Configuring Cisco Secure ACS v5.5 to use RADIUS for Orchestrator Authentication

This document outlines the procedure for configuring Cisco Secure Access Control System to provide RADIUS services for Orchestrator authentication.

- This procedure for configuring RADIUS references the ACS server’s internal user datastore.
- All names and descriptions created by the user are denoted in cyan.
- Advanced users who are familiar with the ACS RADIUS configuration tasks and only need to know the Orchestrator attributes for admin and monitor can refer to the following table:

<table>
<thead>
<tr>
<th>Dictionary Type</th>
<th>Attribute</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Radius Cisco</td>
<td>cisco-av-pair</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>Radius IETF</td>
<td>service Type</td>
<td>Enumeration</td>
</tr>
<tr>
<td>monitor</td>
<td>Radius Cisco</td>
<td>cisco-av-pair</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>Radius IETF</td>
<td>service Type</td>
<td>Enumeration</td>
</tr>
</tbody>
</table>

SUMMARY OF TASKS

1. Add Orchestrator information to Cisco’s Secure Access Control System
2. Create Identity Groups for Orchestrator’s “admin” and “monitor” users
3. Create ACS internal users for the Orchestrator
4. Define attributes for admin and monitor users for Orchestrator
5. Create access services that define policy structure and allowed protocols for admin and monitor
6. Create access rules for the services
7. Create a Service Selection Rule to parse traffic hitting the RADIUS server for appropriate action
8. Configure the Orchestrator for RADIUS authentication with Cisco Secure ACS
1 Add Orchestrator information to Cisco’s Secure Access Control System

a After logging into the Cisco Secure ACS, navigate to Network Resources > Network Devices and AAA Clients.

b Click Create.

c Click Submit. The result displays in the Network Devices table.
2 Create Identity Groups for Orchestrator’s “admin” and “monitor” users

a Navigate to Users and Identity Stores > Identity Groups, and at the bottom of the page, click Create.

To create the group for “admin”, complete the following fields:

- Name: orchestrator-admin-group
- Description: Orchestrator administrator group

b Click Submit. The new group displays under All Groups.

c Click Create.
d. Again, navigate to **Users and Identity Stores > Identity Groups**, and at the bottom of the page, click **Create**.

To create the group for “monitor”, complete the following fields:

- **Name**: orchestrator-monitor-group
- **Description**: Orchestrator monitor group

Click **Submit**. The new group displays under **All Groups**.

e. Again, navigate to **Users and Identity Stores > Identity Groups**, and at the bottom of the page, click **Create**.
3 Create ACS internal users for the Orchestrator

a Navigate to Users and Identity Stores > Internal Identity Stores > Users, and at the bottom of the page, click Create.

b To create an admin-level user for Orchestrator, complete the following fields:

Name: orchadmin
Description: Orchestrator administrator
Identity Group: [select] All Groups: orchestrator-admin-group
Password Type: Internal Users
Password / Confirm Password: [create one]
c  Click **Submit**. The new user name appears in the **Internal Users** list.

![Image of Internal Users list](image)

---

d  Click **Create**.

To create a **monitor**-level user for Orchestrator, complete the following fields:

![Image of Create user dialog](image)

- **Name**: orchmonitor
- **Description**: Orchestrator monitor
- **Identity Group**: [select] All Groups: orchestrator-monitor-group
- **Password Type**: Internal Users
- **Password / [create one]**
- **Confirm Password**:
e Click **Submit**. The new user name appears in the **Internal Users** list.
4 Define attributes for admin and monitor users for Orchestrator

a To create an admin profile, navigate to Policy Elements > Authorizations and Permissions > Network Access > Authorization Profiles, and at the bottom of the page, click Create.

b In the General tab, complete the following:

Name: RADIUS admin profile
Description: authorization profile for admin
c Click the **RADIUS Attributes** tab and complete the following:

![Cisco Secure ACS Interface](image1.png)

- **Dictionary Type:** RADIUS-Cisco
- **RADIUS Attribute:** cisco-av-pair
- **Attribute Type:** String
- **Attribute Value:** Static
- Enter this `LOGIN:priv-lvl=7`

![Entry Added](image2.png)

Click **Add**. The entry appears in the **Manually Entered** table.

Now, we'll add a second attribute.

![Add Second Attribute](image3.png)
e  In the **RADIUS Attributes** tab, complete the following:

- **Dictionary Type**: RADIUS-IETF
- **RADIUS Attribute**: Service-Type
- **Attribute Type**: Enumeration
- **Attribute Value**: Static
- **NAS Prompt**

f  Click **Add**. The entry appears in the **Manually Entered** table.
g Click **Submit**. The **RADIUS admin profile** appears in the **Authorization Profiles** list.

![Cisco Secure ACS](image)

Now, we’ll create the monitor profile.

h Click **Create**. In the **General** tab, complete the following:

- **Name:** RADIUS monitor profile
- **Description:** authorization profile for monitor
i  Click the **RADIUS Attributes** tab and complete the following:

```
Dictionary Type: RADIUS-Cisco
RADIUS Attribute: cisco-av-pair
Attribute Type: String
Attribute Value: Static

[enter this] LOGIN:priv-lvl=0
```

Notice that for the monitor, the **level equals zero**.
j  Click Add. The entry appears in the Manually Entered table.

Now, we’ll add the second attribute.

k  In the RADIUS Attributes tab, complete the following:

- **Dictionary Type**: RADIUS-IETF
- **RADIUS Attribute**: Service-Type
- **Attribute Type**: Enumeration
- **Attribute Value**: Static NAS Prompt
1. Click **Add**. The entry appears in the **Manually Entered** table.

![Configuration screen](image1)

2. Click **Submit**. The **RADIUS monitor profile** appears in the **Authorization Profiles** list.

![Configuration screen with RADIUS monitor profile highlighted](image2)
5 Create access services that define policy structure and allowed protocols for admin and monitor

a Navigate to Access Policies > Access Services, and click Create. When Step 1 - General appears, complete the following:

- **Name:** Orch-admin services
- **Description:** Orchestrator admin services for administrator
- **User Selected Service Type:** Network Access
- **Policy Structure:** Identity
- **Authentication Protocols:** Allow PAP/ASCII
- **Authentication Protocols:** Allow CHAP

b Click Next. When Step 2 - Allowed Protocols appears, select the following:

- **Process Host Lookup:** [deselect]
Click **Finish**. When asked if you'd like to activate this service, click **Yes**.

Notice that **Orch-admin services** is now listed under **Access Policies** in the navigation panel.
6 **Create access rules for the services**

These specify the conditions users must meet for access to Orchestrator.

a  Navigate to **Access Policies > Access Services > Orch-admin services > Identity**, and click **Select**.

![Access Policies Menu](image1)

![Identity Select](image2)

b  Select **Internal Users**, and click **Save Changes**.
c  Navigate to **Access Policies > Access Services > Orch-admin services > Authorization**, and click **Customize**.

The **Customize Conditions** window appears.

d  Select and move **Compound Condition** from the **Selected** column to the **Customize Conditions** column.
e Select and move **Identity Group** to the **Selected** column.

f Click **OK**. The result displays in the **Conditions** column.
g. Click **Create**. A dialog box appears.

![](image1.png)

h. Select the **Identity Group** checkbox, and click **Select**.

![](image2.png)

The **Network Device Groups** list appears.

![](image3.png)

i. Select **orchestrator-admin-group** and click **OK**. The **Rule-1** dialog returns.
j Below the **Authorization Profiles** field, click **Select**.

The **Authorization Profiles** dialog appears.

k Select **RADIUS admin profile** and click **OK**.
The input window returns.

1. Click **OK**. The **Network Access Authorization Policy** returns, with **Rule-1** included.

2. At the bottom of the page, click **Save Changes**.

3. Now you’ll add **Rule-2** to include the **RADIUS monitor profile**.
   - At the bottom of the page, click **Create**. The **Rule-2** dialog box appears.
   - Select the **Identity Group** checkbox, and click **Select**. The **Network Device Groups** list appears.
   - Select **orchestrator-monitor-group** and click **OK**. The **Rule-2** dialog returns.
   - Below the **Authorization Profiles** field, click **Select**. The **Authorization Profiles** dialog appears.
Select RADIUS monitor profile and click OK. The input window returns.

Click OK. The Network Access Authorization Policy returns, with Rule-2 included.

Click Save Changes.
7 Create a Service Selection Rule to parse traffic hitting the RADIUS server for appropriate action

a Navigate to Access Policies > Access Services: Service Selection Rules, and click Create.

A dialog appears for creating a new rule.
b Complete the following:

- Select the Protocol checkbox, and select match and Radius.
- From the drop-down list in the Service field, select Orch-admin services.
- Click OK.
  The Service Selection Policy page appears, displaying the new rule at the bottom of the list.

C Select the new rule, and click the caret to move the rule up to the appropriate priority.
d  Click **Save Changes**.

You have now finished configuring Cisco Secure ACS to use RADIUS for authenticating Orchestrator users.
8 Configure the Orchestrator for RADIUS authentication with Cisco Secure ACS

a After logging into the Orchestrator as admin, navigate to Orchestrator Administration > Authentication.

b Select RADIUS, and complete the following:

- **Authentication Order:** Remote first
- **Server IP:** [Cisco Secure ACS IP address]
- **Server Port:** 1812
- **Server Secret Key:** [Orchestrator’s shared secret]

c Click Save.

d Log out of Orchestrator.
On the welcome page, log in as `orchadmin`, the identity you created in the RADIUS server.

Orchestrator is now authenticating users via the RADIUS server.