silver peak™ | 2860 De La Cruz Boulevard, Suite 100 | Santa Clara, CA 95050 | 408.935.1800 | www.silver-peak.com

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

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

- This procedure for configuring TACACS+ 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 TACACS+ configuration tasks and only need to know the Orchestrator attributes for **admin** and **monitor** can refer to the following table:

		admin		monitor	
	Attribute	**Requirement**	**Value**	**Requirement**	**Value**
Common Tasks	Assigned Privilege Level	Mandatory	7	Mandatory	0
	Max Privilege Level	Mandatory	7	Mandatory	0
Manually Entered	role	Mandatory	admin	Mandatory	monitor

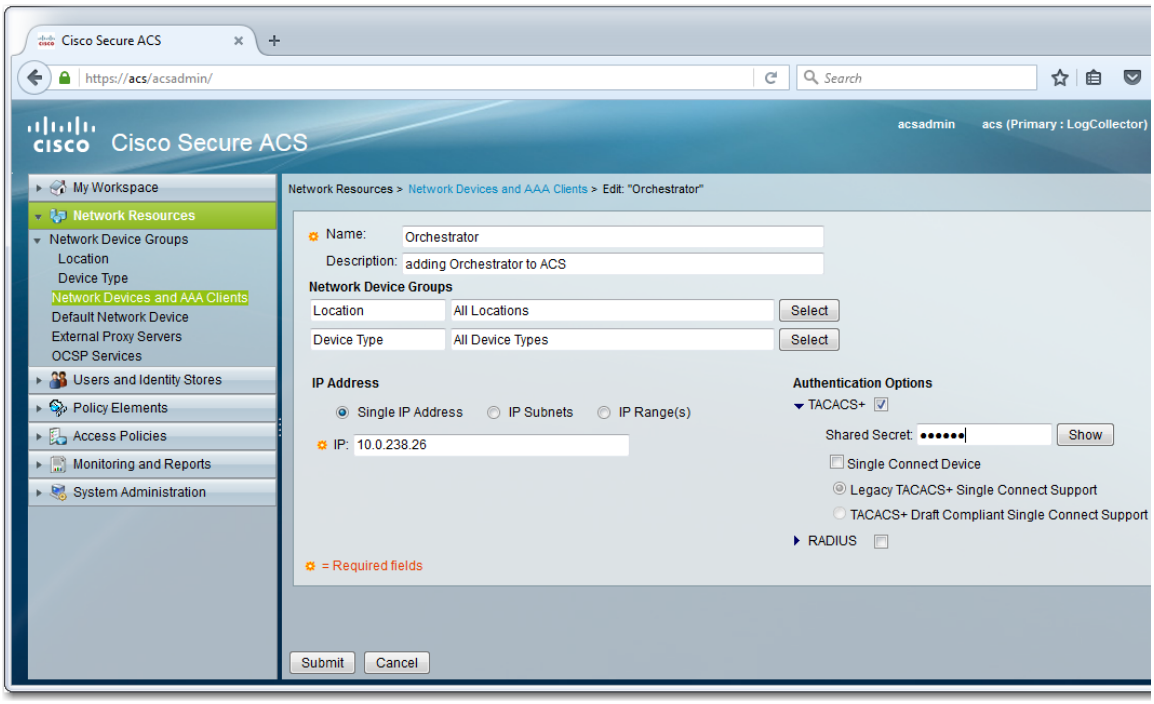
SUMMARY OF TASKS

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 TACACS+ server for appropriate action**
8. **Configure the Orchestrator for TACACS+ authentication with Cisco Secure ACS**

I 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**.

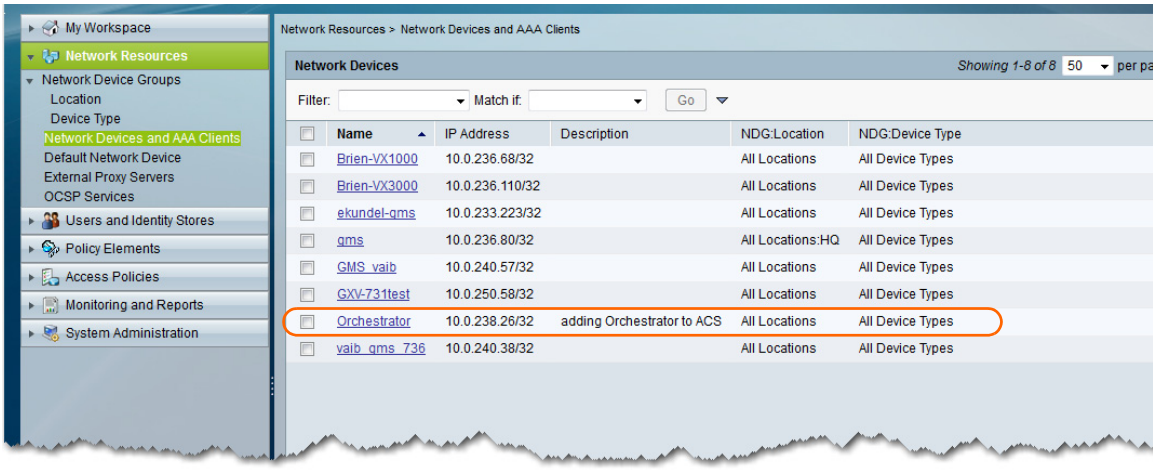
b Click **Create**.



Complete the following fields:

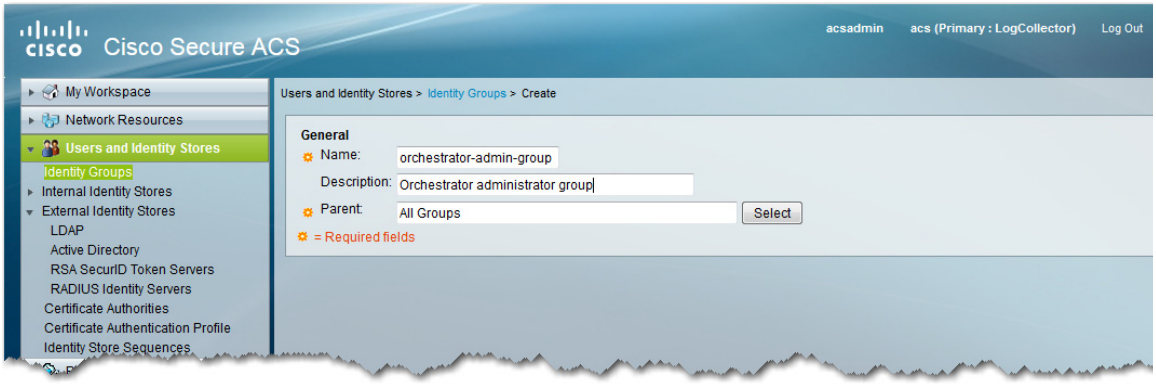
Name:	`Orchestrator`
Description:	`adding Orchestrator to ACS`
Single IP Address:	[select]
IP:	[Orchestrator IP address]
TACACS+:	[select]
Shared Secret:	[Orchestrator's shared secret]

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**.

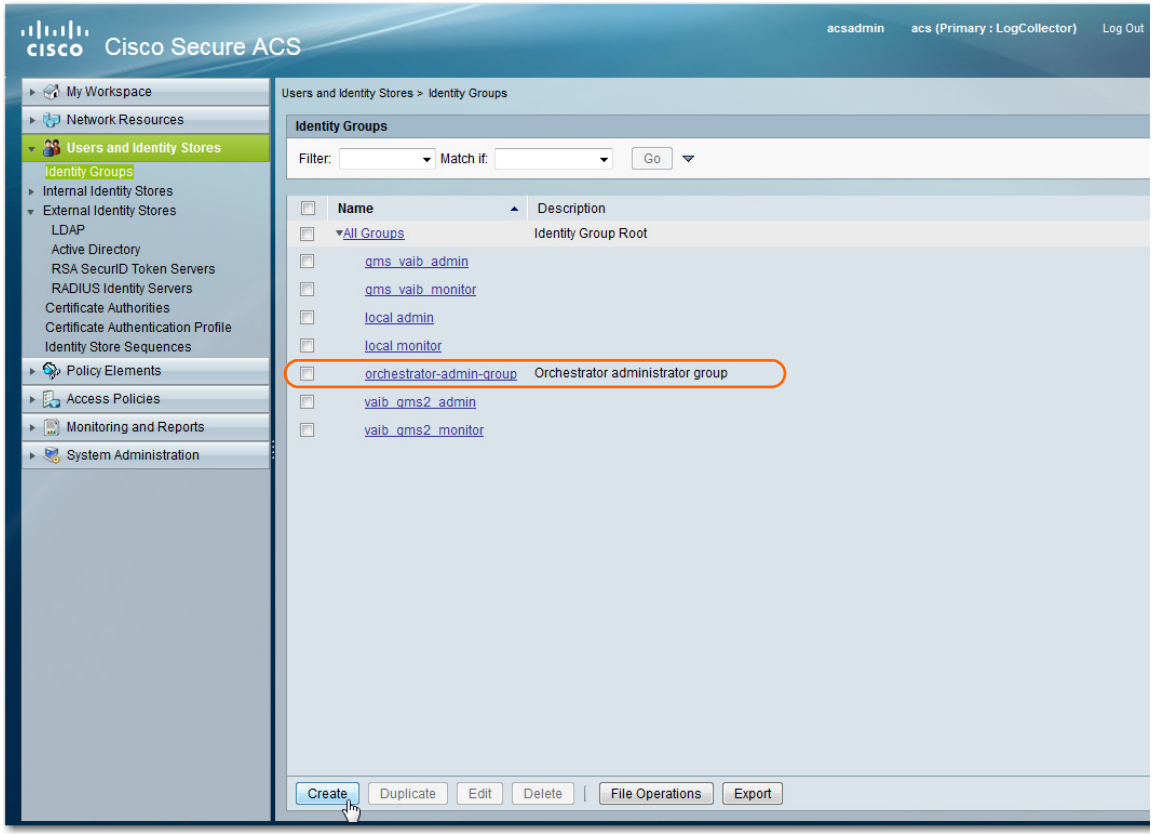


To create the group for "**admin"**, complete the following fields:

Name: `orchestrator-admin-group`

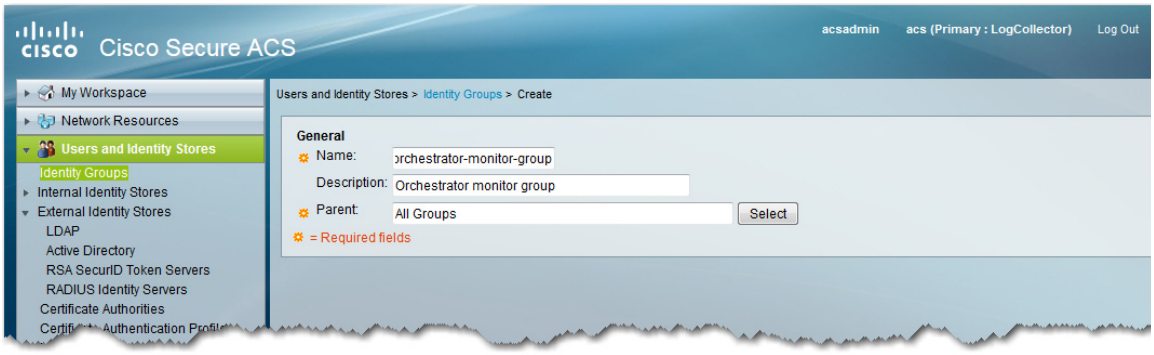
Description: `Orchestrator administrator group`

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**.

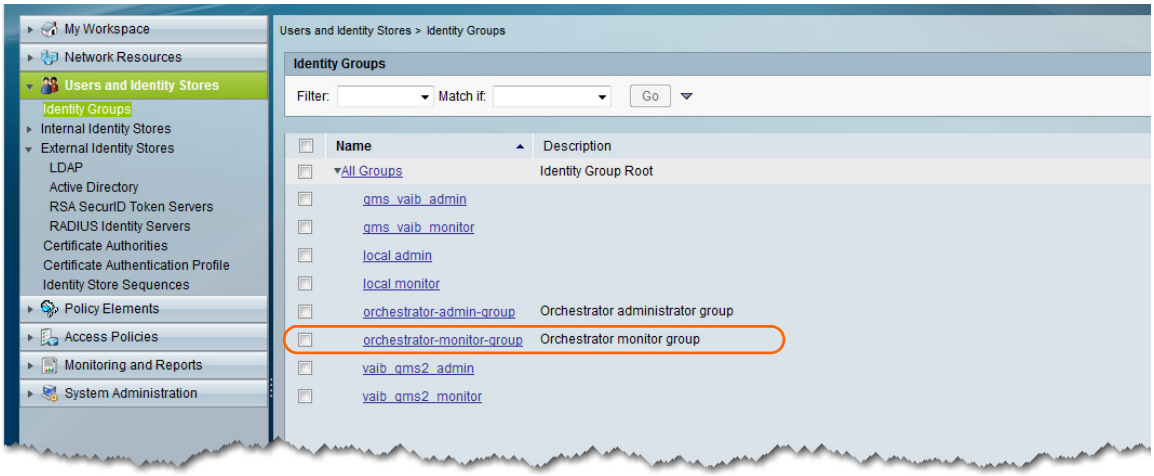


To create the group for "**monitor**", complete the following fields:

Name: `orchestrator-monitor-group`

Description: `Orchestrator monitor group`

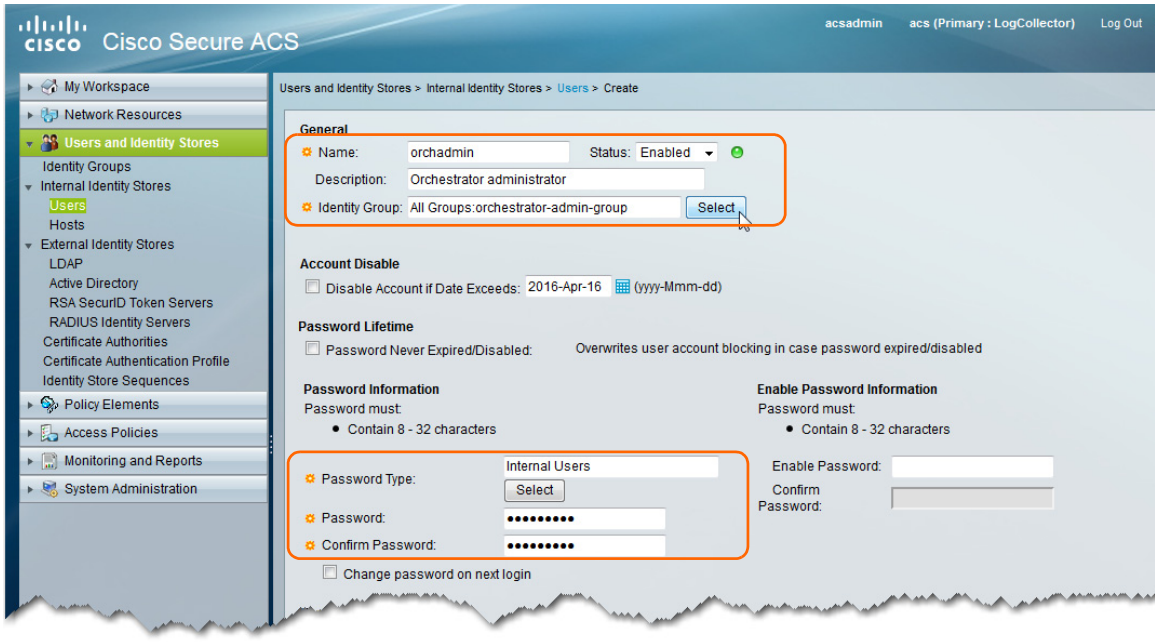
e Click **Submit**. The new group displays under **All Groups**.



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`

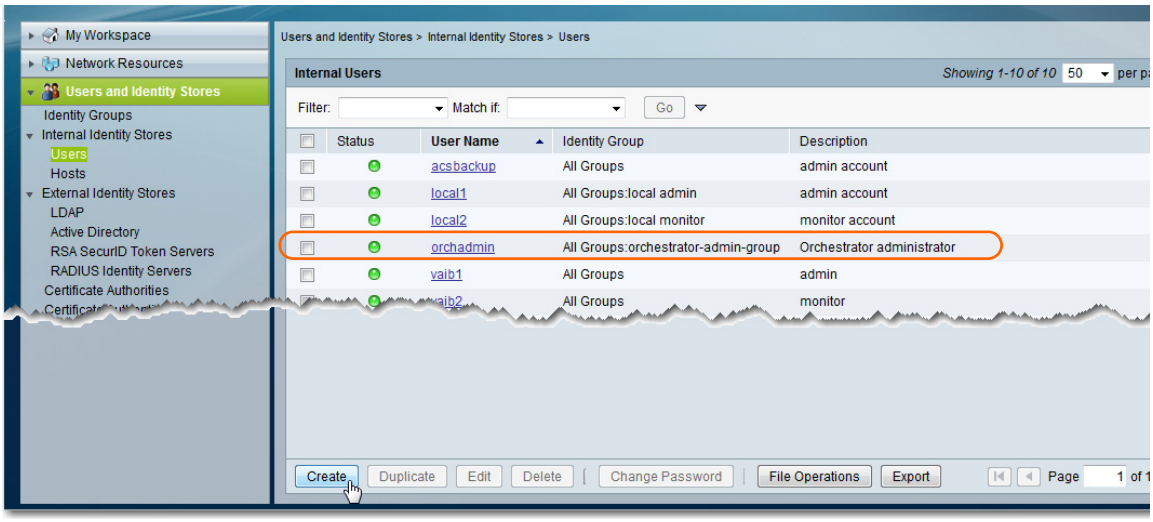
Description: `Orchestrator administrator`

Identity Group: [select] All Groups: `orchestrator-admin-group`

Password Type: Internal Users

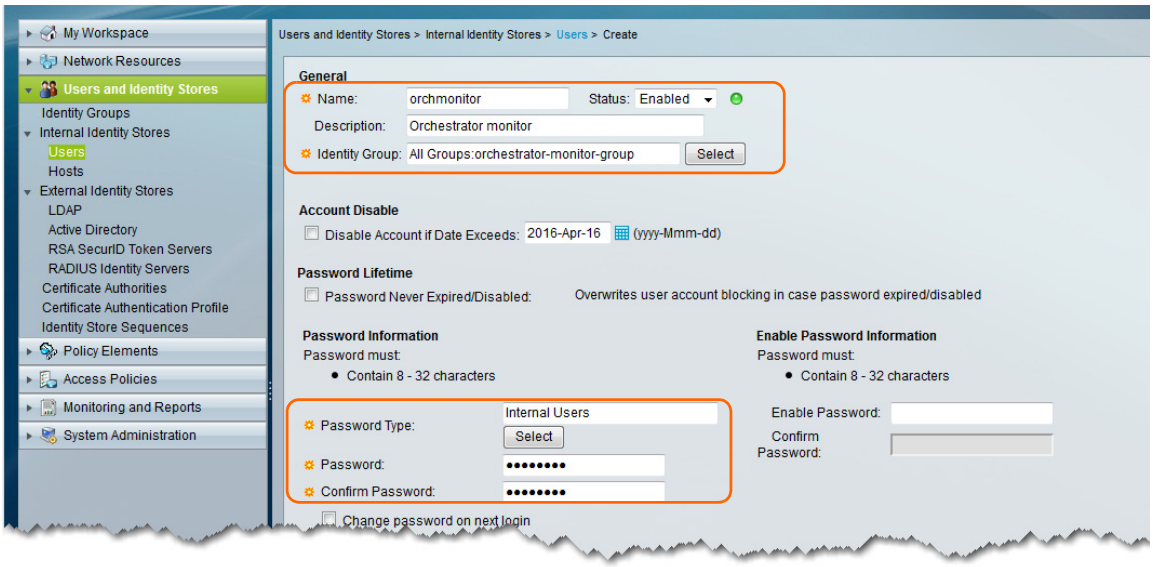
Password / Confirm Password: [create one]

c Click **Submit**. The new user name appears in the **Internal Users** list.



d Click **Create**.

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



Name: orchmonitor

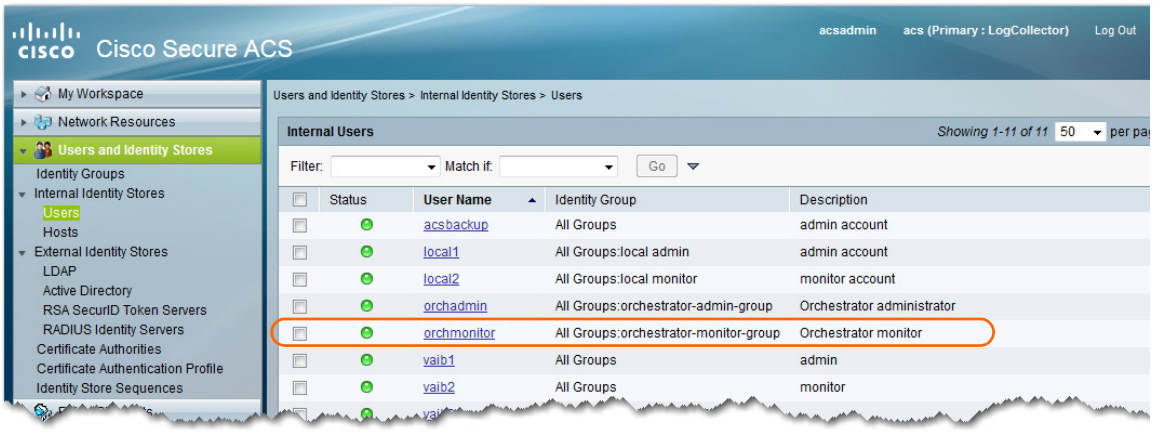
Description: Orchestrator monitor

Identity Group: [select] All Groups: orchestrator-monitor-group

Password Type: Internal Users

Password / Confirm Password: [create one]

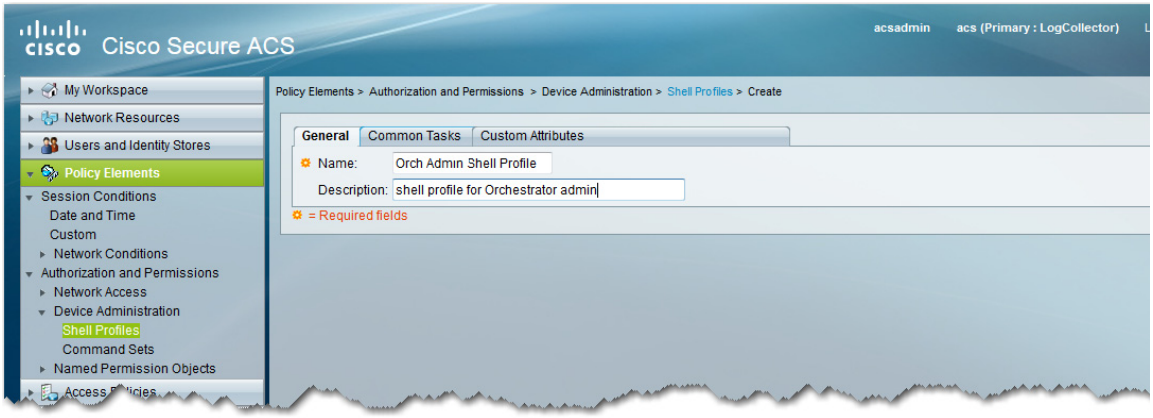
e Click **Submit**. The new user name appears in the **Internal Users** list.



4 Define attributes for admin and monitor users for Orchestrator

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

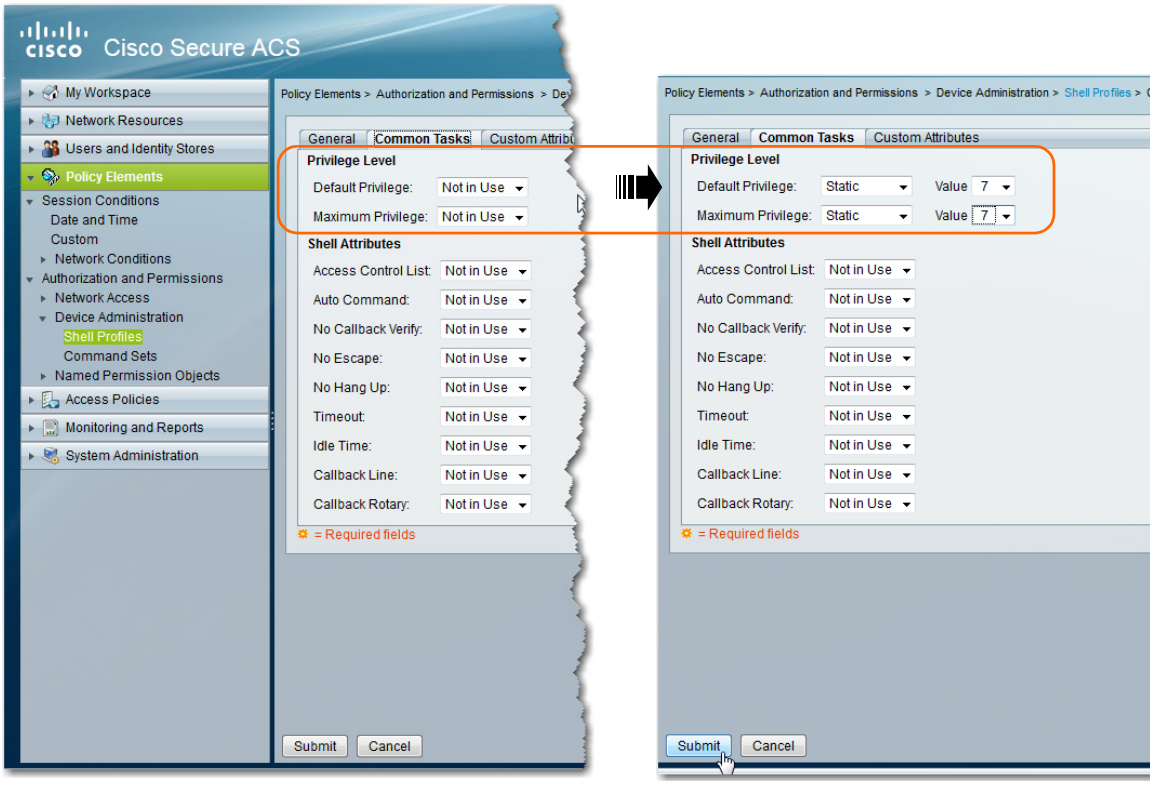
b In the **General** tab, complete the following:



Name: `Orch Admin Shell profile`

Description: `shell profile for Orchestrator admin`

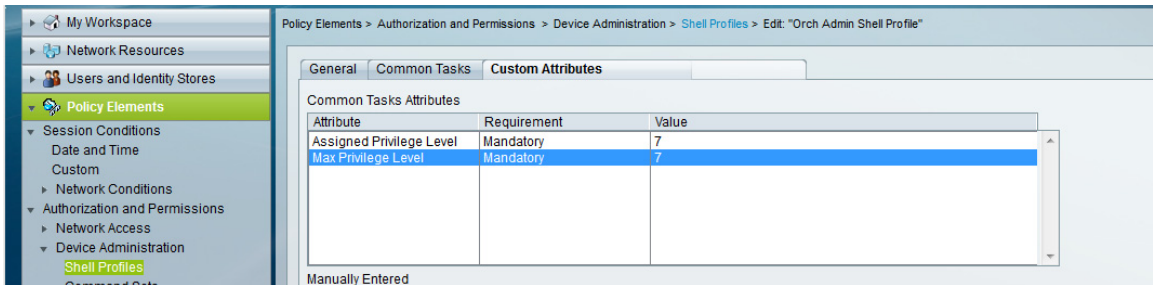
c Select the **Common Tasks** tab and set the following **Privilege Level** values:



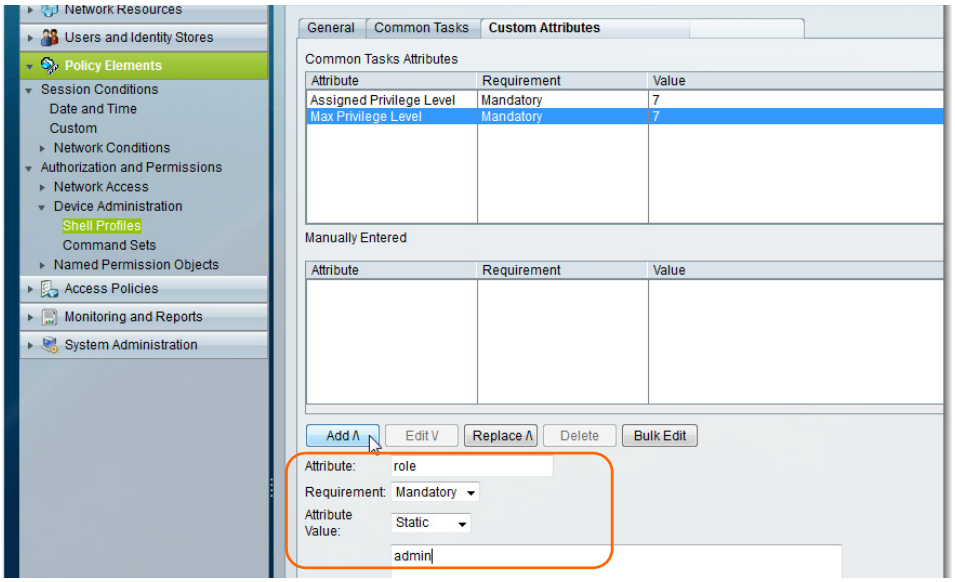
Default Privilege: Static **Value:** 7

Maximum Privilege: Static **Value:** 7

d Click **Submit**.
The **Custom Attributes** tab displays the new entries.



e In the **Manually Entered** section, complete the following:

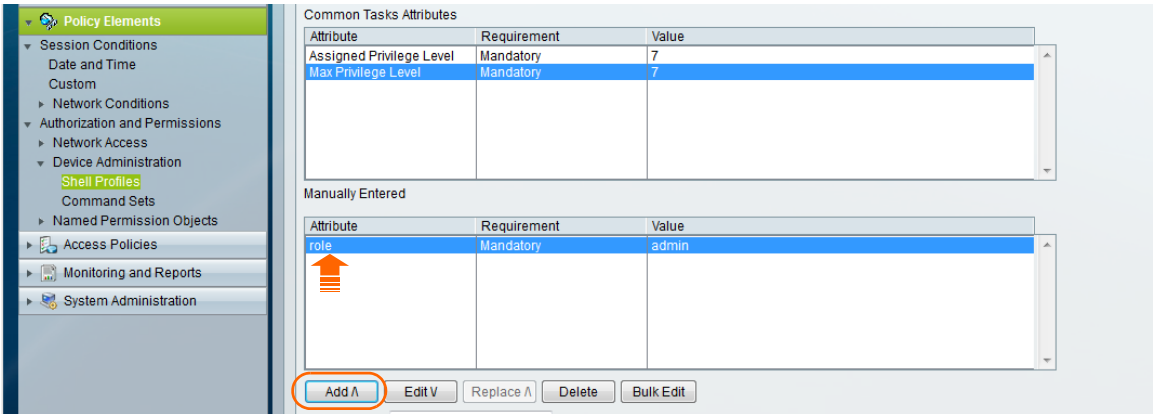


Attribute: `role`

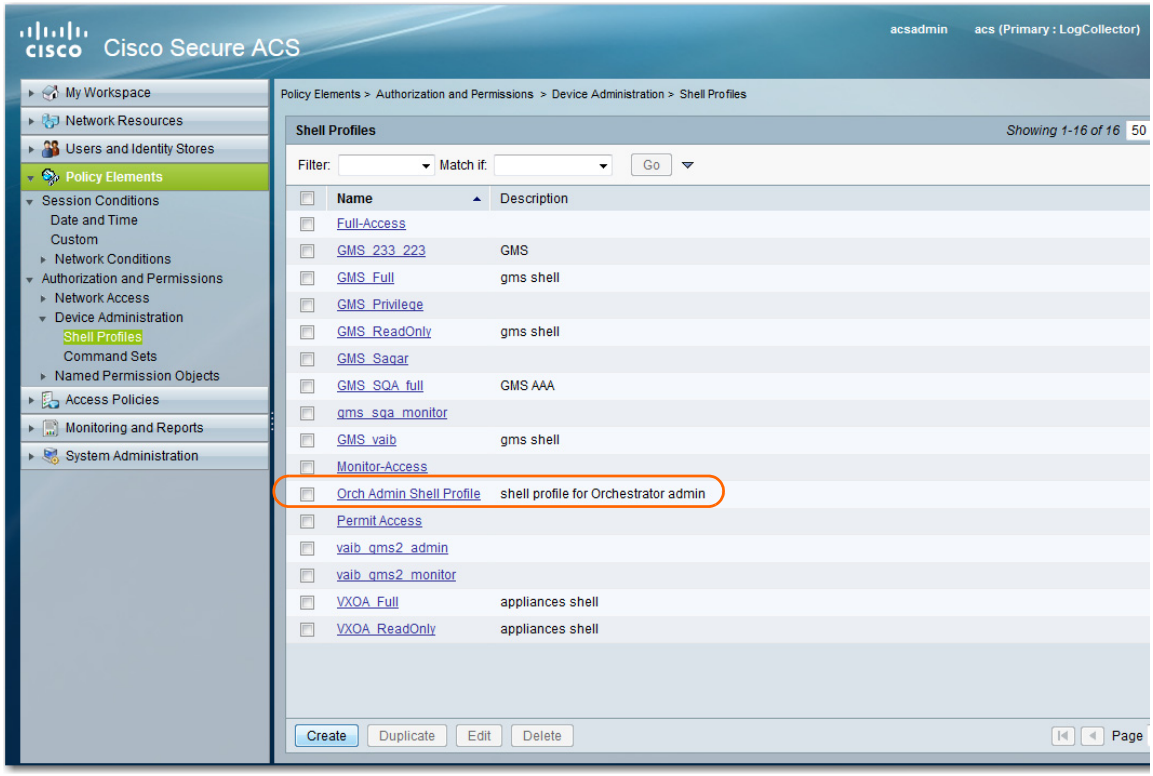
Requirement: Mandatory

Attribute Value: Static
`admin`

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

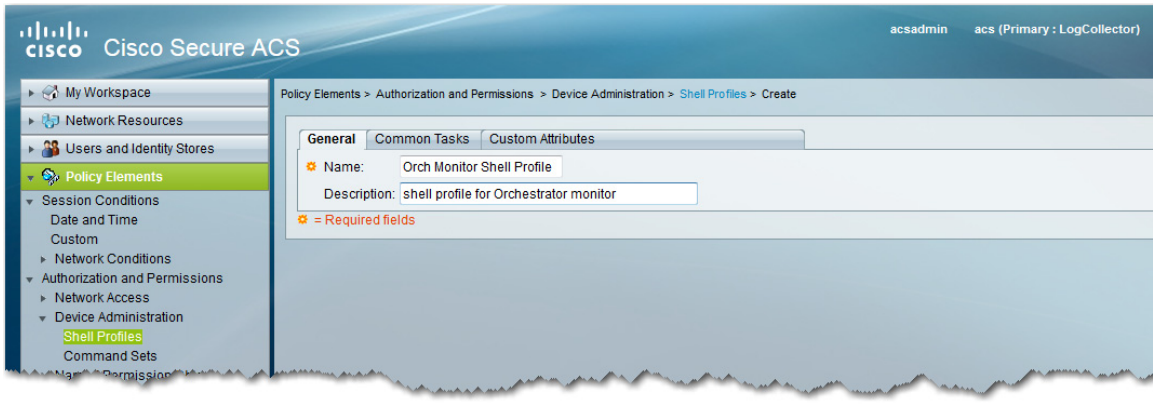


g At the bottom of the page, click **Submit**.
The **Shell Profiles** table appears and displays the new entry.



h Click **Create**.

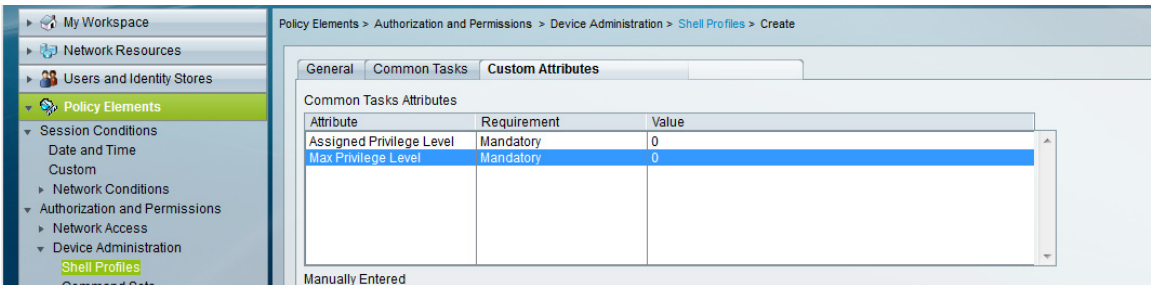
i In the **General** tab, complete the following:



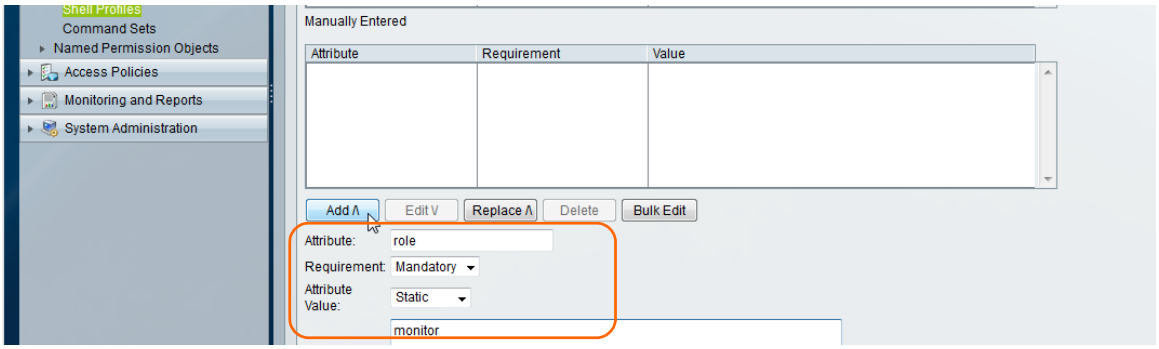
Name: `Orch Monitor Shell profile`

Description: `shell profile for Orchestrator monitor`

j Click **Submit**.
The **Custom Attributes** tab displays the new entries.



k Lower, in the **Manually Entered** section, complete the following:

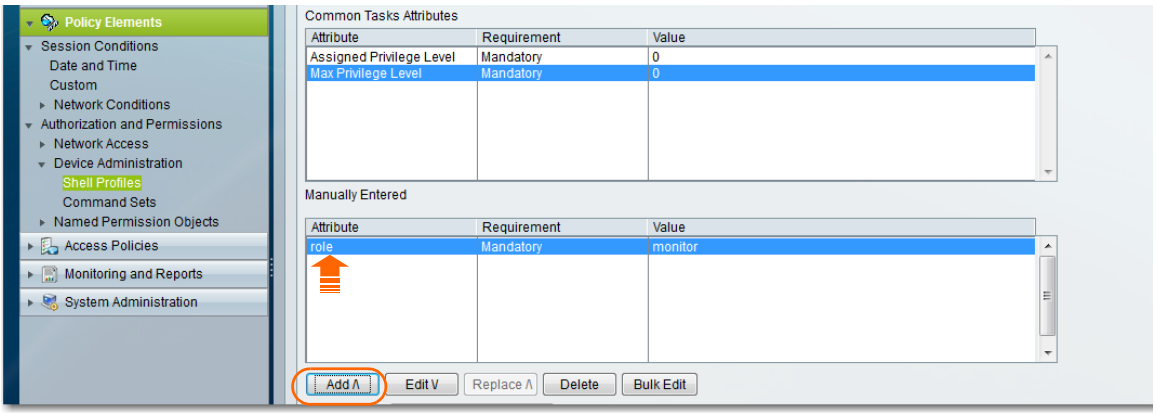


Attribute: `role`

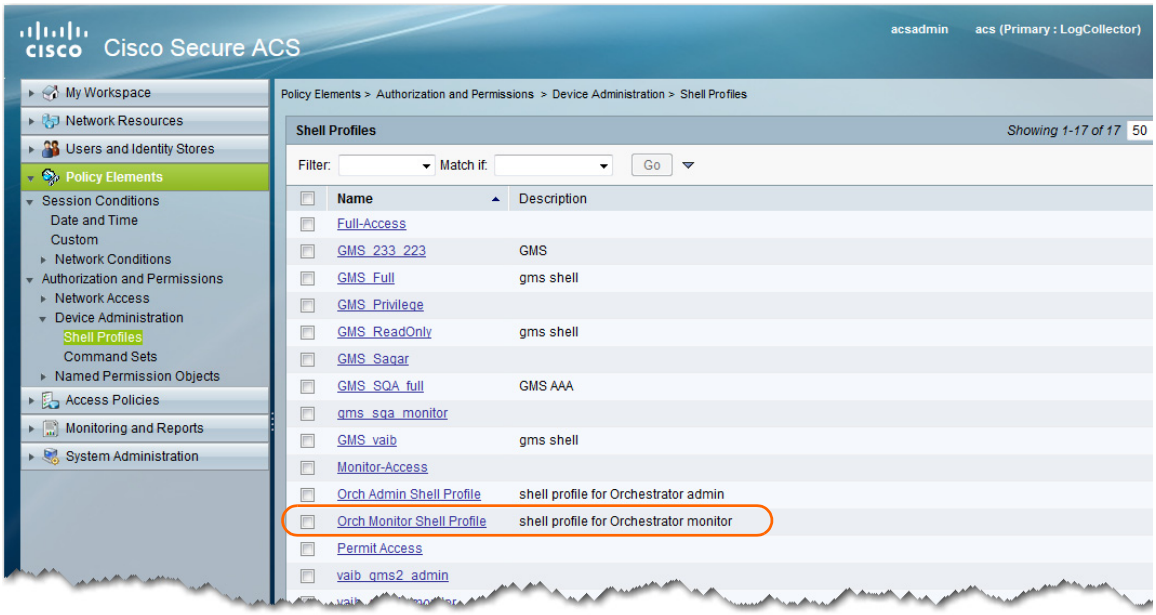
Requirement: Mandatory

Attribute Value: Static
`admin`

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

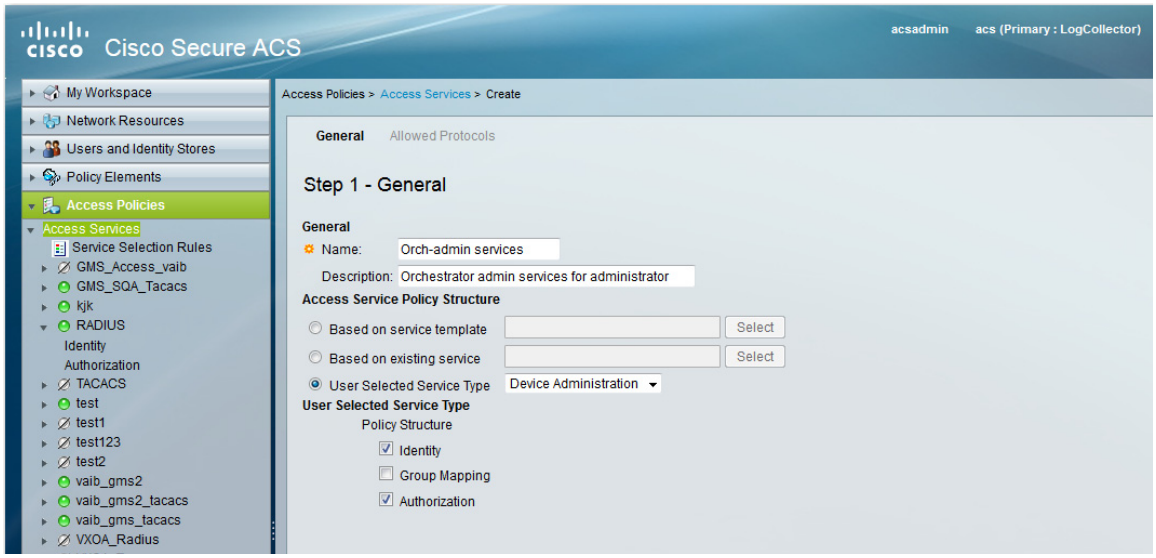


m Click **Submit**.
The **Shell Profiles** table appears, with the new entry.



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:



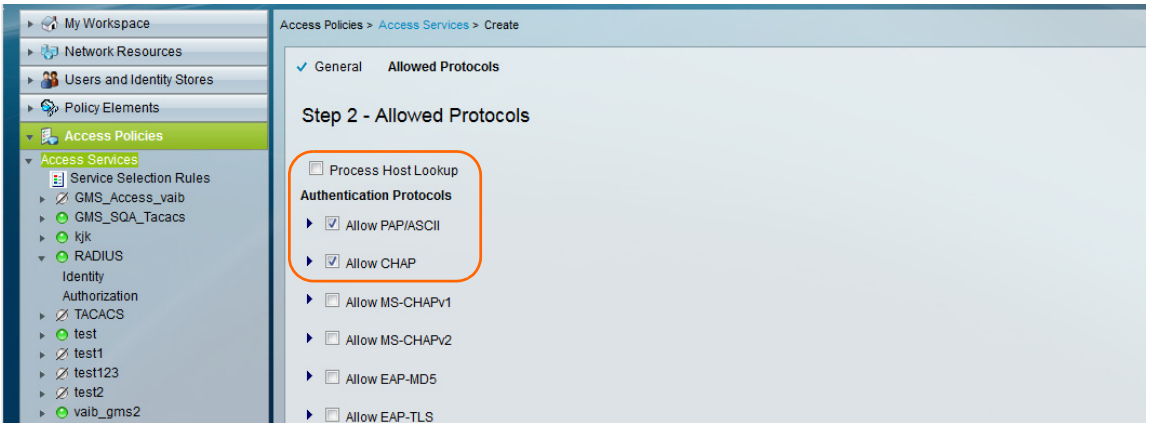
Name: `Orch-admin services`

Description: `Orchestrator admin services for administrator`

User Selected Service Type: Device Administration

Policy Structure: Identity
Authorization

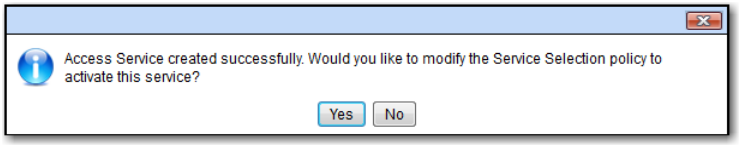
b Click **Next**. When **Step 2 - Allowed Protocols** appears, make the following changes:



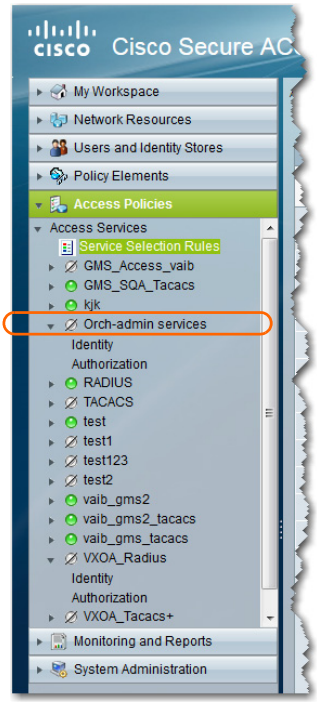
Process Host Lookup: [deselect]

Authentication Protocols: Allow PAP/ASCII
Allow CHAP

c Click **Finish**. When asked if you'd like to activate this service, click **Yes**.



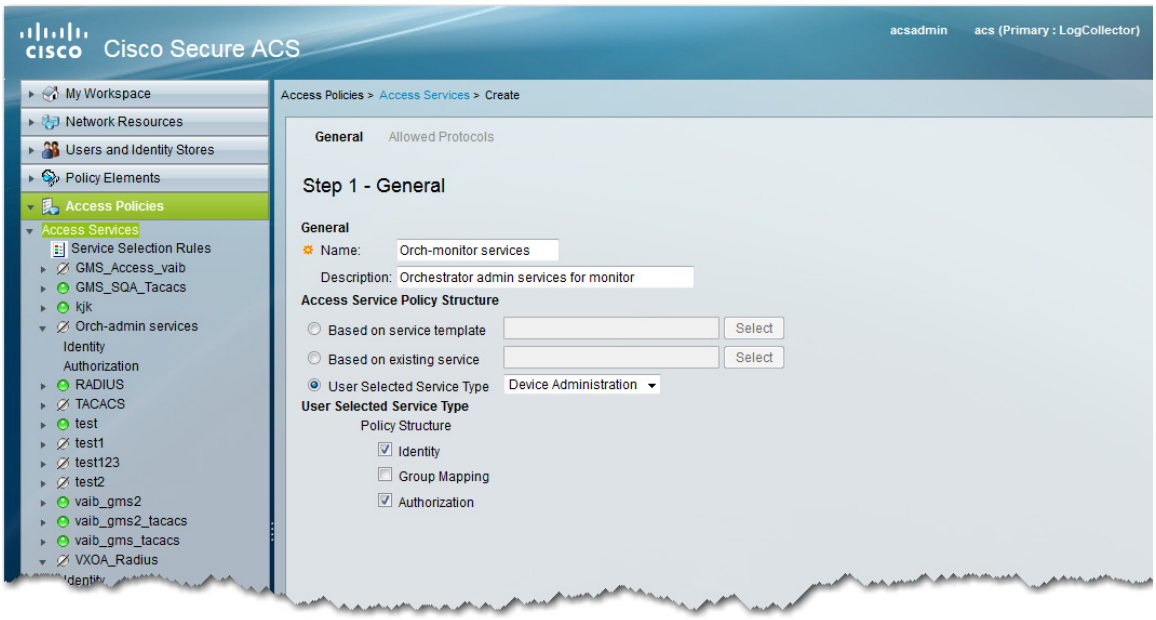
Notice that **Orch-admin services** is now listed under **Access Policies** in the navigation panel.



6 Create access rules for the services

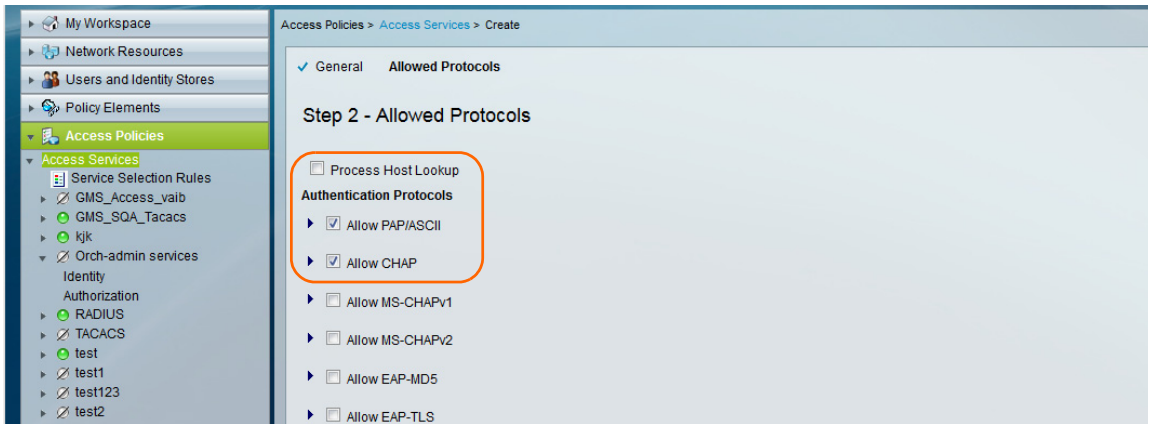
These specify the conditions users must meet for access to Orchestrator.

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



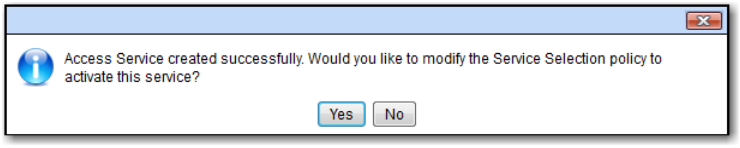
Name:	`Orch-monitor services`
Description:	`Orchestrator admin services for monitor`
User Selected Service Type:	Device Administration
Policy Structure:	Identity Authorization

b Click **Next**. When **Step 2 - Allowed Protocols** appears, make the following changes:

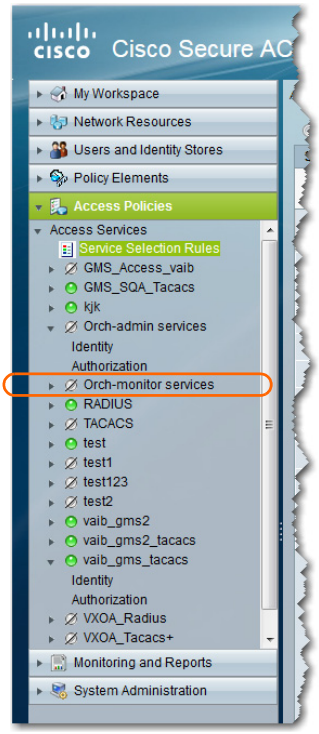


Process Host Lookup:	[deselect]
Authentication Protocols:	Allow PAP/ASCII Allow CHAP

c Click **Finish**. When asked if you'd like to activate this service, click **Yes**.

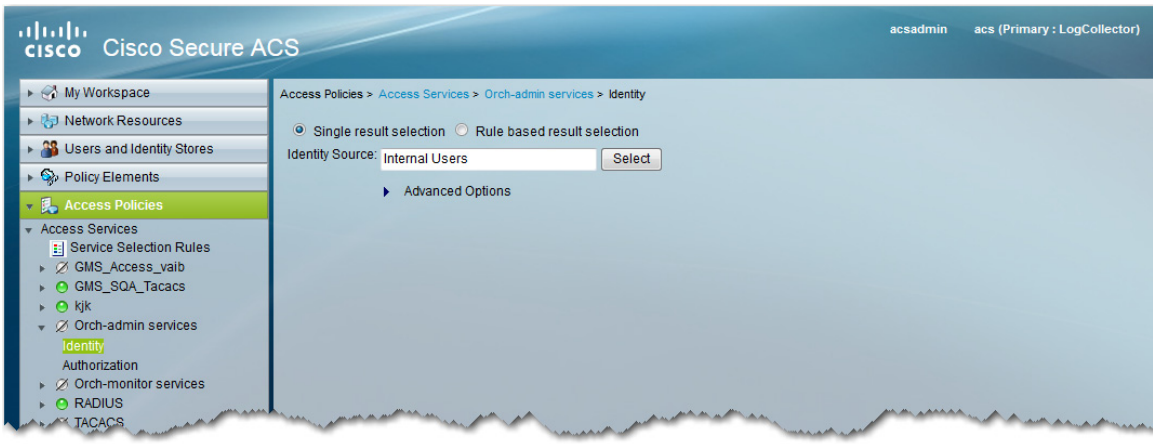


Notice that **Orch-monitor services** is now listed under **Access Policies** in the navigation panel.



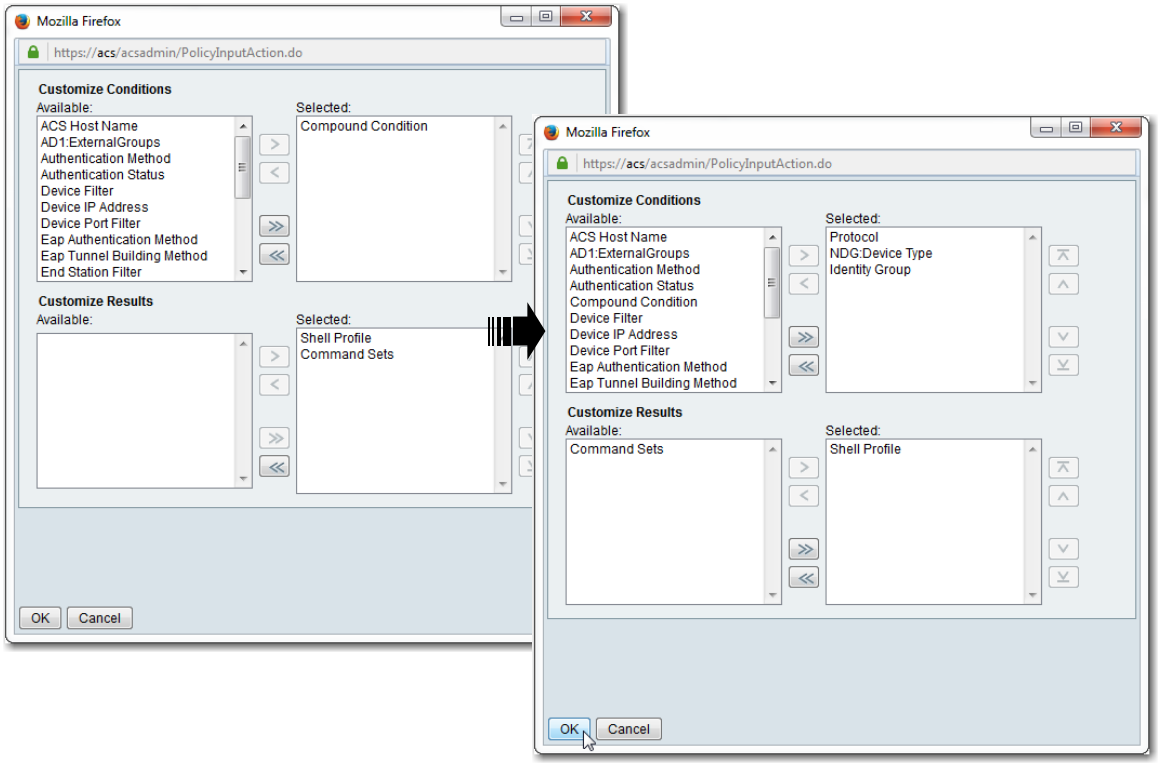
d Navigate to **Access Policies > Access Services > Orch-admin services > Identity**.

e For **Identity Source**, select **Internal Users**, and click **Save Changes**.



f Navigate to **Access Policies > Access Services > Orch-admin services > Authorization**, and click **Customize**.

g When the **Customize Conditions** window appears, make the following changes:

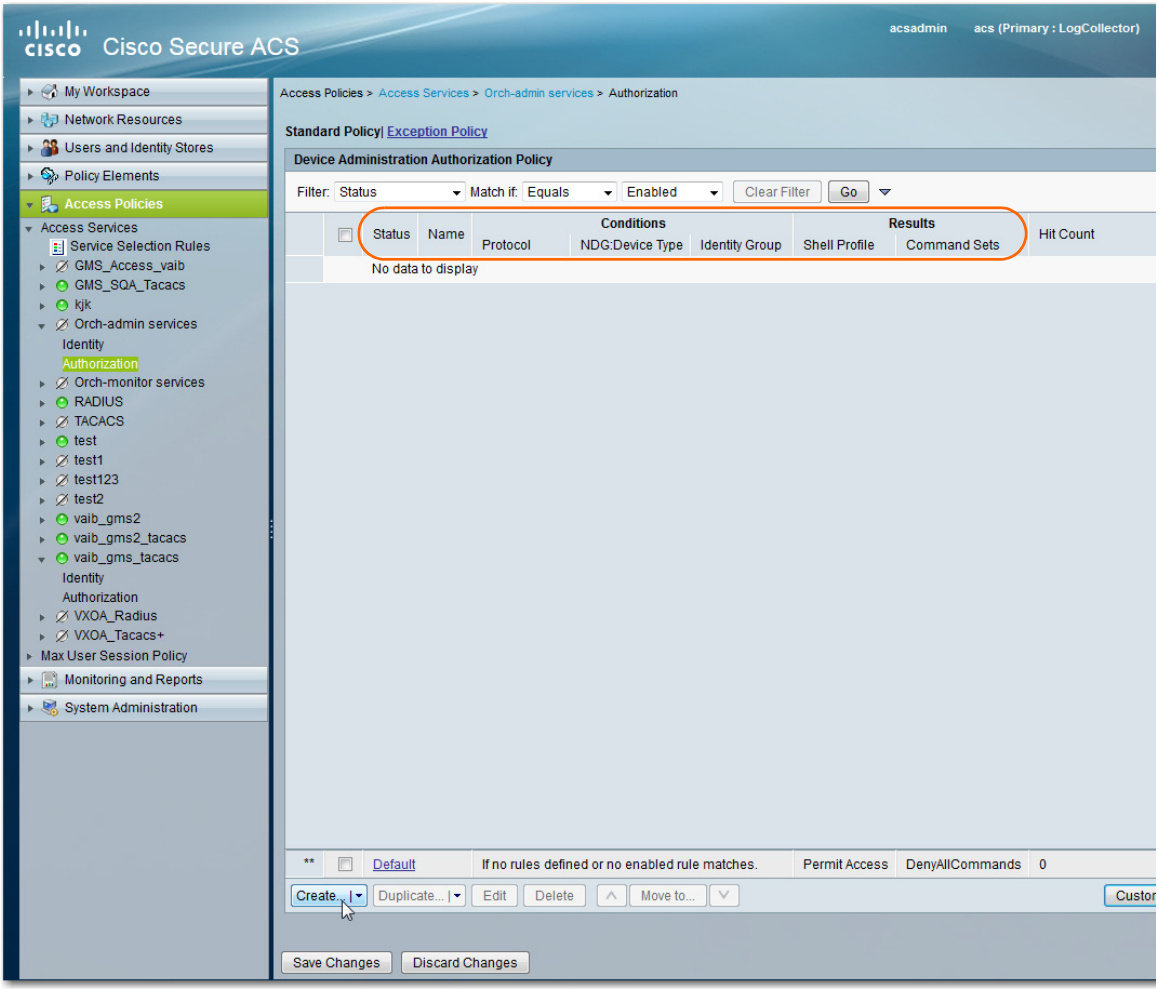


☐ **Customize Conditions - Selected** box — *Remove:* **Compound Condition**

Add: **Protocol**, **NDG:Device Type**, **Identity Group**

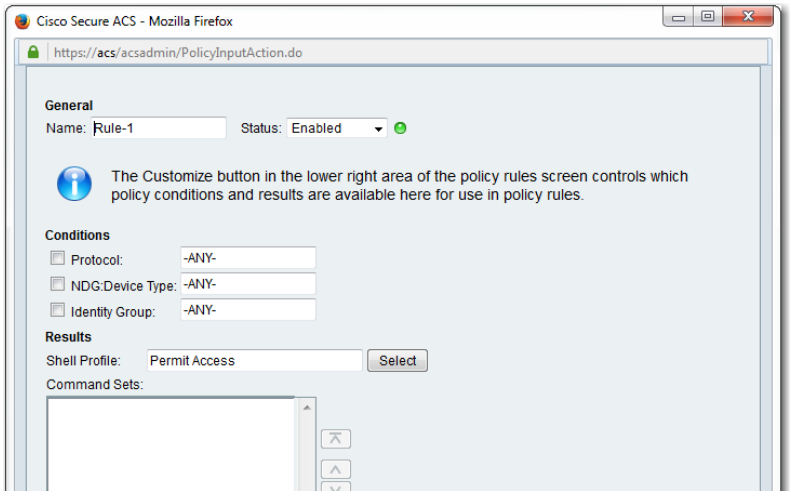
☐ **Customize Results - Selected** box — *Remove:* **Command Sets**

h Click **OK**. The result displays in the **Standard Policy** table.

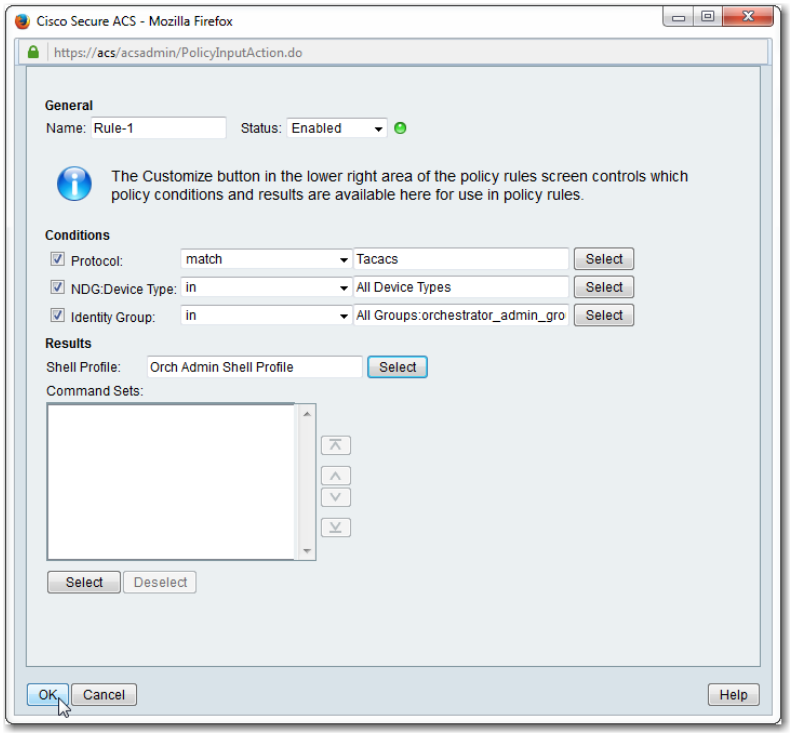


Now we'll create an authorization rule for **admin**.

i Click **Create**. A Rule dialog box appears.



j Make the following selections and changes:



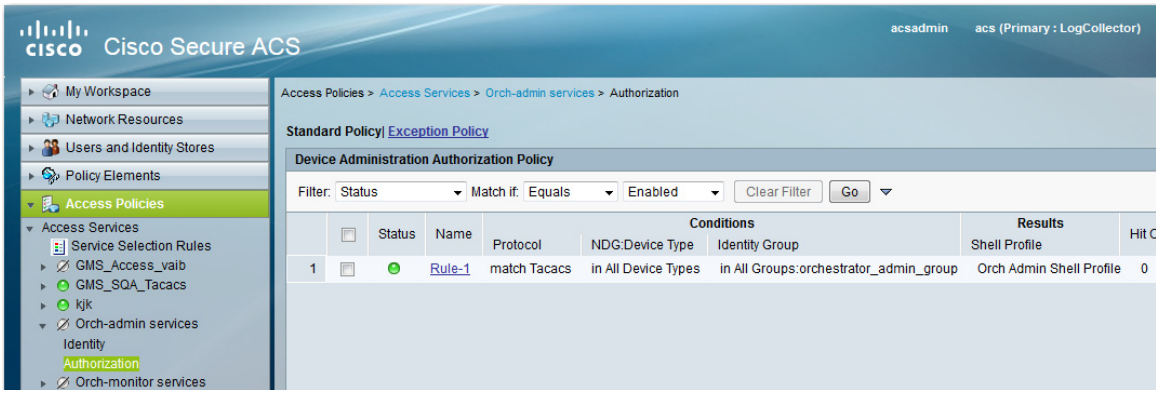
Conditions

Protocol:	match	Tacacs
NDG:Device Type:	in	All Device Types
Identity Group:	in	All Groups : orchestrator_admin_group

Results

Shell Profile:	Orch Admin Shell Profile

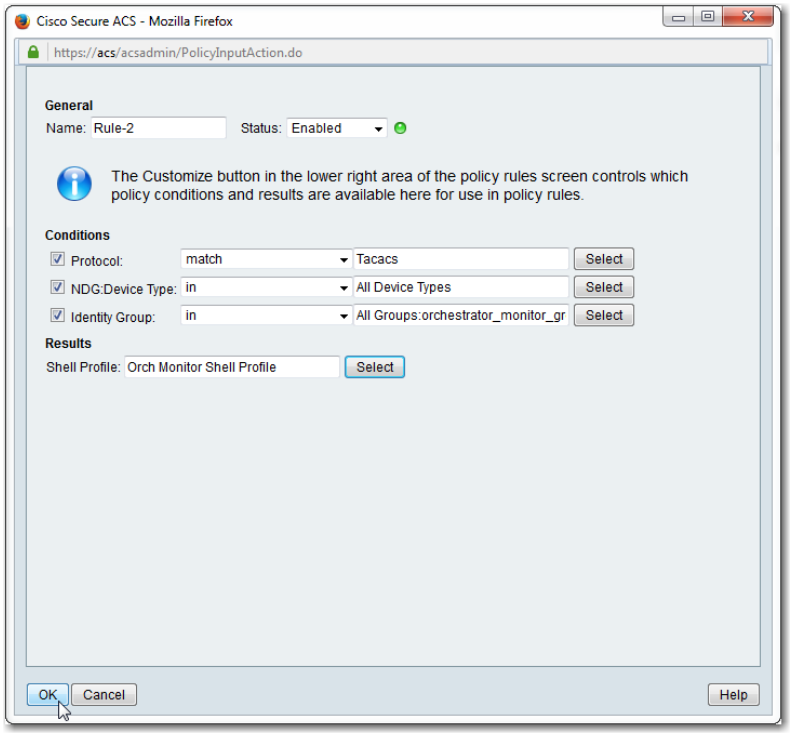
k Click **OK**. The **Device Administration Authorization Policy** appears, with **Rule-1** included.



Now we'll create an authorization rule for **monitor**.

l At the bottom of the page, click **Create**. The **Rule-2** dialog box appears.

m Make the following selections and changes:



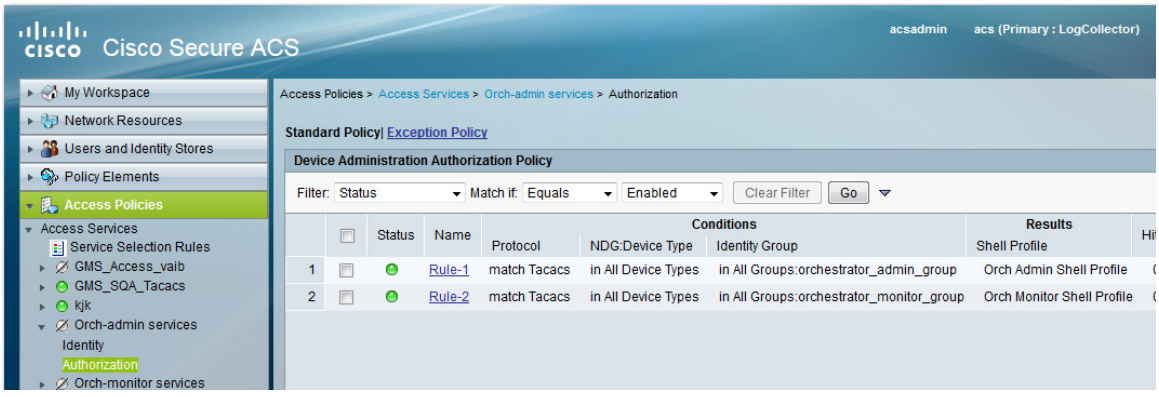
Conditions

Protocol:	match	Tacacs
NDG:Device Type:	in	All Device Types
Identity Group:	in	All Groups : orchestrator_monitor_group

Results

Shell Profile:	Orch Monitor Shell Profile

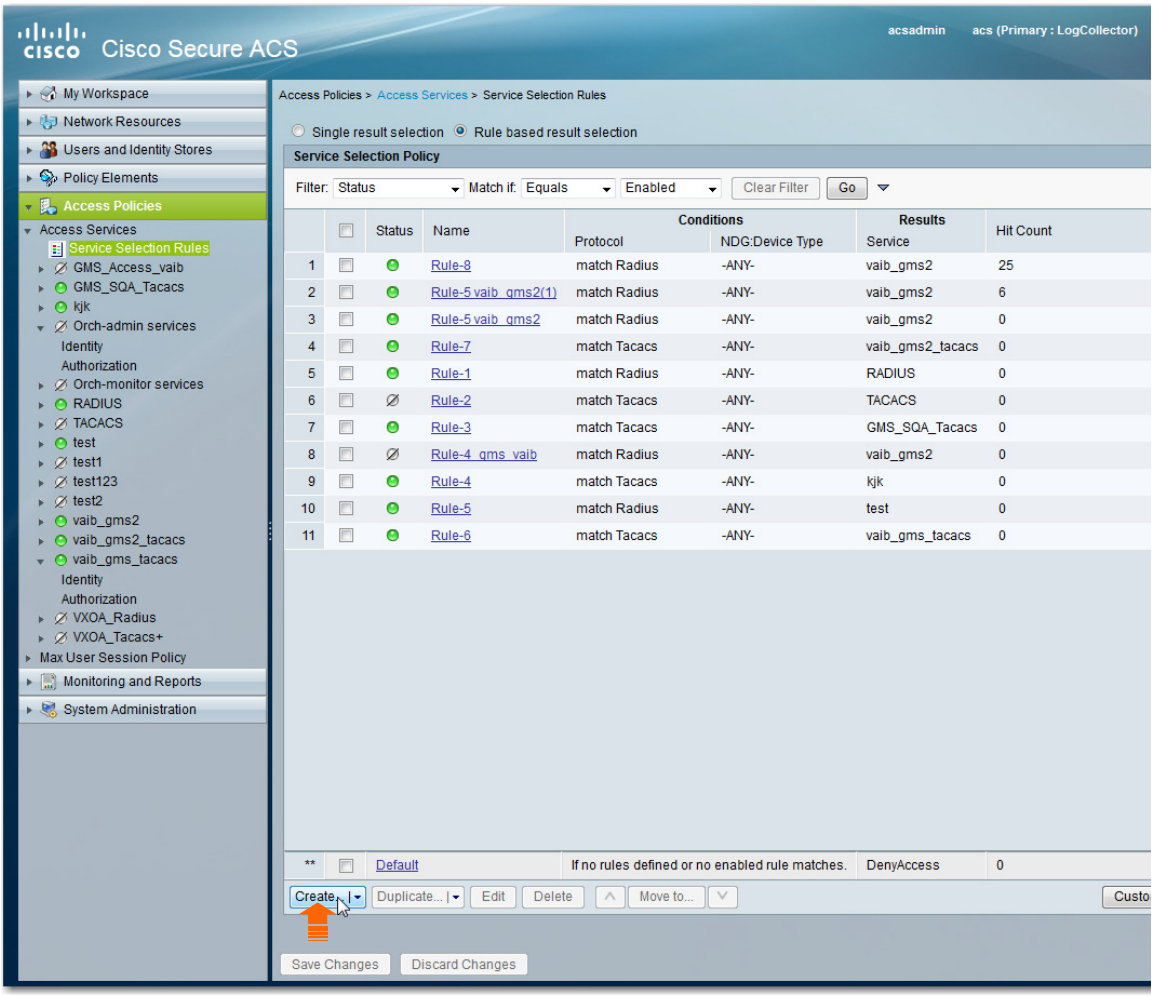
n Click **OK**. The **Device Administration Authorization Policy** appears, with **Rule-2** included.



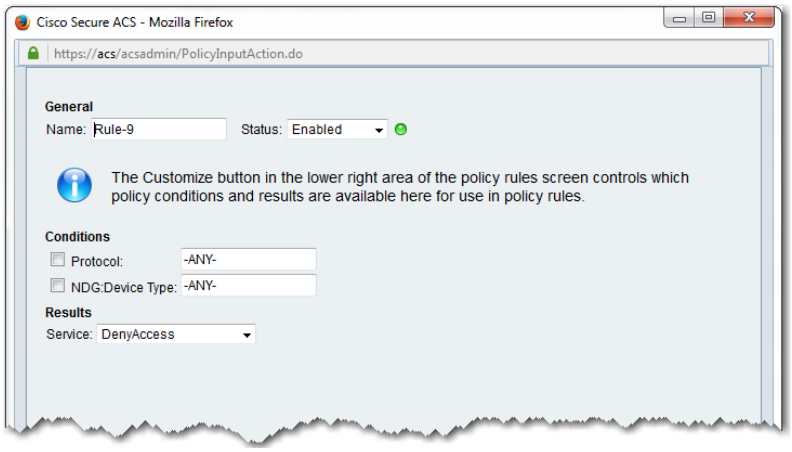
o Click **Save Changes**.

7 Create a Service Selection Rule to parse traffic hitting the TACACS+ server for appropriate action

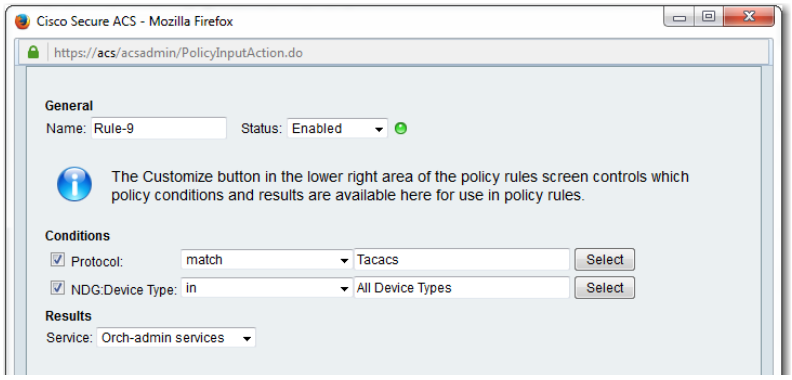
a Navigate to **Access Policies > Access Services: Service Selection Rules**, and click **Create**.



A dialog appears for creating a new rule.

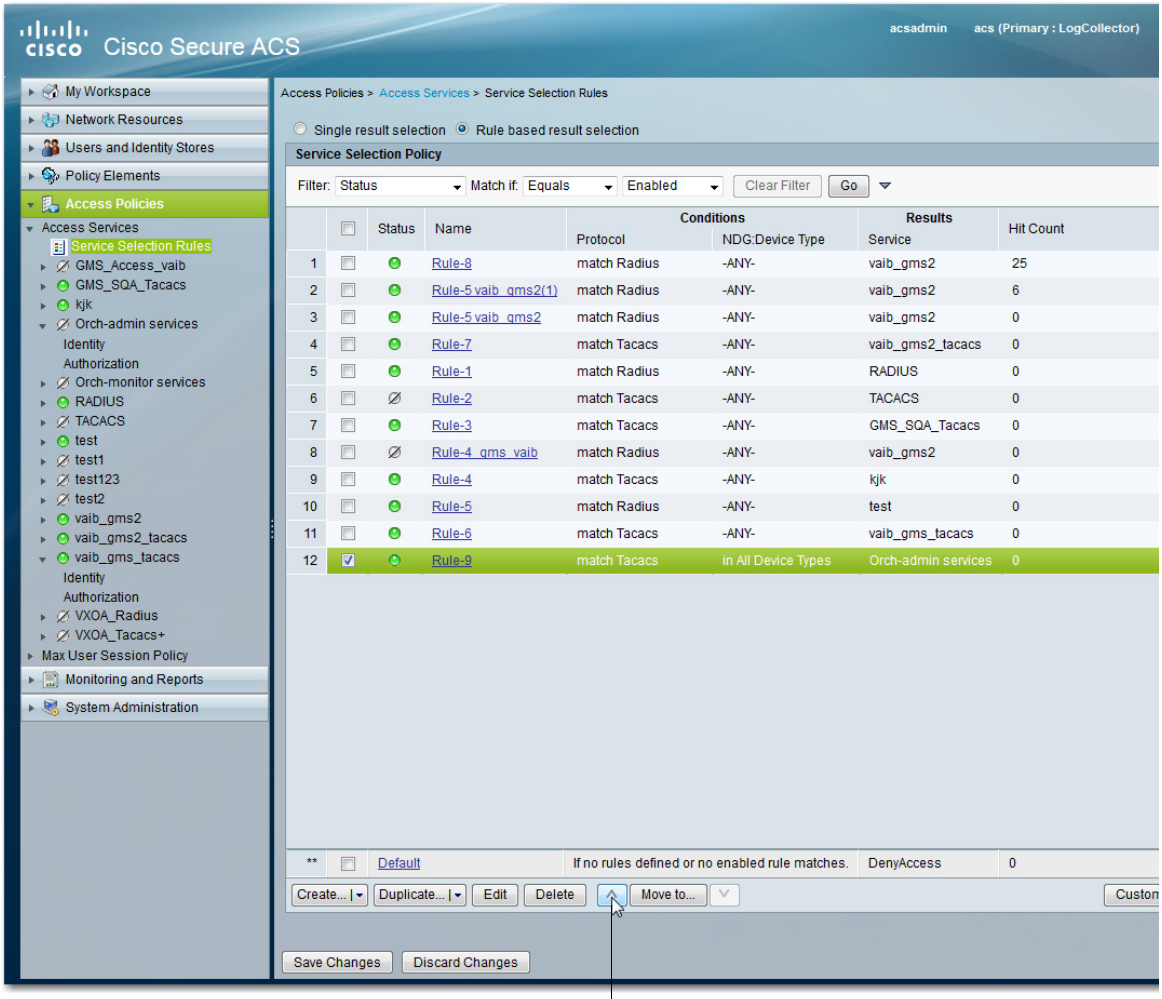


b Complete the following:



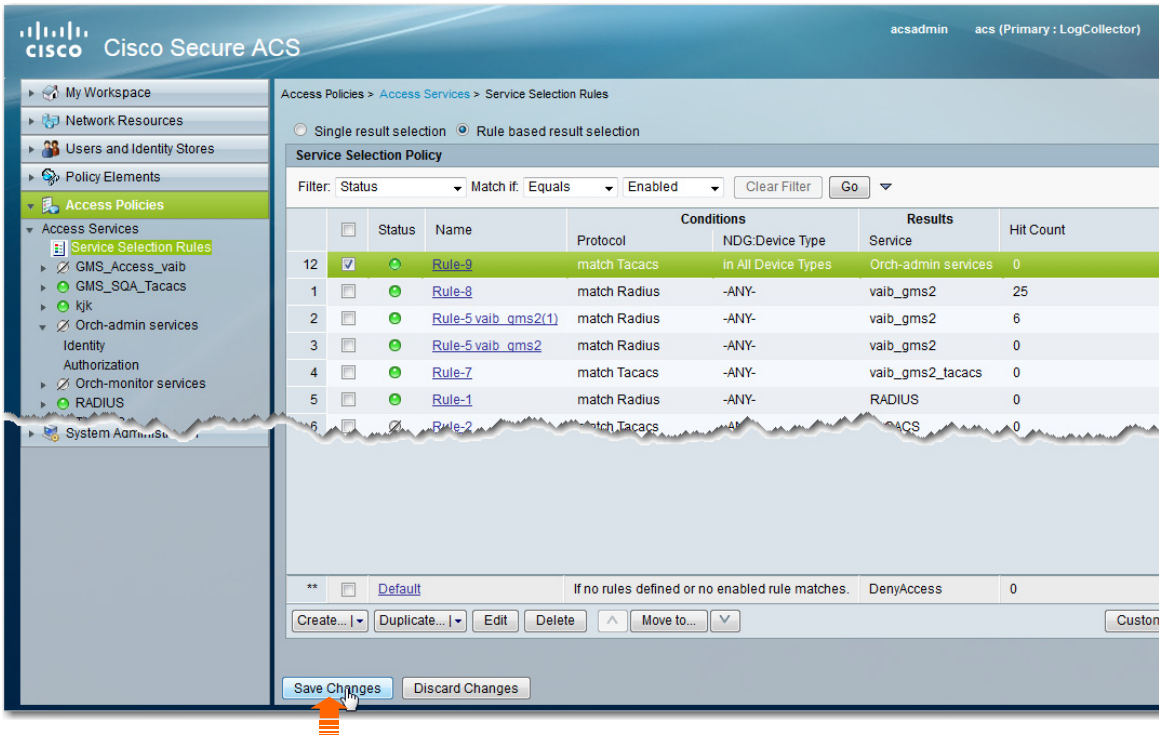
- ☐ Select the **Protocol** checkbox, and select **match** and **Tacacs**.
- ☐ Select the **NDG:Device Type** checkbox, and select **in** and **All Device Types**.
- ☐ From the drop-down list in the **Service** field, select **Orch-admin services**.
- ☐ Click **OK**.
  The **Service Selection Policy** 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.



Use the caret to move the Service Selection Rule up to the appropriate priority.

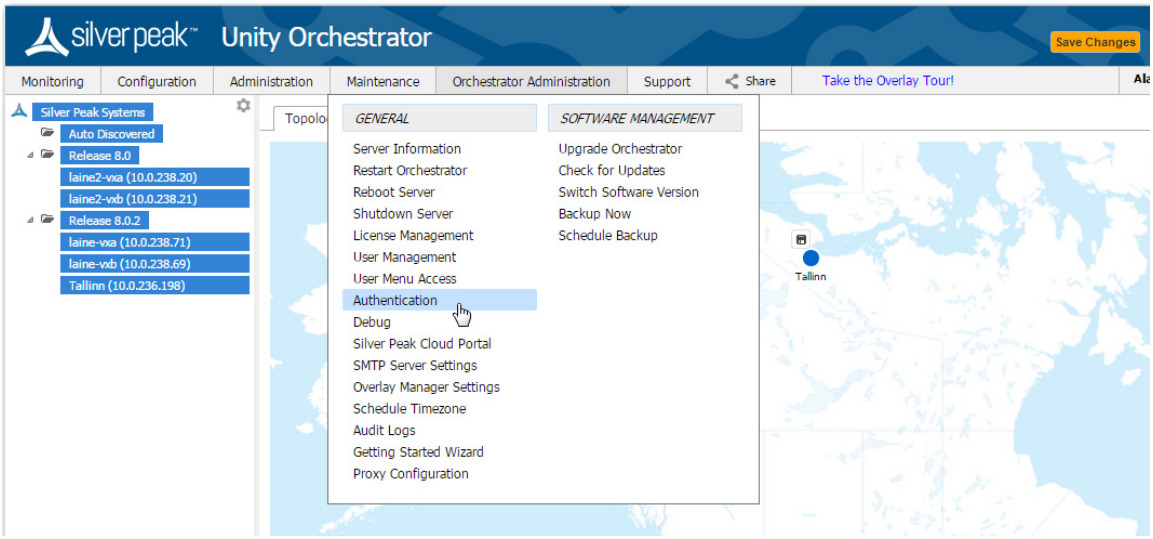
d Click **Save Changes**.



You have now finished configuring Cisco Secure ACS to use TACACS+ for authenticating Orchestrator users.

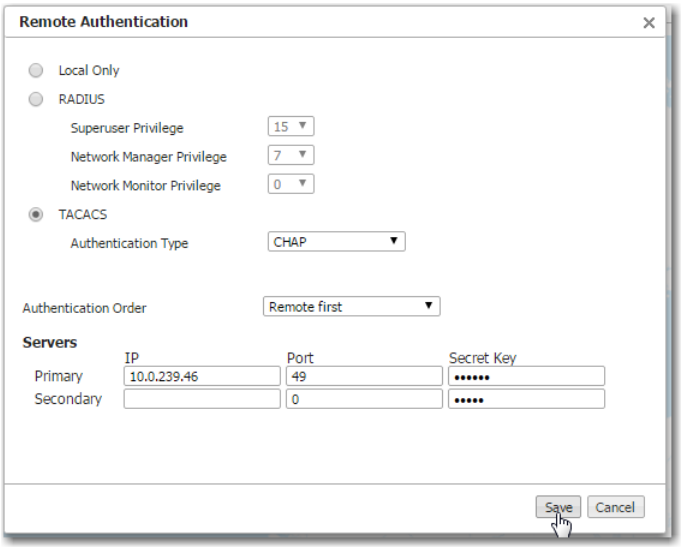
8 Configure the Orchestrator for TACACS+ authentication with Cisco Secure ACS

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



The **Remote Authentication** dialog box appears.

b Select **TACACS**, and complete the following:

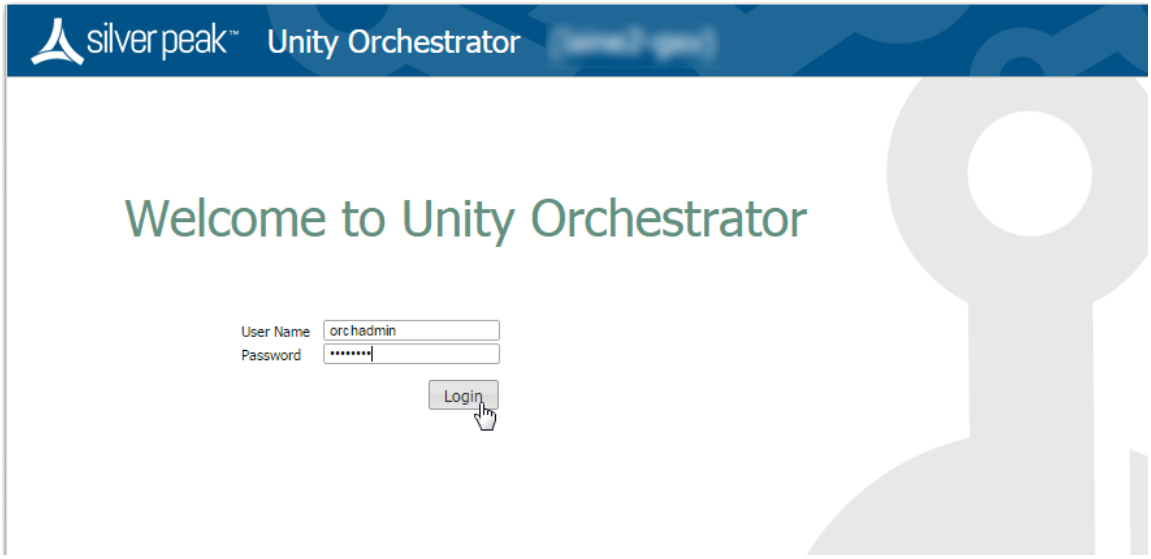


Authentication Type:	CHAP
Authentication Order:	Remote first
Server IP:	[Cisco Secure ACS IP address]
Server Port:	49
Server Secret Key:	[Orchestrator's shared secret]

c Click **Save**.

d Log out of Orchestrator.

e On the welcome page, log in as `orchadmin`, the identity you created in the TACACS+ server.



Orchestrator is now authenticating users via the TACACS+ server.