Enable RADIUS, LDAP and TACACS+ Support on the VCS Console

Overview

Introduction

The Videoscape Control Suite (VCS) Console is an integrated solution that allows you to efficiently manage the Explorer Control Suite (ECS) headend. Using the VCS Console, you can streamline day-to-day operations such as management of services, schedules, monitoring and software downloads, managing users and roles, using one single point of entry.

The VCS Console is traditionally deployed at sites where authentication of users is performed using credentials that are stored locally. The benefit of storing user credentials locally is that they are self-contained and do not require an external resource for user authentication. This simple method of local authentication may be appropriate and sufficient for isolated machines/networks, and for a small set of users. However, this method becomes unmanageable and cumbersome when the number of users increases. In addition, the local authentication method is inadequate when user login access controls, such as access times and authorized client/network locations, are required.

To address these issues, the VCS Console includes support for the following protocols:

- **Remote Authentication Dial In User Service (RADIUS)** — a client/server protocol that provides centralized Authentication, Authorization, and Accounting (AAA) services.
- **Lightweight Directory Access Protocol (LDAP)** — an application protocol that queries and modifies directory entries in a directory server (for example, Active Directory).
- **Terminal Access Controller Access Control System (TACACS+)** — a protocol, common in UNIX networks, that handles remote authentication and related services for networked access control through a centralized server (for example, Cisco Secure Access Control System).

This guide provides the procedures and guidelines to configure the VCS Console to enable support for RADIUS, LDAP and TACACS+.

Purpose

The purpose of this guide is to provide system administrators with procedures and guidelines to enable RADIUS, LDAP and TACACS+ support on the VCS Console.

Important: This guide does not provide instructions for customizing advanced features of RADIUS, LDAP and TACACS+ nor does it cover procedures for various directory servers.

Audience

This document is written for system operators who are responsible for managing the VCS Console version 4.0.19 or later on ECS 3.0 or later. Our engineers may also find this document to be useful.

Required Skills and Expertise

System operators or engineers who manage the VCS Console need the following skills:

- Advanced knowledge of Linux
  - Some system configuration files are edited using the Linux vi editor. The Linux vi editor is not intuitive. The instructions provided in this guide are no substitute for an advanced working knowledge of vi.
- Extensive knowledge of the ECS system and the VCS Console
- Extensive knowledge of either the RADIUS, LDAP or TACACS+ protocol
- Extensive knowledge about creating groups, accounts, policies and attributes on directory servers (for example, Active Directory)

Document Version

This is the first formal release of this document.

Enable RADIUS Support

This section provides the steps to configure the VCS Console Web UI to use RADIUS authentication for user logins.

Prerequisites for Configuring RADIUS Authentication

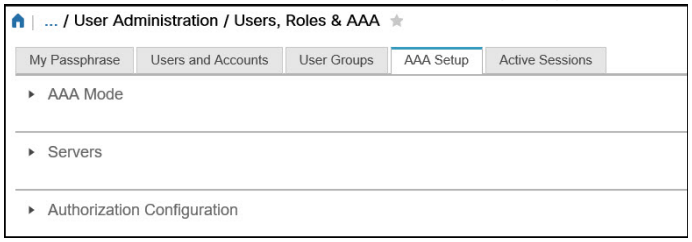
You must meet the following prerequisites before configuring RADIUS authentication for the VCS Console Web UI.

- VCS Console is running and web access is working as expected
- You have verified network connectivity between the VCS Console and the RADIUS server
- You have a RADIUS user account
- You have obtained the following information from your network administrator:
  - RADIUS server IP address
  - RADIUS authentication port number
  - RADIUS shared secret

Configuring RADIUS Authentication on the VCS Console Web UI

Complete the following steps to configure RADIUS authentication on the VCS Console.

1. From a Web browser, log into the VCS Console with a **root** user account. The Home page opens and lists the status of the server instances.
2. Click the **Navigation** icon,  , and then select **Console Admin > Users, Roles & AAA**. The My Passphrase view opens by default.
3. Click the **AAA Setup** tab. The following page opens.



4. Click the dropdown arrow next to **Servers**.
5. Maintain the **RADIUS** tab view and click the + icon. The Add Radius Server page opens.

6 Update the following fields:

- **Server Address** — enter the IP address of the RADIUS server
- **Authentication Port** — enter the authentication port of the RADIUS server. This is typically port 1812
- **Shared Secret Format** — select the appropriate format type for the shared secret

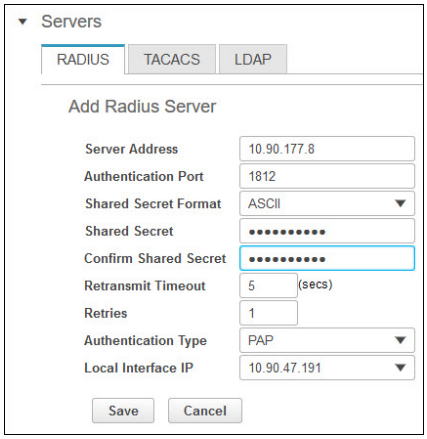
  Note: The default is ASCII.
- **Shared Secret** — enter the shared secret key defined on the RADIUS server

  Important: The shared secret you enter here must match the shared secret configured on the RADIUS server.
- **Confirm Shared Secret** — re-enter the shared secret key
- **Retransmit Timeout** — define the maximum amount of time, in seconds, that the VCS Console will wait for an authentication response from the TACACS server before timing out

  Note: The default value is 5 and the valid range is between 2 and 15.
- **Retries** — define the number of times the VCS Console will attempt to connect to the RADIUS server

  Note: The default is 1 and the valid range is 1 through 3.
- **Authentication Type** — select PAP (Password Authentication Protocol)
- **Local Interface IP** — enter the virtual IP address (VIP) of the VCS Console

Example:



7 Click **Save**. A "RADIUS server added successfully" message appears in the lower, right corner of the window.

8 Click the **RADIUS** tab again to view the new RADIUS server.

Configuring Authorization for RADIUS on the VCS Console

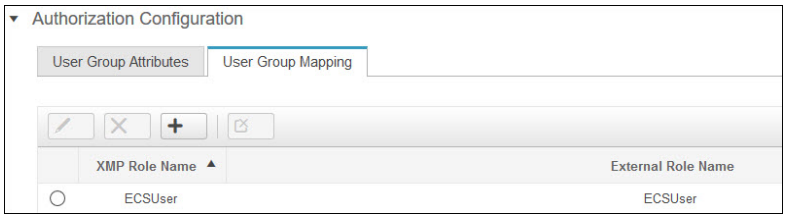
The Authorization Configuration options allow you to define which attributes the RADIUS server will send group information for the authenticated user. Complete the following steps to create a new user group mapping between the VCS Console and the RADIUS server.

Important: If necessary, you can add a new user on the VCS Console and assign it to any of the existing groups.

1. From the **Users, Roles & AAA > AAA Setup** window, click the dropdown arrow next to **Authorization Configuration**. The User Group Attributes page opens by default.
2. In the **Radius User Group Attribute** text box, enter an attribute type in which RADIUS will send information about the authenticated user. The default entry is **role**.
3. Did you edit the attribute?
   - If **yes**, click **Save**. A "Data Saved Successfully" message appears in the lower, right corner of the window.
   - If **no**, go to the next step.
4. Click the **User Group Mapping** tab.
5. Click the + icon to add a new user group mapping. The Add Mapping window opens.
6. From the **Xmp Role** text box, type the role associated with the VCS Console that you want to map to the external role.
7. From the **External Role** text box, type the name of the external role (for example, the role on the RADIUS server) that you want to map to the Xmp role.

   Note: If needed, consult with your network administrator to obtain this value.
8. Click **Add**. A "User Group Mappings Data Saved Successfully" message appears in the lower, right corner of the window.
9. Click **Close**. The User Group Mapping page updates with the mapping you added.

   Example:



Configuring the RADIUS AAA Mode and Authorization

Complete the following steps to set up the Authentication, Authorization, and Accounting (AAA) details for RADIUS on the VCS Console.

1. From the **Users, Roles & AAA > AAA Setup** window, click the dropdown arrow next to **AAA Mode**. The AAA Mode configuration options are displayed.
2. From the **AAA Source** dropdown menu, select **RADIUS**.
3. Enable the **Fall back to local on authentication failure or no server response** option to fall back to the local VCS Console source if the external server does not respond.

   Note: This setting is optional.
4. From the **Authorization Mode** dropdown menu, select one of the following options:
   - **Local** — authorization is maintained by the VCS Console
   - **Remote** — authorization is maintained by the RADIUS server
   - **Both** — authorization is maintained by the combination of the VCS Console and RADIUS authorization and authentication information

   Example:

5. Click **Save**. An "AAA Mode Settings Saved Successfully" message appears in the lower, right corner of the window.

Updating the Client Configuration File on the RADIUS Server

The **clients.conf** file is a FreeRADIUS client configuration file that contains definitions for RADIUS clients. You must update this file with information about your VCS Console client.

Format when adding a client to the clients.conf file:

```
client [VIP/Mask bits] {
secret       = [RADIUS shared secret]
shortname           = [short alias used in place of the VIP]
}
```

1. From a terminal window, log into the RADIUS server.
2. Enter the following command to change to the **/etc/raddb** directory.

   `-bash-3.2$ cd /etc/raddb`
3. Enter the following command to open the **clients.conf** file in a text editor.

   `-bash-3.2$ vi clients.conf`
4. Go to the end of the list of clients and open a new line for your VCS Console client entry.

5 Enter the configuration data for the VCS Console client.

Example entry:

```
client 10.90.47.191/22 {
        secret          = testing123
        shortname       = private-network-8
}
```

6 Save and close the file.

Updating the Users Authorization File on the RADIUS Server

Important:

- This procedure is optional as maintaining user credentials in plain text in the users file is a security risk. Updating this file also requires a restart of the RADIUS service.
- You should be familiar with configuring the users file. If you are not, please review the man page (man 5 users) on the RADIUS server for details.

The **users** file is a user authorization file that contains a series of configuration directives (also known as attributes) used to authorize and authenticate a user login request.

Complete the following steps to add a user to the users file on the RADIUS server.

1 Enter the following command to change to the **/etc/raddb** directory.

```
-bash-3.2$ cd /etc/raddb
```

2 Enter the following command to open the **users** file in a text editor.

```
-bash-3.2$ less users
```

3 Open a line after an existing user entry in the file.

4 Add the entries for the username that you want to authenticate for access to the VCS Console.

Important: Each username entry *must* also include the following entries.

- `Cisco-AVPair += "vcsconsole:virtual-domain0=ROOT-DOMAIN"`
- `Cisco-AVPair += "vcsconsole:task[n]=GLOBAL"`

  Note: Substitute a numeric value for [n].
- For an EC entry, append "_ec" and for DTACS entry, append "_dtacs".

Note:

- This external role name can be mapped to a local role name (Xmp role name), if desired.

Example entry for user ecsuser2:

```
ecsuser2   Auth-Type := Local, User-Password == "Zaq12wsx"
        User-Name = "ecsuser2",
        Cisco-AVPair += "vcsconsole:role0=ECSUser2",
        Cisco-AVPair += "vcsconsole:role1=EC80condor_ec",
        Cisco-AVPair += "vcsconsole:role2=ec9prod1vodultra_ec",
        Cisco-AVPair += "vcsconsole:role3vodtini_ec",
        Cisco-AVPair += "vcsconsole:task0=GLOBAL",
        Cisco-AVPair += "vcsconsole:virtual-domain0=ROOT-DOMAIN"
```

5 Save and close the file.

6 Are you managing the user attributes remotely (for example, on the RADIUS server)?
   - If **yes**, go to the next step.
   - If **no**, go to Step 9.

7 Add the entries for the username that you want to authenticate for access to the VCS Console.

   Important: Each username entry *must* also include the following tasks.
   - `Cisco-AVPair += "vcsconsole:virtual-domain0=ROOT-DOMAIN"`
   - `Cisco-AVPair += "vcsconsole:task[n]=GLOBAL"`

     Note: Substitute a numeric value for [n].
   - For an EC entry, append "_ec" and for DTACS entry, append "_dtacs".

   Example entry for user ecsuser:

```
ecsuser   Auth-Type := Local, User-Password == "Zaq12wsx"
        User-Name = "ecsuser",
        Cisco-AVPair += "vcsconsole:role3=lab1dtacs51_dtacs",
        Cisco-AVPair += "vcsconsole:role2=lab1ec9_ec",
        Cisco-AVPair += "vcsconsole:role1=ec9prod1_ec",
        Cisco-AVPair += "vcsconsole:role0=ECSUser",
        Cisco-AVPair += "vcsconsole:task0=EC Alarm Summary",
        Cisco-AVPair += "vcsconsole:task1=ECS Dashboard",
        Cisco-AVPair += "vcsconsole:task2=GLOBAL",
        Cisco-AVPair += "vcsconsole:virtual-domain0=ROOT-DOMAIN"
```

8 Save and close the file.

9 Enter the following command to restart the RADIUS service.

```
sudo /etc/init.d/radiusd restart
```

Testing VCS Console Login Using RADIUS Support

1 Navigate to the VCS Console IP address from a supported web browser.

2 Enter the login credentials for an account configured on the external RADIUS server.

3 Were you able to log in successfully?
   - If **yes**, you have successfully configured RADIUS authentication for the VCS Console Web UI. Go to the next step.
   - If **no**, contact Cisco Services for assistance.

4 Navigate to the various options on the Console Admin and Control Plane and verify the options available to the specific user?

5 Are the options correct for the specific user?
   - If **yes**, you have successfully configured the attributes for this user.
   - If **no**, contact Cisco Services for assistance.

Configure LDAP Support

This section provides the steps to configure the VCS Console Web UI to use LDAP authentication for user logins.

Note: This section assumes that your network administrator has set up a user account on a directory server for use with the VCS Console.

Prerequisites for Configuring LDAP Access

You must meet the following prerequisites before configuring LDAP authentication on the VCS Console Web UI.

Note: This section assumes that your network administrator has set up a user account on a directory server for use with the VCS Console.

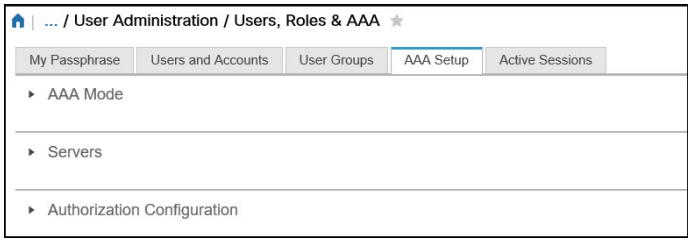
- All services on the VCS Console are running and web access is working as expected
- Network connectivity exists between the VCS Console and the LDAP server
- The LDAP server is an OpenLDAP server running version 2.4 or later
- You have obtained the following values from your network administrator:
  - LDAP user account
  - LDAP user account password
  - LDAP server IP address
  - LDAP authentication port number
  - Bind userDN
  - Bind Password
  - Server User Base
  - User Search Filter
- If you are configuring the LDAP protocol as **ldaps://** or **STARTTTLS over ldap://,** obtain the following values as well:
  - Server Root CA certificate file
  - Client certification file
  - Client key file

Configuring LDAP Authentication on the VCS Console Web UI

1 From a Web browser, log into the VCS Console with a **root** user account. The Home page opens and lists the status of the server instances.

2 Click the **Navigation** icon, , and then select **Console Admin > Users, Roles & AAA**. The My Passphrase view opens by default.

3 Click the **AAA Setup** tab. The following page opens.



4 Click the dropdown arrow next to **Servers**.

5 Click the **LDAP** tab view and then click the + icon. The Add Ldap Server page opens.

6 Update the following fields:

- **Server Address** — enter the IP address or hostname of the LDAP server
- **LDAP Protocol** — select one of the following protocols:
  - **ldap://** — all communication between the VCS Console and the LDAP server is in clear text and not considered secure
  - **ldaps://** — all communication between the VCS Console and the LDAP server is secure
  - **STARTTTLS over ldap://** — all communication between the VCS Console and the LDAP server is secure
- **Server Port** — depending on the LDAP protocol you defined, enter one of the following values:
  - **389** — for ldap:// and STARTTLS over ldap://
  - **636** — for ldaps://
- **Bind userDN** — enter the distinguished name (DN) for the user account

  Example:

  ```
  cn=hsw_lab_ldap.gen,ou=Generics,ou=Cisco
  Users,dc=cisco,dc=com
  ```
- **Bind Password** — enter the password associated with the bindDN user
- **Confirm Bind Password** — re-enter the bind password
- **Server User Base** — enter the starting point for searches

  Example:

  ```
  ou=Cisco Users,dc=cisco,dc=com
  ```
- **User Search Filter** — enter the template or attribute to use when searching for a user

  Example:

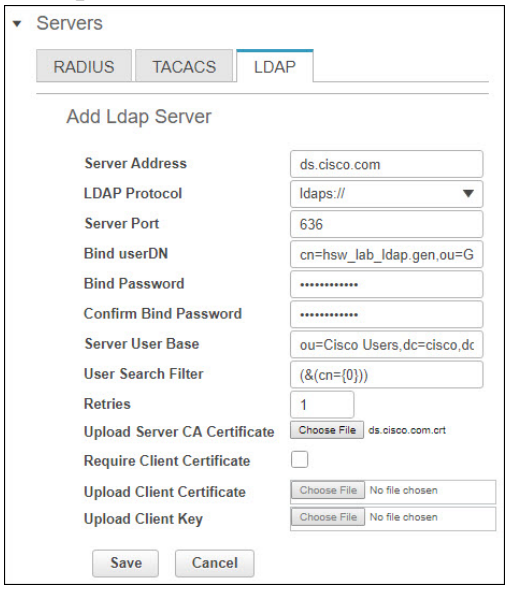
  ```
  (&(cn={0}))
  ```

  Note: You can map this entry to a user ID or an email address.

- **Retries** — define the number of times the VCS Console will attempt to connect to the LDAP server

  Note: The default is 1 and the maximum number of retries is 3.
- **Upload Server CA Certificate** — upload the LDAP CA certificate if the LDAP Protocol is set to ldaps:// or STARTTTLS over ldap://
- **Requires Client Certificate** — select this option if the client certificate and key is required
- **Upload Client Certificate** — upload the VCS Console certificate if the LDAP server requires client certificates
- **Upload Client Key** — upload the VCS Console key if the LDAP server requires client certificates

Example:



7 Click **Save**. An "LDAP server added successfully" message appears in the lower, right corner of the window.

8 Click the **LDAP** tab again to view the new LDAP server.

Configuring Authorization for LDAP on the VCS Console

Complete the following procedure to define a user group attribute and user group mapping.

Important:

- Obtain the appropriate attribute type and its associated value from your network administrator.
- If necessary, you can add a new user on the VCS Console and assign it to any of the existing groups.

1 From the **Users, Roles & AAA > AAA Setup** window, click the dropdown arrow next to **Authorization Configuration**. The User Group Attributes page opens by default.

2 In the **LDAP User Group Attribute** text box, enter the attribute type in which LDAP will send information about the authenticated user. The default attribute is **primaryGroupID**.

3 Did you edit the attribute?
   - If **yes**, click **Save**. A "Data Saved Successfully" message appears in the lower, right corner of the window.
   - If **no**, go to the next step.

4 Click the **User Group Mapping** tab.

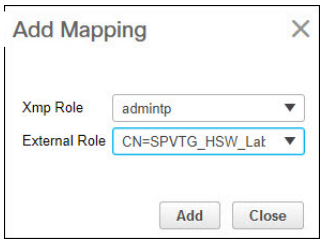
5 Click the + icon to add a new user group mapping. The Add Mapping window opens.

6 From the **Xmp Role** text box, type the role associated with the VCS Console user group that you want to map to the external role.

7 From the **External Role** text box, type the value for the external role (for example, the value for the attribute type defined in Step 2) that you want to map to the Xmp role.

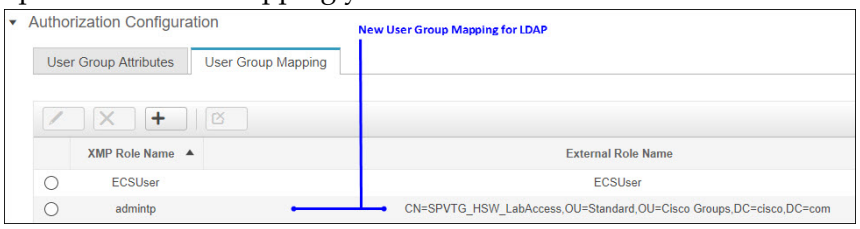
   Note: If needed, consult with your network administrator to obtain this value.

   Example:



8 Click **Add**. A "User Group Mappings Data Saved Successfully" message appears in the lower, right corner of the window.

9 Click **Close** to close the Add Mapping window. The User Group Mapping page updates with the mapping you added.



Configuring the LDAP AAA Mode and Authorization

Complete the following steps to set up the Authentication, Authorization, and Accounting (AAA) details for LDAP on the VCS Console.

1 From the **Users, Roles & AAA > AAA Setup** window, click the dropdown arrow next to **AAA Mode**. The AAA Mode configuration options are displayed.

2 From the **AAA Source** dropdown menu, select **LDAP**.

3 Enable the **Fall back to local on authentication failure or no server response** option to fall back to the VCS Console if the external server does not respond.

Note: This setting is optional.

4 From the **Authorization Mode** dropdown menu, select one of the following options:

- **Local** — authorization is maintained by the VCS Console
- **Remote** — authorization is maintained by the LDAP server
- **Both** — authorization is maintained by the combination of the VCS Console and LDAP authorization and authentication information

Example:

5 Click **Save**. An "AAA Mode Settings Saved Successfully" message appears in the lower, right corner of the window.

Testing the Connection to the LDAP Server

Complete the following steps to test the connection between the VCS Console Web UI and the LDAP server.

1. From the **Servers** area, select the check box for the LDAP server. Several buttons become active after the LDAP server is selected.
2. Click the **Test Connection** button. The LDAP Testing window opens.
3. In the **LDAP Username** text box, enter user name configured for the PC that you are using (for example, Cisco personal will enter their CEC username).
4. In the **LDAP Password** text box, type the password associated with the username.
5. Click **Test**.
6. Was the test successful?
   - If **yes**, a pop-up window indicates that the LDAP connectivity test was successful. Click **OK** and then go to the next step.
   - If **no**, contact Cisco Services.
7. Click **Cancel** to close the LDAP Testing window.
8. Navigate to the VCS Console IP address from a supported web browser.
9. Enter the login credentials for an account configured on the external LDAP server.
10. Were you able to log in successfully?
    - If **yes**, you have successfully configured LDAP authentication for the VCS Console Web UI. Go to the next step.
    - If **no**, contact Cisco Services for assistance.
11. Navigate to the various options on the Console Admin and Control Plane and verify the options available to the specific user?
12. Are the options correct for the specific user?
    - If **yes**, you have successfully configured the attributes for this user.
    - If **no**, contact Cisco Services for assistance.

Configure TACACS+ Support

Important: TACACS+ should only be configured on the VCS Console if you are using the Cisco Secure Access Control Server (ACS) server for authentication, accounting, and authorization services.

This section provides the steps to configure the VCS Console Web UI to use TACACS+ authorization and authentication services for user logins.

Note: This section assumes that your network administrator has set up a user account on the ACS for use with the VCS Console.

Prerequisites for Configuring TACACS+ Access

The following prerequisites must be met before configuring TACACS+ authentication on the VCS Console Web UI.

- VCS Console is running and web access is working as expected
- Network connectivity exists between the VCS Console and the TACACS+ server
- The ACS server includes the following items created by your network administrator:
  - TACACS+ identity group
  - TACACS+ user account
  - Custom attributes — go to ***Requirements for Custom Attributes on the ACS Server*** (on page 16) for guidance
- You have obtained the following values from your network administrator:
  - TACACS+ server IP address
  - TACACS+ authentication port
  - TACACS+ shared secret
  - TACACS+ user group attribute
  - TACACS+ (External) role name

Requirements for Custom Attributes on the ACS Server

Important: This procedure assumes the network administrator has created a shell profile on the ACS server. Complete this procedure in conjunction your network administrator.

This section includes the guidelines to create custom attributes for authorization profiles.

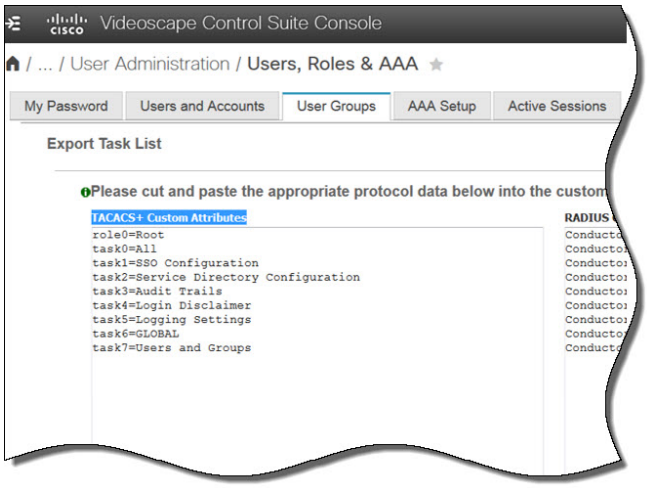
1 Log into the VCS Console as **root** user.

2 Click the **Navigation** icon, , and then select **Console Admin > Users, Roles & AAA**. The My Passphrase view opens by default.

3 Click the **Users Groups** tab.

4 Click the **Task List** link for the Group Name where the user account is a member. The Export Task List window opens.

Note: Leave this window open, as you will need to reference it later in this procedure.



5 Log in to the ACS server application.

6 Navigate to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**.

7 Click the **Custom Attributes** tab.

8 In the **Attribute** field, enter the attribute name.

Note: From the example graphic above, the first attribute is a **role**.

9 From the **Requirement** dropdown menu, enter **Mandatory**.

10 From the **Attribute Value** dropdown menu, select **Static**.

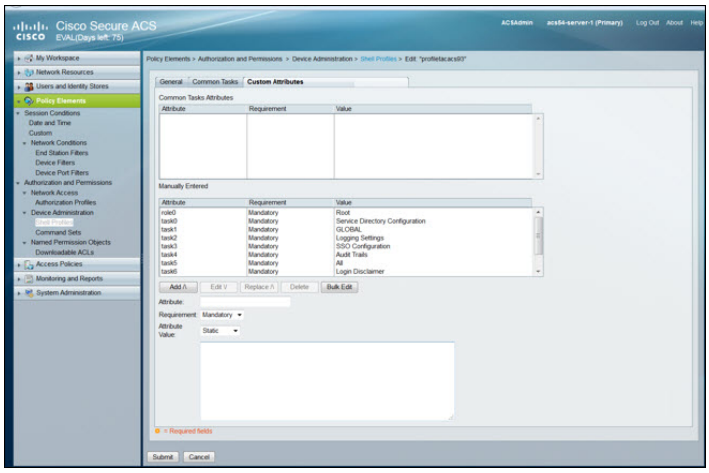
11 In the text area below the Attribute Value field, enter the value for the field.

Note: From the example graphic above, the first value is **Root**.

12 Click the **Add** button to add the entry to the table.

13 Do you need to add another attribute?
- If **yes**, repeat Steps 8 through 12.
- If **no**, go to the next step.

Example:



14 Once you have added each attribute, click **Submit**.

15 From the left area of the ACS web interface, click **Access Policies > Default Device Admin > Authorization**.

16 If desired, create authorization rules for the user.

17 Enter the following commands to restart the ACS service.

```
acs stop
acs start
```

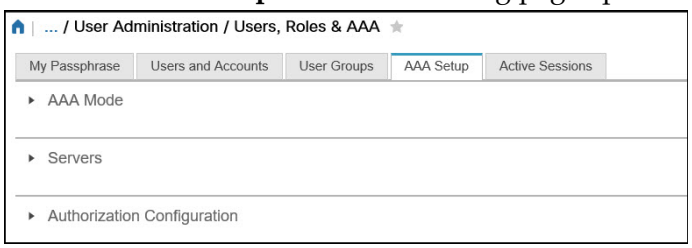
Configuring TACACS+ Authentication on the VCS Console Web UI

Complete the following steps to configure TACACS+ authentication on the VCS Console.

1 From a Web browser, log into the VCS Console with a **root** user account. The Home page opens and lists the status of the server instances.

2 Click the **Navigation** icon, , and then select **Console Admin > Users, Roles & AAA**. The My Passphrase view opens by default.

3 Click the **AAA Setup** tab. The following page opens.



4 Click the dropdown arrow next to **Servers**. The RADIUS view displays by default.

5 Click the **TACACS** tab view and then click the + icon. The Add Tacacs Server page opens.

6 Update the following fields, leaving the default values for any fields not listed below.

- **Server Address** — enter the IP address of the TACACS+ server
- **Authentication Port** — enter the authentication port of the TACACS+ server

  Note: The default port is 49.
- **Shared Secret Format** — select the appropriate format type for the shared secret

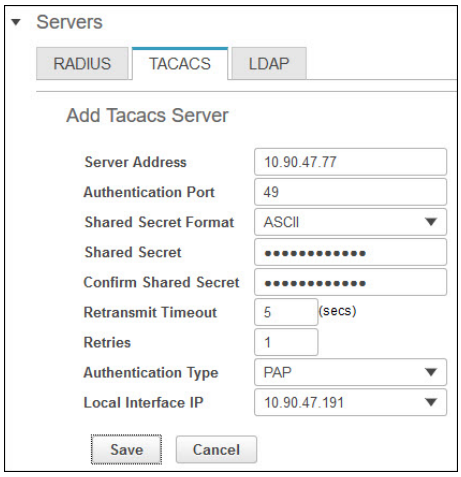
  Note: The default is ASCII.
- **Shared Secret** — enter the shared secret key defined on the TACACS+ server

  Important: The shared secret you enter here must match the shared secret configured on the TACACS+ server.
- **Confirm Shared Secret** — re-enter the shared secret key
- **Retransmit Timeout** — define the maximum amount of time, in seconds, that the VCS Console will wait for an authentication response from the TACACS+ server before timing out

  Note: The default value is 5 and the valid range is between 2 and 15.
- **Retries** — define the number of times the VCS Console will attempt to connect to the TACACS+ server

  Note: The default is 1 and the valid range is 1 through 3.
- **Authentication Type** — select PAP (Password Authentication Protocol)
- **Local Interface IP** — enter the virtual IP address (VIP) of the VCS Console

Example:



7 Click **Save**. A "TACACS+ server added successfully" message appears in the lower, right corner of the window.

8 Click the **TACACS** tab again to view the new TACACS+ server.

Configuring Authorization for TACACS+ on the VCS Console

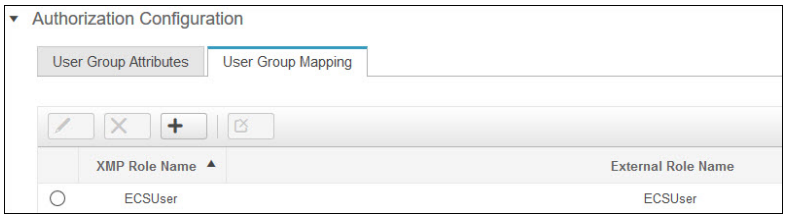
The Authorization Configuration options allow you to define which attributes the TACACS+ server will send group information for the authenticated user. Complete the following steps to create a new user group mapping between the VCS Console and the TACACS+ server.

Important: If necessary, you can add a new user on the VCS Console and assign it to any of the existing groups.

1. From the **Users, Roles & AAA > AAA Setup** window, click the dropdown arrow next to **Authorization Configuration**. The User Group Attributes page opens by default.
2. In the **TACACS User Group Attribute** text box, enter an attribute type in which TACACS will send information about the authenticated user. The default entry is **role**.
3. Did you edit the attribute?
   - If **yes**, click **Save**. A "Data Saved Successfully" message appears in the lower, right corner of the window.
   - If **no**, go to the next step.
4. Click the **User Group Mapping** tab.
5. Click the + icon to add a new user group mapping. The Add Mapping window opens.
6. From the **Xmp Role** text box, type the role associated with the VCS Console user group that you want to map to the external role.
7. From the **External Role** text box, type the name of the external role (for example, the role on the TACACS server) that you want to map to the Xmp role.

   Note: If needed, consult with your network administrator to obtain this value.
8. Click **Add**. A "User Group Mappings Data Saved Successfully" message appears in the lower, right corner of the window.
9. Click **Close**. The User Group Mapping page updates with the mapping you added.

   Example:



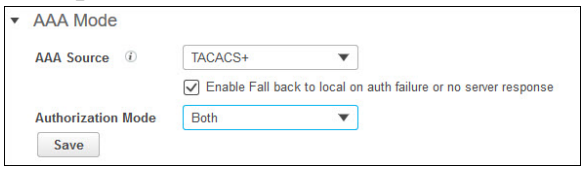
Configuring the TACACS+ AAA Mode and Authorization

Complete the following steps to set up the Authentication, Authorization, and Accounting (AAA) details for TACACS+ on the VCS Console.

1. From the **Users, Roles & AAA > AAA Setup** window, click the dropdown arrow next to **AAA Mode**. The AAA Mode configuration options are displayed.
2. From the **AAA Source** dropdown menu, select **TACACS+**.
3. Enable the **Fall back to local on authentication failure or no server response** option to fall back to the VCS Console source if the external server does not respond.

   Note: This setting is optional.
4. From the **Authorization Mode** dropdown menu, select one of the following options:
   - **Local** — authorization is maintained by the VCS Console
   - **Remote** — authorization is maintained by the TACACS+ server
   - **Both** — authorization is maintained by the combination of the VCS Console and TACACS+ authorization and authentication information

   Example:



5. Click **Save**. An "AAA Mode Settings Saved Successfully" message appears in the lower, right corner of the window.

Testing VCS Console Login Using TACACS+ Support

1. Navigate to the VCS Console IP address from a supported web browser.
2. Enter the login credentials for the account configured on the external TACACS+ server.
3. Were you able to log in successfully?
   - If **yes**, you have successfully configured TACACS+ authentication for the VCS Console Web UI. Go to the next step.
   - If **no**, contact Cisco Services for assistance.
4. Navigate to the various options on the Console Admin and Control Plane and verify the options available to the specific user?
5. Are the options correct for the specific user?
   - If **yes**, you have successfully configured the attributes for this user.
   - If **no**, contact Cisco Services for assistance.

For Information

If You Have Questions

If you have technical questions, contact Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

March 2018