access Policies section and select the Default Device Admin policy.
Step 2 Make sure that “Allow PAP/ASCII” option in the Authorization section is enabled (selected).
Step 3 In the Authorization section, create a new rule named “Rule-1”.
Step 4 Make sure that the status of the new rule (“Rule-1”) is Enabled, and set the identity group as “<user-group>”.
Step 5 Select the shell profile that outlines the cvp-roles for all users under the group named <user-group>.

Note
Alternatively, you can set add shell profile in the “default rule” section.

Step 6 Make sure that “Service Selection Rules” (under the “Access Policies” section), is using the policy named “Default Device Admin”. The policy should be listed in the “Results” column of “Service Selection Policy” table, and the “status” column should be green, indicating that the policy is enabled.
The shell profile should be automatically applied to all users under the ground named <user-group>.

14.2.2.2 Supported TACACS Types

CloudVision Portal (CVP) supports different types of TACACS. Table 14-2 on page 296 lists the supported types of TACACS, including the following information for each TACACS type:

- Supported version
- Service shell (whether it is supported for each type)
- Service exec (only the following attributes are supported):
  - acl
  - default
  - double-quote-values
  - message
  - optional
  - protocol
  - return
  - script
  - set

<table>
<thead>
<tr>
<th>TACACS Type</th>
<th>Supported Version</th>
<th>Service Shell</th>
<th>Service Exec</th>
</tr>
</thead>
<tbody>
<tr>
<td>tac_plus (Shruberry)</td>
<td>F4.0.4.26</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>tac_plus (Probono)</td>
<td>201706241310</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>201503290942/DES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CISCO ACS</td>
<td>4.4.0.46</td>
<td>Supported</td>
<td>Not Applicable</td>
</tr>
<tr>
<td></td>
<td>5.3.0.40</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related topics:
- Access to the Access Control Page on page 290
- Adding AAA Servers on page 292
- Removing AAA Servers on page 296

14.2.3 Removing AAA Servers

Complete these steps to remove AAA servers:

**Step 1** Navigate to the Access Control page.

**Step 2** Select required options from Authentication source and Authorization source drop-down menus.

The systems lists all current servers.

**Step 3** Select required servers for removal.

**Step 4** Click Remove Server(s) at the upper right corner of the Servers section. See Figure 14-8.
The system prompts to confirm deletion.

**Figure 14-8: Remove AAA Servers**

Step 5  Click **Delete**.

The system deletes selected AAA servers.

**Related Topics:**
- Access to the Access Control Page on page 290
- Adding AAA Servers on page 292
- Modifying AAA Servers on page 293

### 14.3 About Users and Roles

Account management is based on users and roles. In the CloudVision Portal, users and roles have specific meaning.

| Users          | A user is a person who uses the CVP application and is authenticated by the system through the use of account credentials (username and password), which is maintained by CVP or external enterprise servers. Only the users with account management module credentials (Account management administrator) can create and manage users.  
|                |  
|                | The account management administrator specifies the authentication credentials, name and contact information, status, and CVP permissions when creating user accounts for new users.  
|                | Account management administrators control which CVP modules users are authorized to use by assigning roles to users (the role assignments can be changed as needed at any time).  
|                | **Note**  
|                | Activity of CVP users is logged and can be viewed in the Audit Logs page. |
| Roles          | A role is a set of read and write module permissions that defines user authorization to modules in CloudVision Portal. The account management administrator specifies the read and write permissions of each module when they create roles. Only account management administrators can create and manage roles.  
|                | Roles enable account management administrators to efficiently manage user permissions by assigning roles to users, and by changing the role assigned to users.  
|                | CloudVision Portal provides two default roles, one for the system administrator (network-admin) and one for a basic operator (network-operator). |
14.3.1 Default Roles

CloudVision Portal provides two default roles. These default roles can be assigned to users as needed.

<table>
<thead>
<tr>
<th>Role</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-admin</td>
<td>A user with the default “network-admin” role has read and write permissions for all CVP modules. In addition, this role has both device-level write permissions and database-level write permissions.</td>
</tr>
<tr>
<td>network-operator</td>
<td>A user with the default “network-operator” role has only read permissions for all CVP modules. Users with this role cannot make changes to the CVP database.</td>
</tr>
</tbody>
</table>

Note

The read and write permissions cannot be changed for the default roles. But, custom roles can be created where read and write permissions can be modified.

For more information, see Managing User Roles on page 301.

14.4 Managing User Accounts

The system uses the following functionalities to manage user accounts:

- Adding New User Accounts on page 298
- Modifying User Accounts on page 300
- Removing User Accounts on page 300

14.4.1 Adding New User Accounts

When you create a new user account, you specify the login information (authentication credentials) of a person that needs to use one or more CVP modules. Personal information for the new user account is optional and can be specified when you create the new user or at a later time.

By default, new user accounts are enabled. The new user is able to use the CVP modules they are permitted to use, based on the role assigned to them. If you do not want the new user to use CVP at this time, select the Disable option (a Status option). You can enable the user account at a later time.

Note

As an alternative to creating user accounts in CVP, you can point CVP to an external AAA server that automatically creates users and maps them to roles during first login.

Complete these steps to create a new user:

**Step 1** Navigate to the **Access Control** page.

**Step 2** Under **Access Control** in the left menu, click **Users**.

The Users page lists all current users. See Figure 14-9.
Figure 14-9: Users Page

Step 3  Click + New User at the upper right corner of the Users page. The system pops-up the New User window. See Figure 14-10.

Note  The New User pop-up window creates users only with the ‘Local’ authentication type.

Figure 14-10: New User Pop-Up Window

Step 4  Provide the required information in corresponding fields.

Step 5  Click Save.

The new user account is created.

Note  If the specified role is unavailable in the local CVP, then the network-operator role is automatically assigned to either the RADIUS or TACACS user. Unless you set the account status to disabled, the new user is active using CVP modules based on the role assigned to the user. If user roles conflict when multiple roles are assigned to a user account, the user role with higher privileges is applied to the user account.

Related topics:
- Modifying User Accounts on page 300
- Removing User Accounts on page 300
14.4.2 Modifying User Accounts

Modifying user accounts enables you to change the following aspects of existing user accounts:

- Login information (password)
- Contact information (email address)
- Status (enabled or disabled)
- Role(s) (the CVP role(s) assigned to the user)
- Personal information (first and last names)

**Note**

Once changes are saved, they are implemented immediately.

Complete these steps to modify a user account.

**Step 1** Navigate to the **Access Control** page.

**Step 2** Under **Access Control**, click **Users**.

**Step 3** In the **Users** page, click the edit icon available next to the corresponding user name.

The system pops-up the **Edit User** window displaying all information related to the corresponding user. See Figure 14-11.

![Edit User Pop-Up Window](image)

**Figure 14-11: Edit User Pop-Up Window**

**Step 4** Modify the required information.

**Step 5** Click **Save**.

**Related Topics:**

- Adding New User Accounts on page 298
- Removing User Accounts on page 300
- Viewing Activity Logs on page 304

14.4.3 Removing User Accounts

Complete these steps to remove a user account:

**Step 1** Navigate to the **Access Control** page.
Step 2 Under **Access Control** in the left, click **Users**.
The Users page appears and displays all current user accounts.

Step 3 Select the users for removal.

Step 4 Click **Remove User/Remove Users** at the upper right corner of the Users page. See Figure 14-12.
The system prompts to confirm deletion.

Step 5 Click **Delete**.
The system deletes selected user accounts.

Related Topics:
- Adding New User Accounts on page 298
- Modifying User Accounts on page 300
- Viewing Activity Logs on page 304

14.5 Managing User Roles
The system uses the following functionalities to manage user roles:
- Adding New User Roles on page 301
- Modifying User Roles on page 303
- Removing User Roles on page 304

14.5.1 Adding New User Roles
CloudVision Portal enables you to create new roles as needed to ensure that you are able to efficiently manage CVP user permissions. When you create a new role, you specify the read and write permissions for each CVP module.

Once a role has been created, it is automatically added to the list of Available roles, and you can assign it to users that should have the permissions defined in the role. When you assign the role to a user, they inherit the read and write permissions defined in the role.

Complete the following steps to create new roles:

Step 1 Navigate to the **Access Control** Page.
**Step 2**  Under **Access Control** in the left menu, click **Roles**.

The Roles page lists all current roles. See **Figure 14-13**.

**Figure 14-13: Roles Page**

[Image of Roles page]

**Step 3**  Click **+ New Role** at the upper right corner of the Roles page.

The system pops-up the **New Role** window. See **Figure 14-14**.

**Figure 14-14: New Role Pop-Up Window**

[Image of New Role pop-up window]

**Step 4**  Provide the required information in corresponding fields.

**Step 5**  Click **Save**.

The new role is saved to the CVP database and is available to be assigned to users.

**Note**

The roles created can be assigned to locally created users or by the external AAA server to its known users.

**Related topics:**
- Adding New User Roles on page 301
- Modifying User Roles on page 303
- Viewing Activity Logs on page 304
14.5.2 Modifying User Roles

CloudVision Portal provides the functionality required to change the permissions of an existing role. This enables you to efficiently change the permissions of all users that are assigned the role. After you modify the role, all users assigned the role inherit the read and write permissions defined in the new version of the role.

Complete the following steps to modify an existing role:

**Step 1** Navigate to the **Access Control** page.

**Step 2** Under **Access Control** in the left menu, click **Roles**.

**Step 3** In the **Roles** page, click the edit icon available next to the corresponding role name.

The system pops-up the **Edit Role** window displaying all information related to the corresponding role. See Figure 14-15.

**Figure 14-15: Edit Role Pop-Up Window**

![Edit Role Pop-Up Window](image)

**Step 4** Modify the required Information.

**Step 5** Click **Save**.

The new version of the role is saved to the CVP database.

**Note**

All users assigned the role inherit the read and write permissions defined in the new version of the role.

**Related topics:**

- Adding New User Roles on page 301
- Removing User Roles on page 304
- Viewing Activity Logs on page 304
14.5.3 Removing User Roles

Complete these steps to remove a user role:

**Step 1** Navigate to the **Access Control** page.

**Step 2** Under **Access Control** in the left menu, click **Roles**.

The Roles page lists all current user roles.

**Step 3** Select the required user roles for removal.

**Step 4** Click **Remove Role**/**Remove Roles** at the upper right corner of the Roles page. See Figure 14-16.

The system prompts to confirm removal.

**Figure 14-16: Remove User Role**

![Roles page](image)

**Step 5** Click **Delete**.

The system deletes selected user roles.

**Note** A role assigned to user(s) cannot be deleted.

**Related topics:**
- Adding New User Roles on page 301
- Modifying User Roles on page 303
- Viewing Activity Logs on page 304

14.6 Viewing Activity Logs

The **Audit Logs** page displays activity logs of user accounts and user roles.

Complete these steps to view activity logs:

**Step 1** Click the gear icon at the upper right corner of the CVP page.
**Step 2** Click **Audit Logs** on the left menu.

The system displays the **Audit Logs** page.

**Step 3** Select desired options from **View logs for** drop-down menus.

The system displays corresponding logs. See **Figure 14-17**.

**Figure 14-17: Audit Logs Page**
14.7 Access Requirements for Image Bundle Upgrades

If AAA is configured (enabled) on the switch, you must have certain access rights before you can perform image bundle upgrades on the switch.

The specific access rights required to perform image bundle upgrades when AAA is configured are:

- Config session
- Bash

The access rights to execute bash commands is required because the following bash command must be executed to upgrade image bundles:

```
bash timeout 10 sudo rm -f /mnt/flash/boot-extensions && echo -e '' > /mnt/flash/boot-extensions
```

**Note**

If AAA is enabled and you attempt to perform image bundle upgrades without having these required access rights, the upgrade will fail and the following error occurs:

```
Jul 11 11:36:45 cd342 Aaa: %AAA-4-CMD_AUTHZ_FAILED: User cvpadmin failed authorization to execute command 'bash timeout 10 sudo rm -f /mnt/flash/boot-extensions && echo -e '' > /mnt/flash/boot-extensions'
```

**Related topics:**

- Access to the Access Control Page on page 290
- Modifying AAA Servers on page 293