Configure SWA External Authentication with ISE as a RADIUS Server

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Network Topology

Configure

- ISE Configuration
- SWA Configuration

Verify

Related Content

Introduction

This document describes the steps to configure external authentication on Secure Web Access (SWA) with Cisco ISE® as a RADIUS server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic RADIUS Knowledge
- Basic Knowledge of Cisco SWA
- Knowledge of Authentication and Authorization Configuration Policies on Cisco Identity Services Engine® (ISE)

Cisco recommends that you also have:

- Compatible SWA and ISE Versions
- SWA and ISE Administration Access

Components Used

The information in this document is based on these software versions:

- ISE 3.0.0
- SWA 14.0.2-012

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

When you enable external authentication for administrative users of your SWA, the device verifies the user credentials with a Lightweight Directory Access Protocol (LDAP) or RADIUS server as specified in the external authentication configuration.

Network Topology



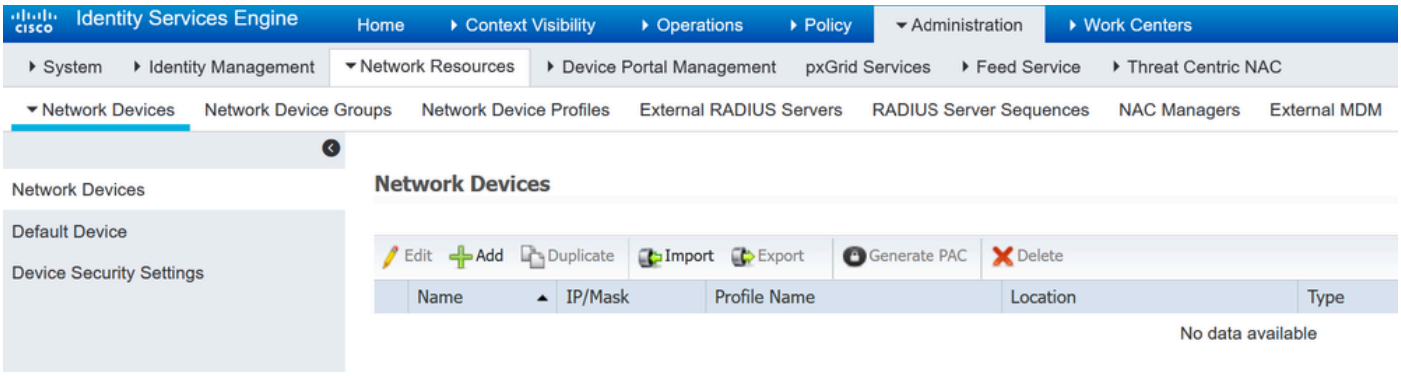
Network Topology Diagram

Administrative users access SWA on port 443 with their credentials and SWA verifies the credentials with the RADIUS server.

Configure

ISE Configuration

1. Add a new Network Device and navigate to **Administration > Network Resources > Network Devices > +Add**.

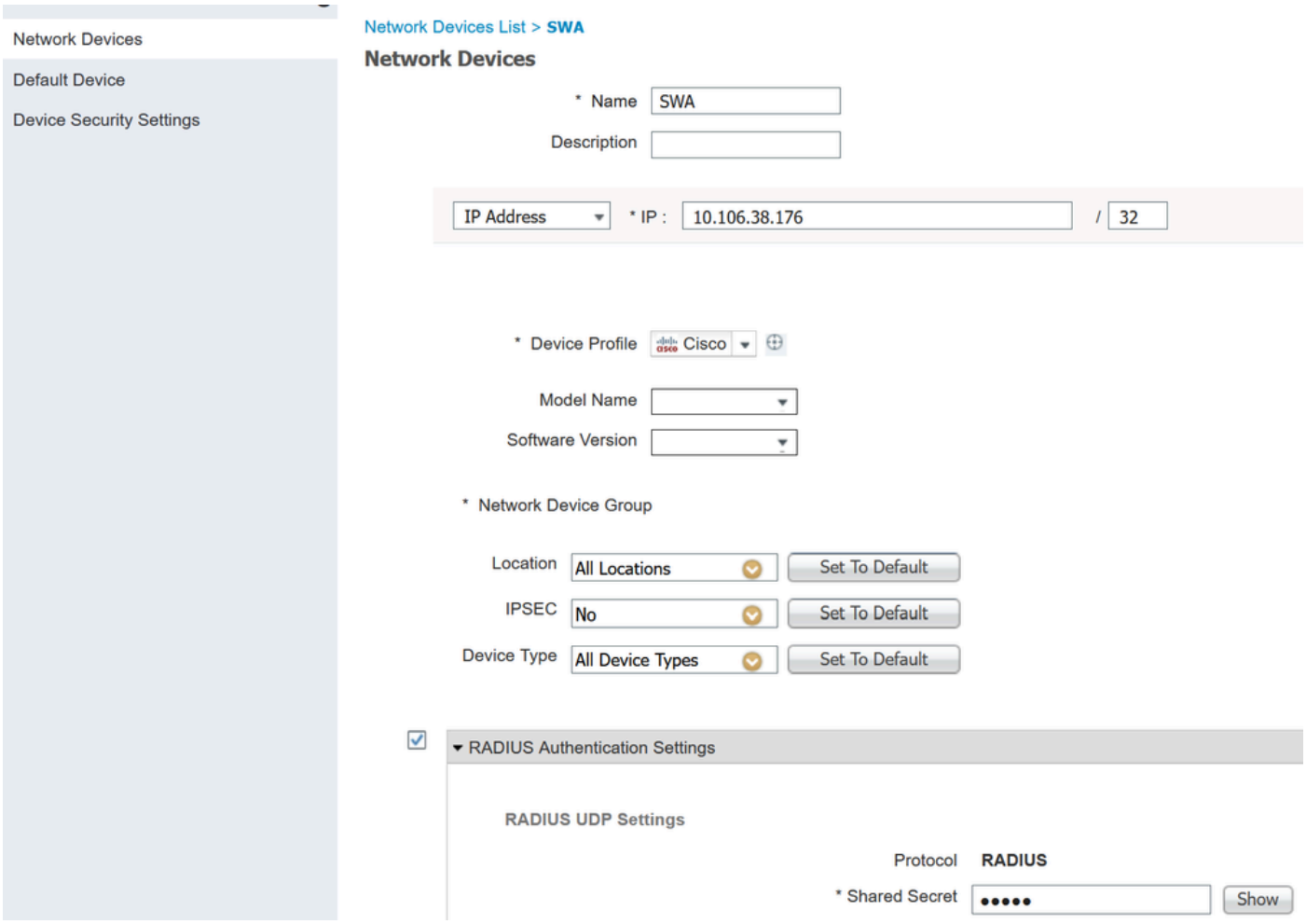


Add SWA as Network Device in ISE

2. Assign a **Name** to the network device object and insert the SWA **IP Address**.

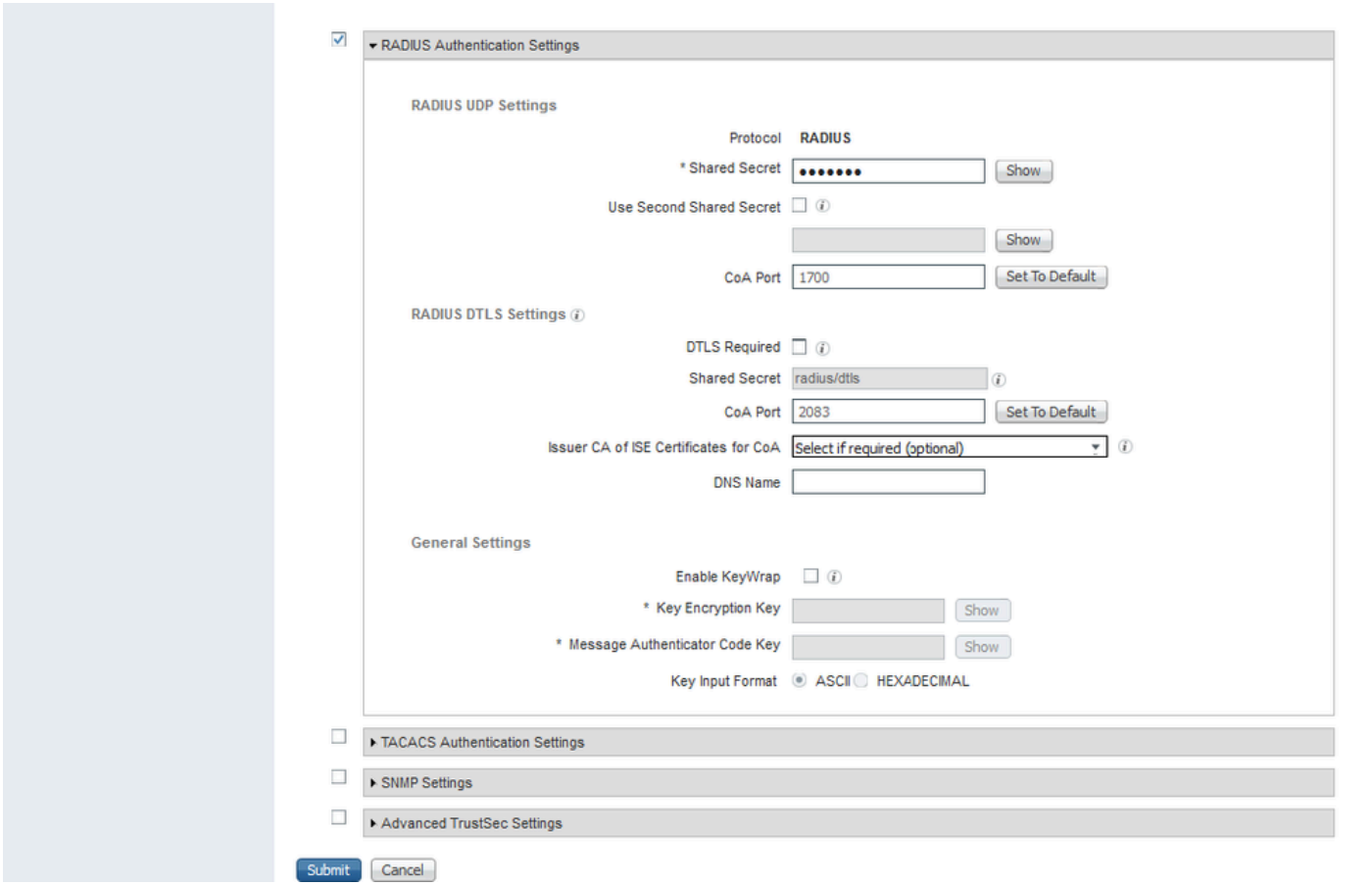
2.1. Check the RADIUS **checkbox** and define a **Shared Secret**.

Note: The same key must be used later to configure the RADIUS server in SWA.



Configure SWA Network Device Shared Key

2.2. Click **Submit**.

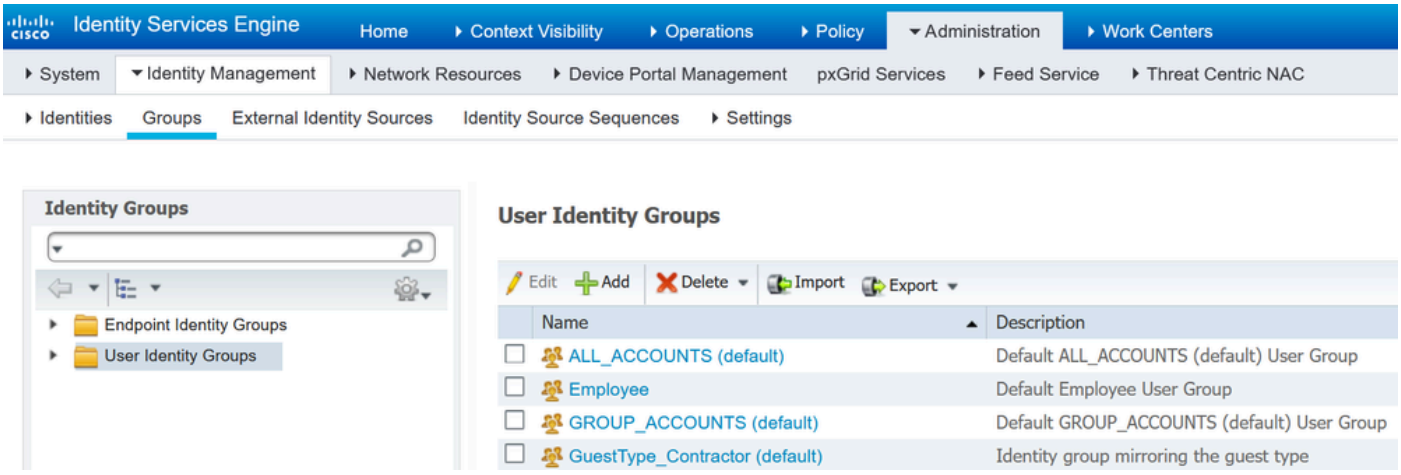


Submit Network Device Configuration

---

3. Create the required User Identity Groups and navigate to **Administration > Identity Management > Groups > User Identity Groups > +Add**.

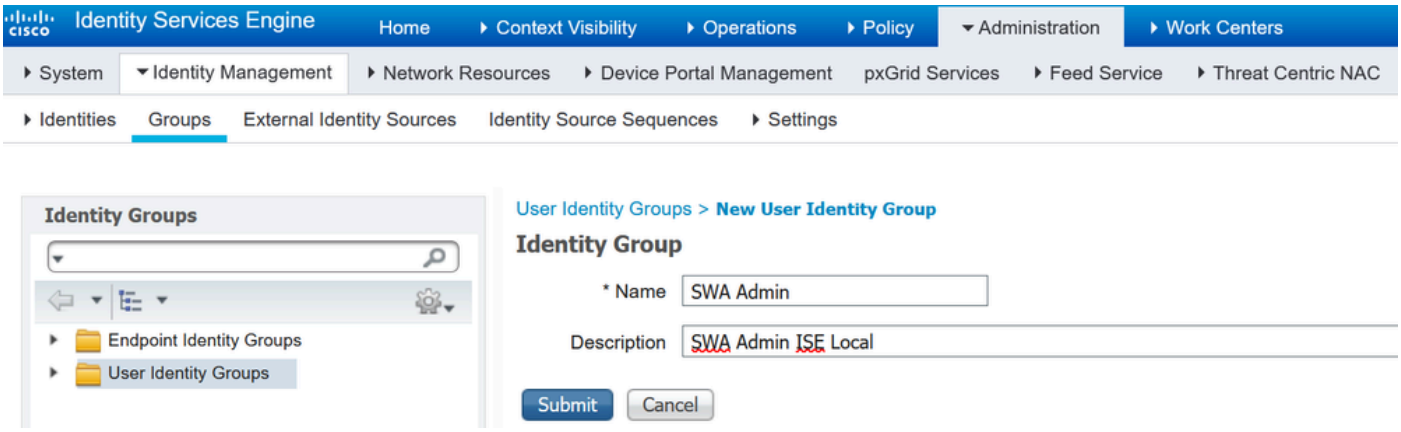
Note: You must configure different user groups to match the different types of users.



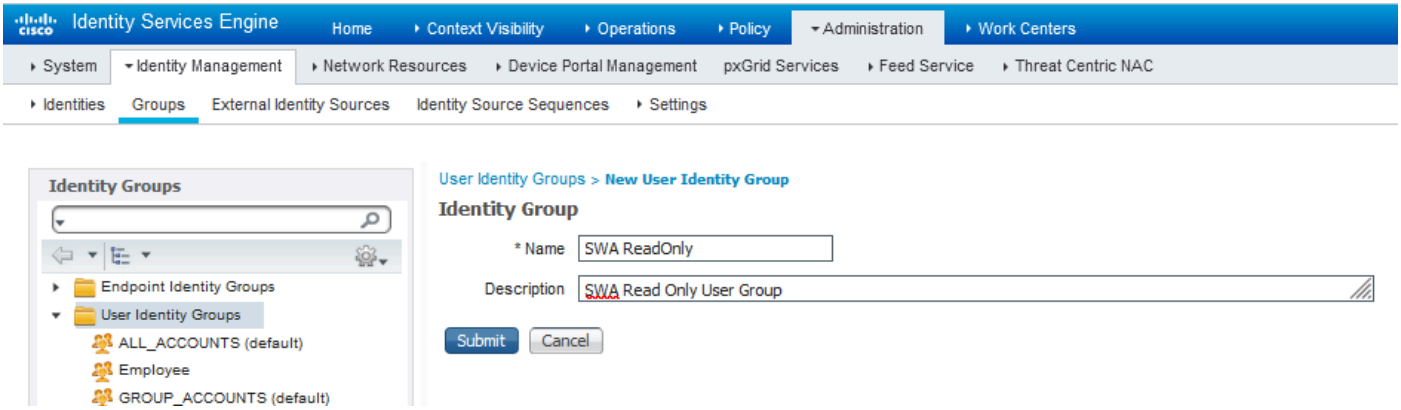
Add User Identity Group

---

4. Input group name, description (optional) and **Submit**. Repeat these steps for each group. In this example, create a group for Administrator Users, and another one for Read-Only Users.



Add User Identity Group

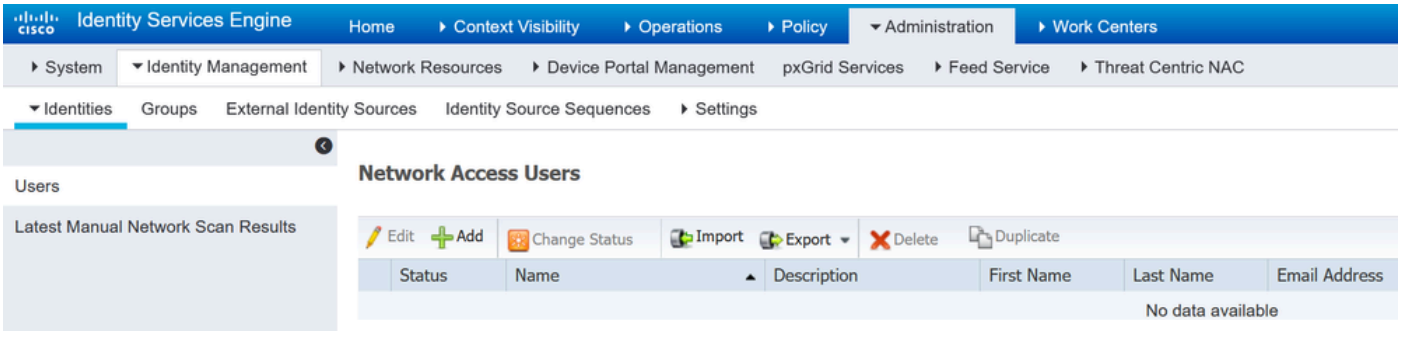


Add User Identity Group for SWA Read Only Users

---

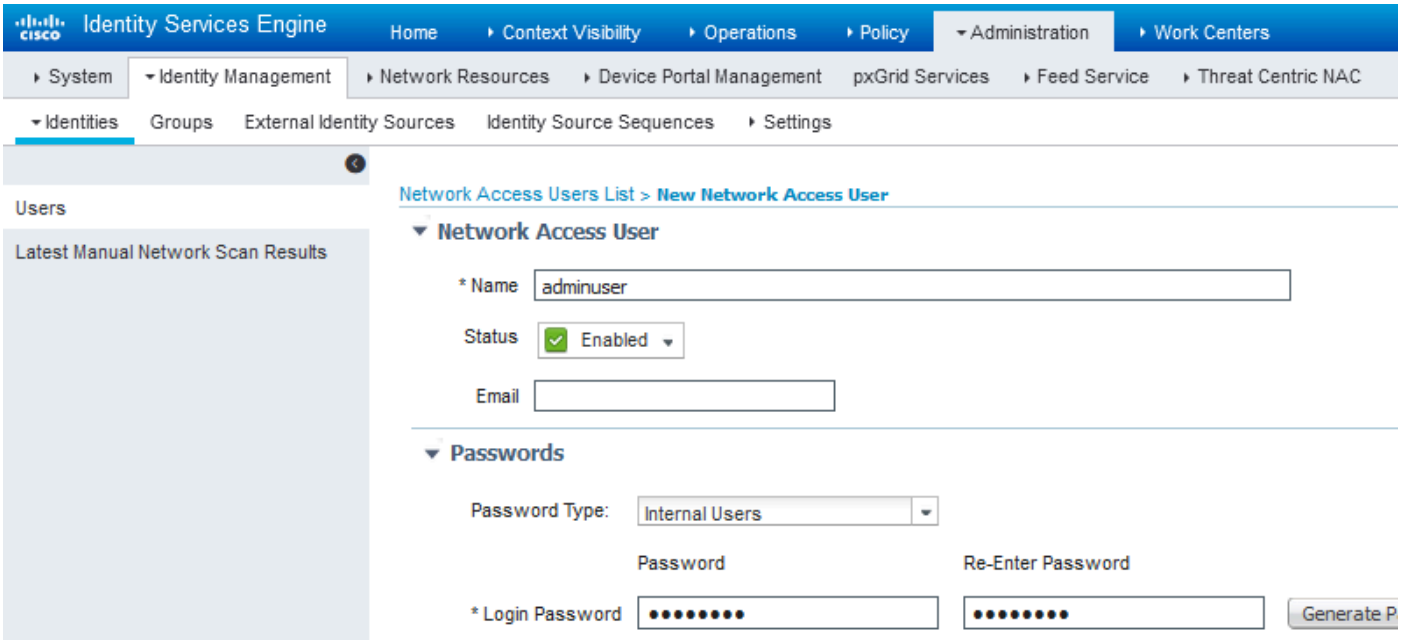
5. You must create Network Access Users that match with the username configured in SWA.

5.1. Create the **Network Access Users** and add them to their correspondent group. Navigate to **Administration > Identity Management > Identities > +Add**.



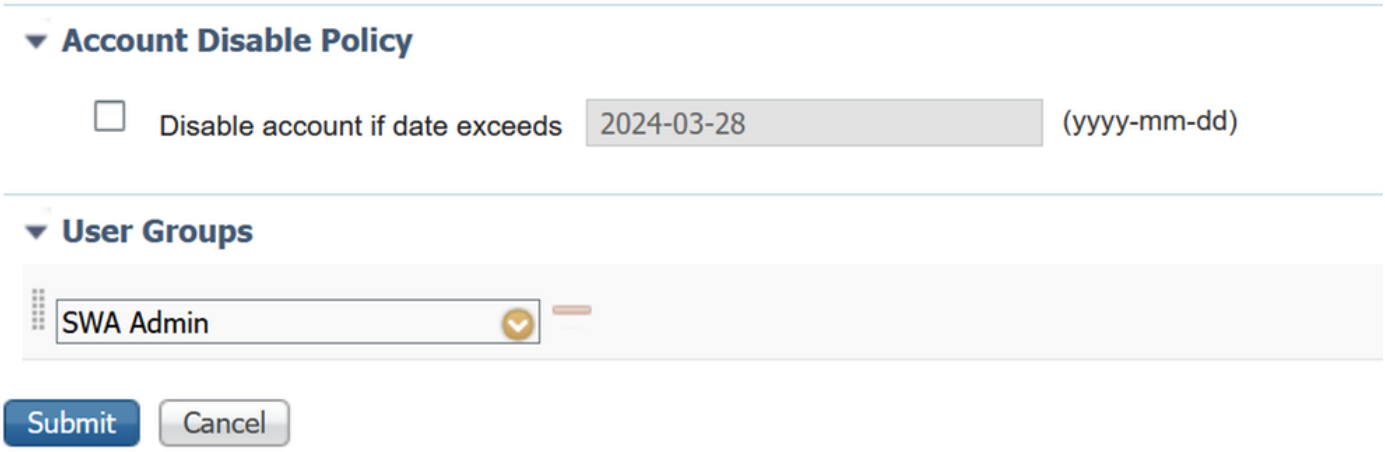
Add Local Users in ISE

5.2. You must create **Network Access Users** with Administrator rights and assign a name and password.



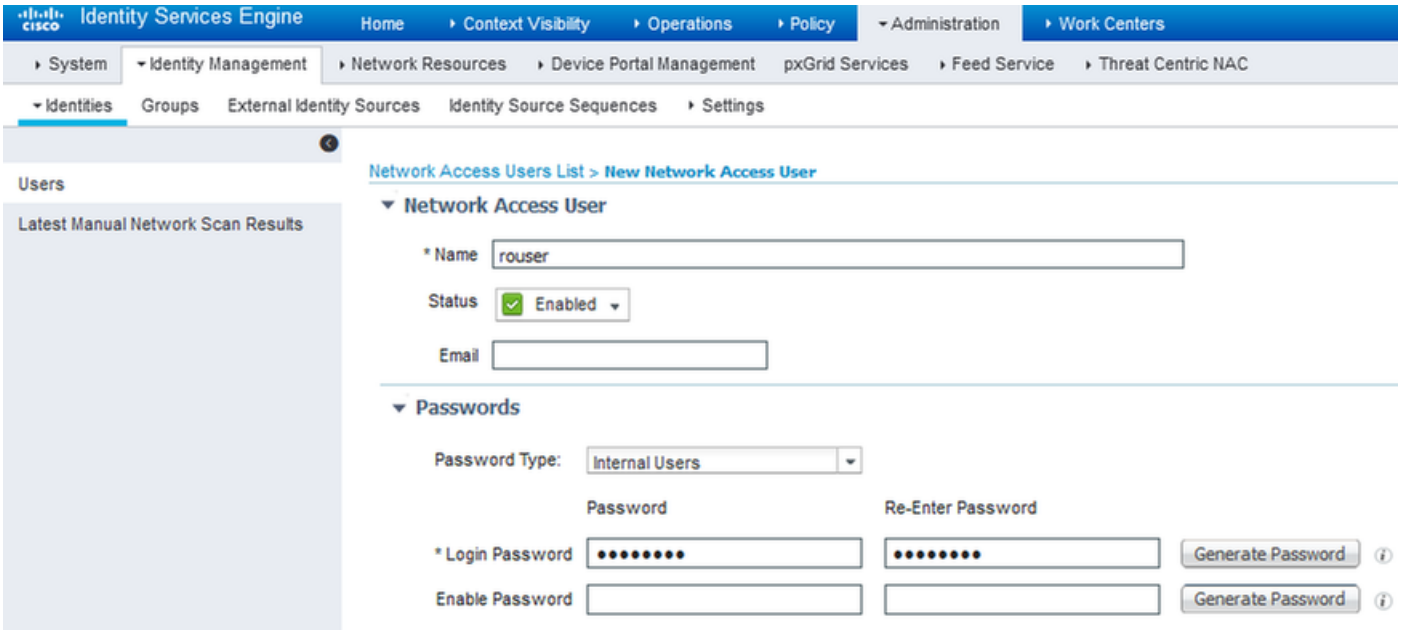
Add Admin User

5.3. Choose **SWA Admin** in the **User Groups** section.



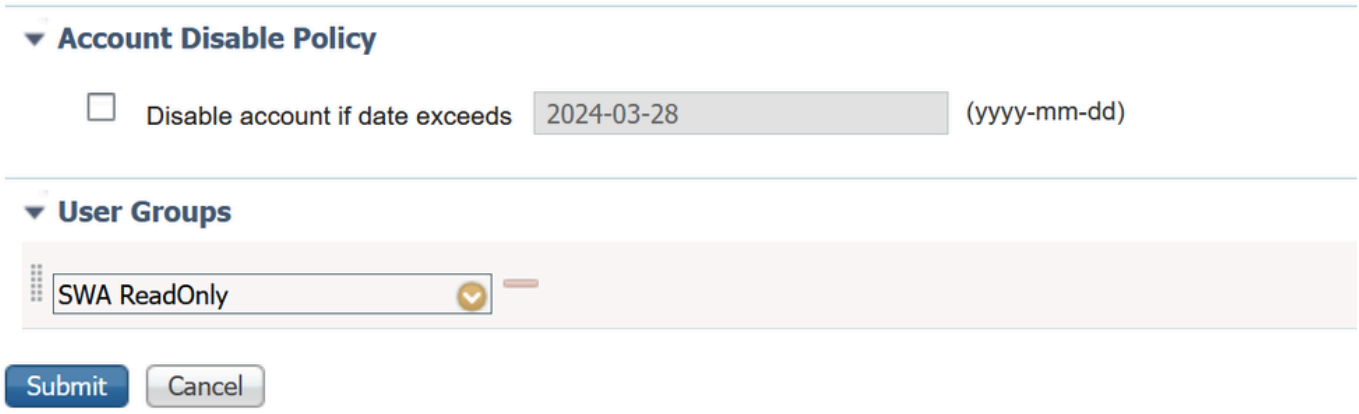
Assign Admin Group to the Admin User

5.4. Create a user with **Read Only** rights and assign a name and password.



Add Read Only User

5.5. Choose **SWA ReadOnly** in the **User Groups** section.



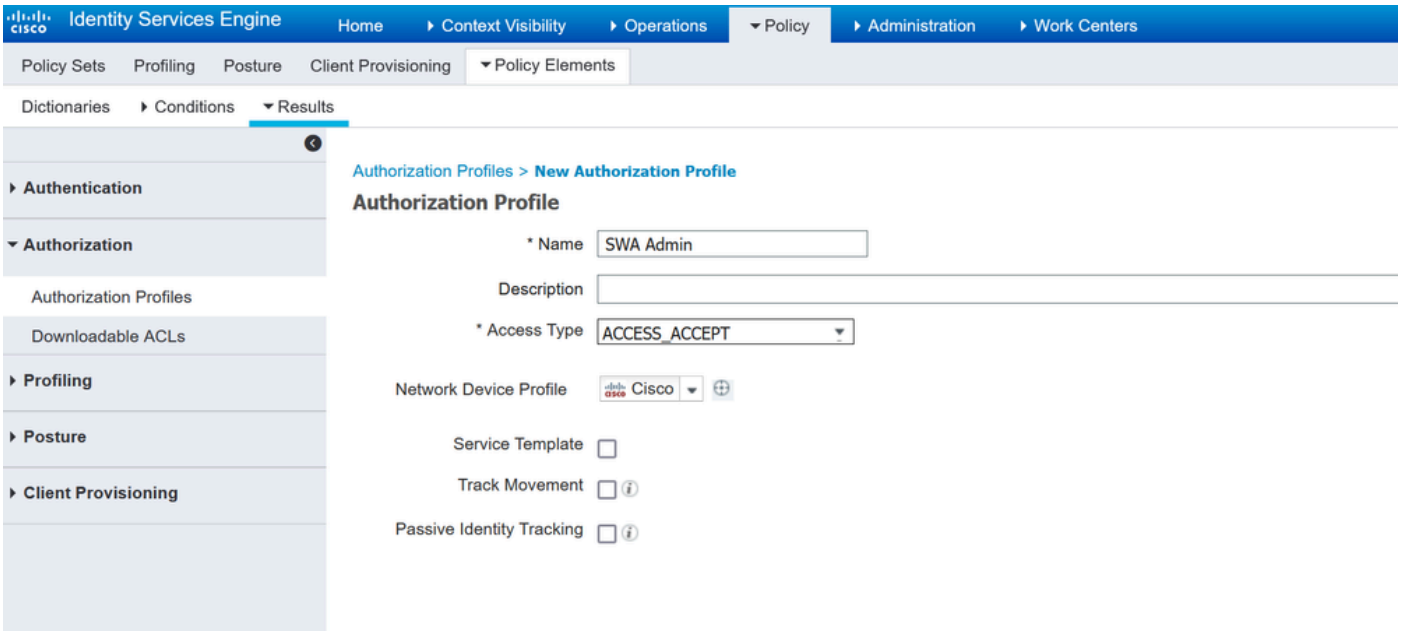
Assign Read Only User group to the Read Only User

---

6. Create the **Authorization Profile** for the Admin user.

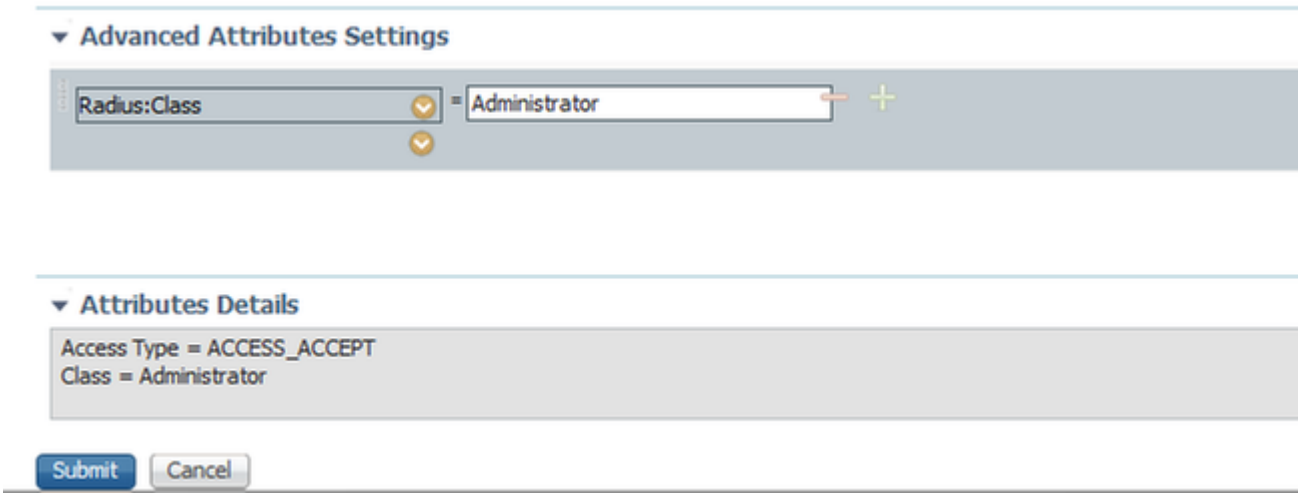
6.1. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add**.

6.2. Define a name for the **Authorization Profile** and ensure the **Access Type** is set to **ACCESS_ACCEPT**.



Add Authorization Profile for Admin Users

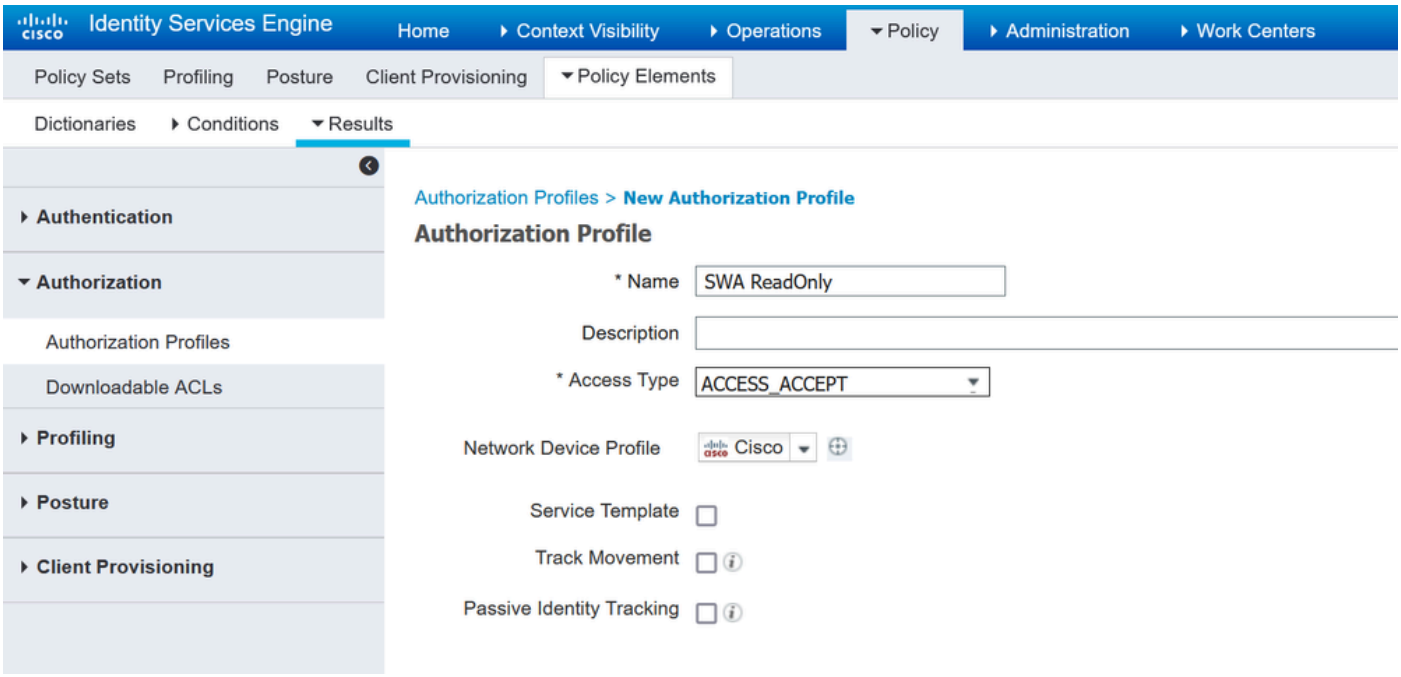
6.3. In the **Advanced Attributes Settings**, navigate to **Radius > Class--[25]** and enter the value **Administrator** and click **Submit**.



Add Authorization Profile for Admin Users

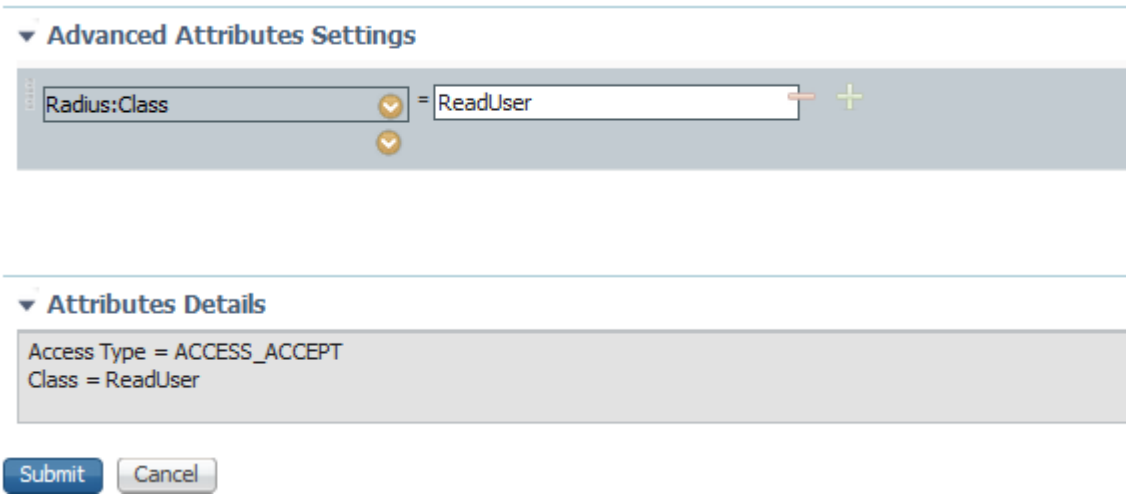
---

7. Repeat **Step 6** to create the **Authorization Profile** for the **Read Only User**.



Add Authorization Profile for Read Only Users

7.1. Create the **Radius:Class** with the value **ReadUser** instead of Administrator this time.

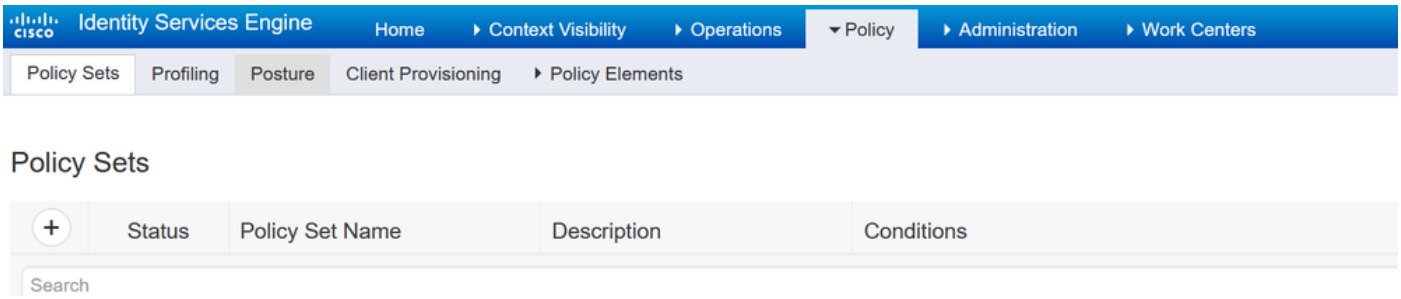


Add Authorization Profile for Read Only Users

---

8. Create **Policy Sets** that matches the SWA IP address. This is to prevent access to other devices with these user credentials.

8.1. Navigate to **Policy** > **Policy Sets** and click the + icon placed at the upper left corner.

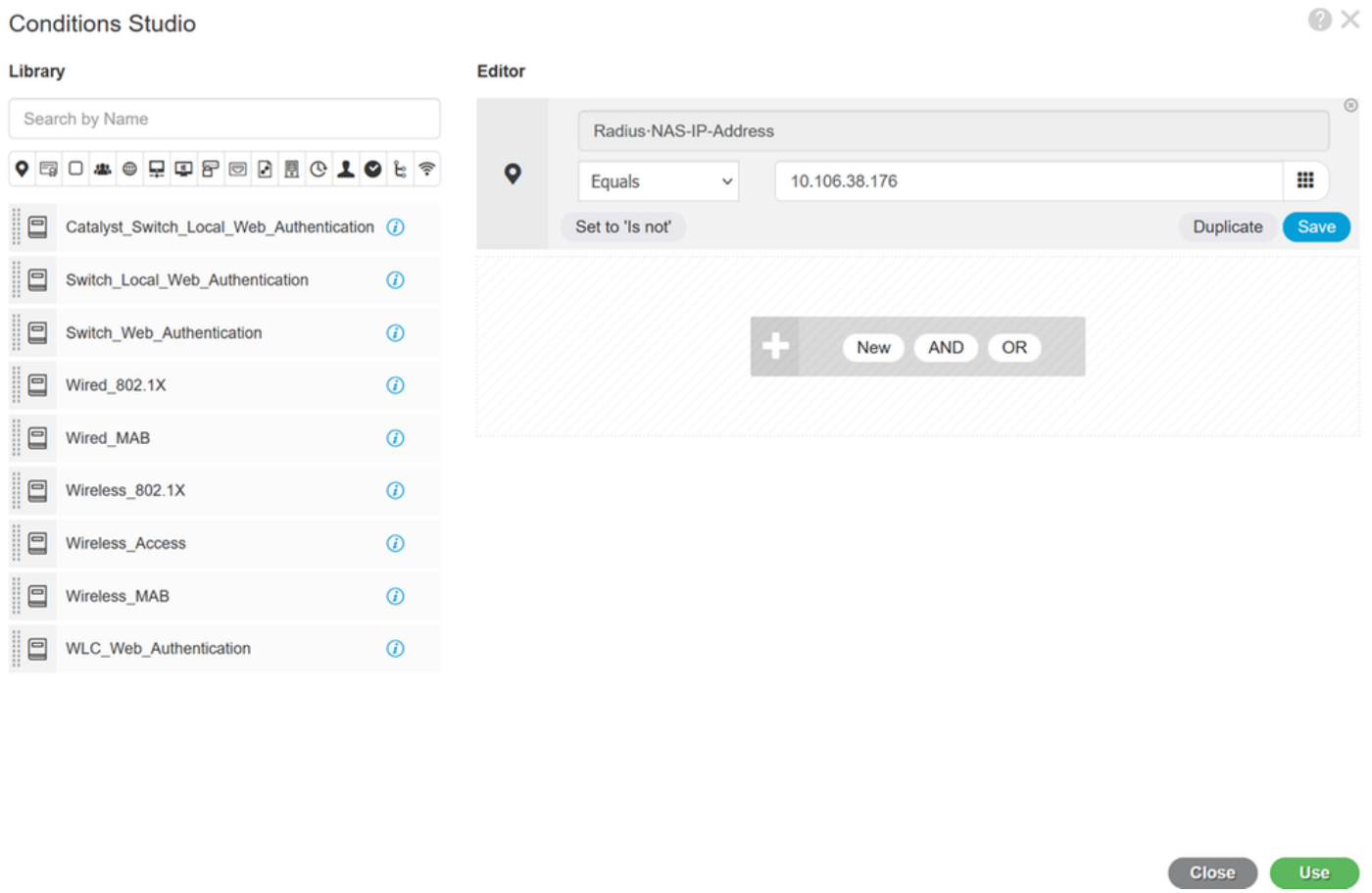


Add Policy Set in ISE

8.2. A new line is placed at the top of your **Policy Sets**.

8.3. Enter a name for the new policy and add a condition for the **RADIUS NAS-IP-Address** attribute to match the SWA IP address.

8.4. Click **Use** to keep the changes and exit the editor.



Add Policy to Map SWA Network Device

8.5. Click **Save**.



Policy Save

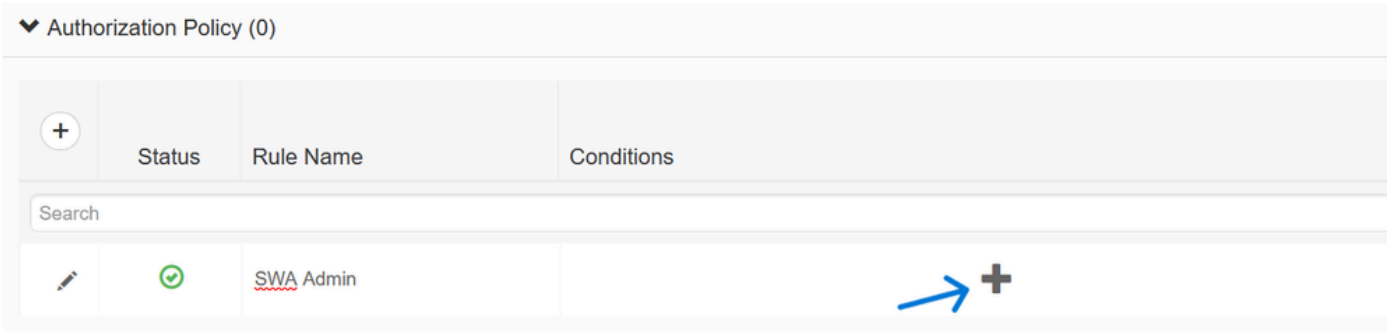
Tip: In this article, the Default Network Access Protocols list is allowed. You can create a new list and narrow down as needed.

---

9. To view the new **Policy Sets**, click the > icon in the **View** column. Expand the **Authorization Policy** menu and click the + icon to add a new rule to allow access to the user with admin rights.

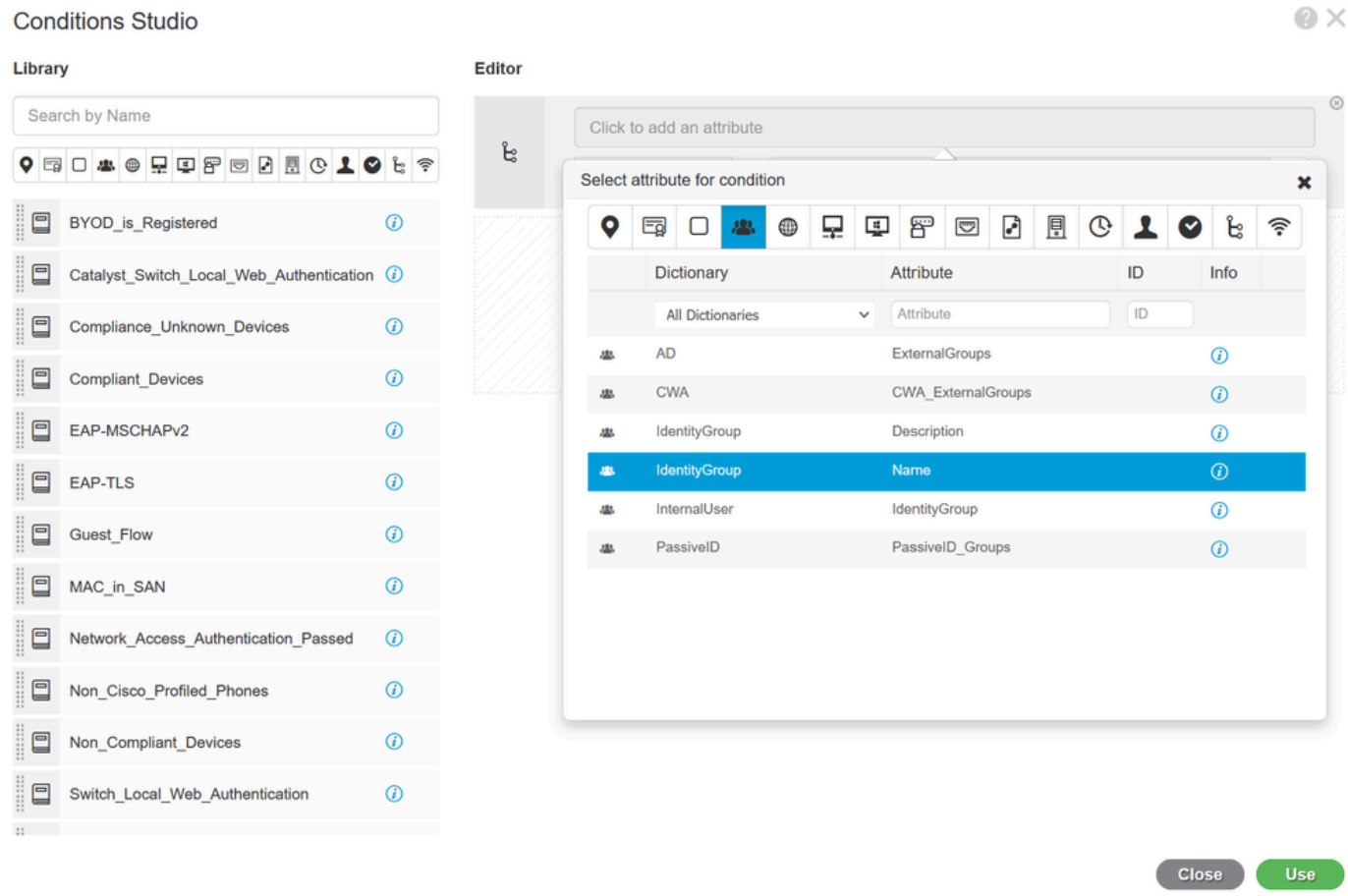
9.1.Enter a Name.

9.2. To create a condition to match the Admin User Group, click the + icon.



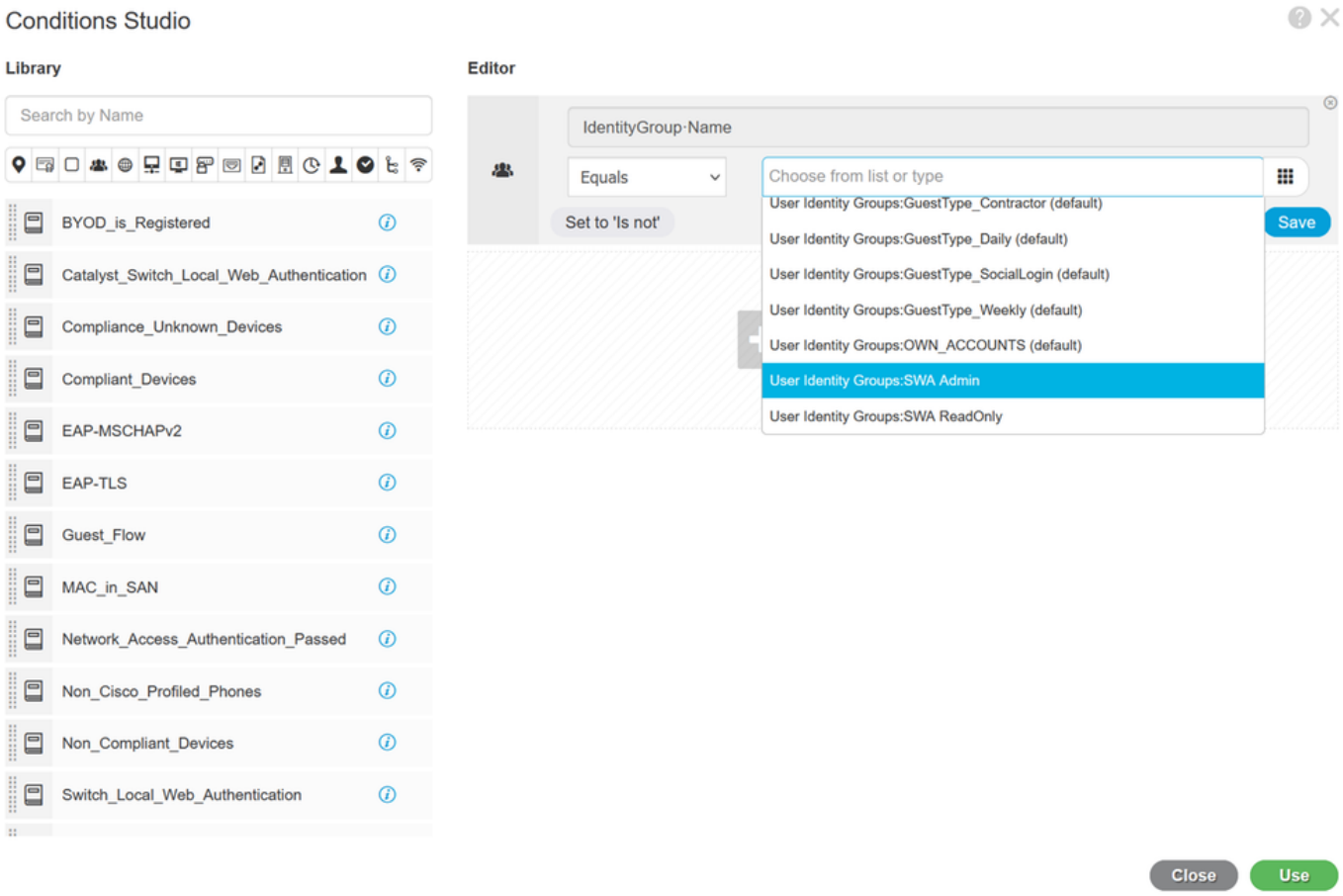
Add Authorization Policy Condition

9.3. Set the conditions to match the **Dictionary Identity Group** with **Attribute Name Equals User Identity Groups: SWA Admin**.



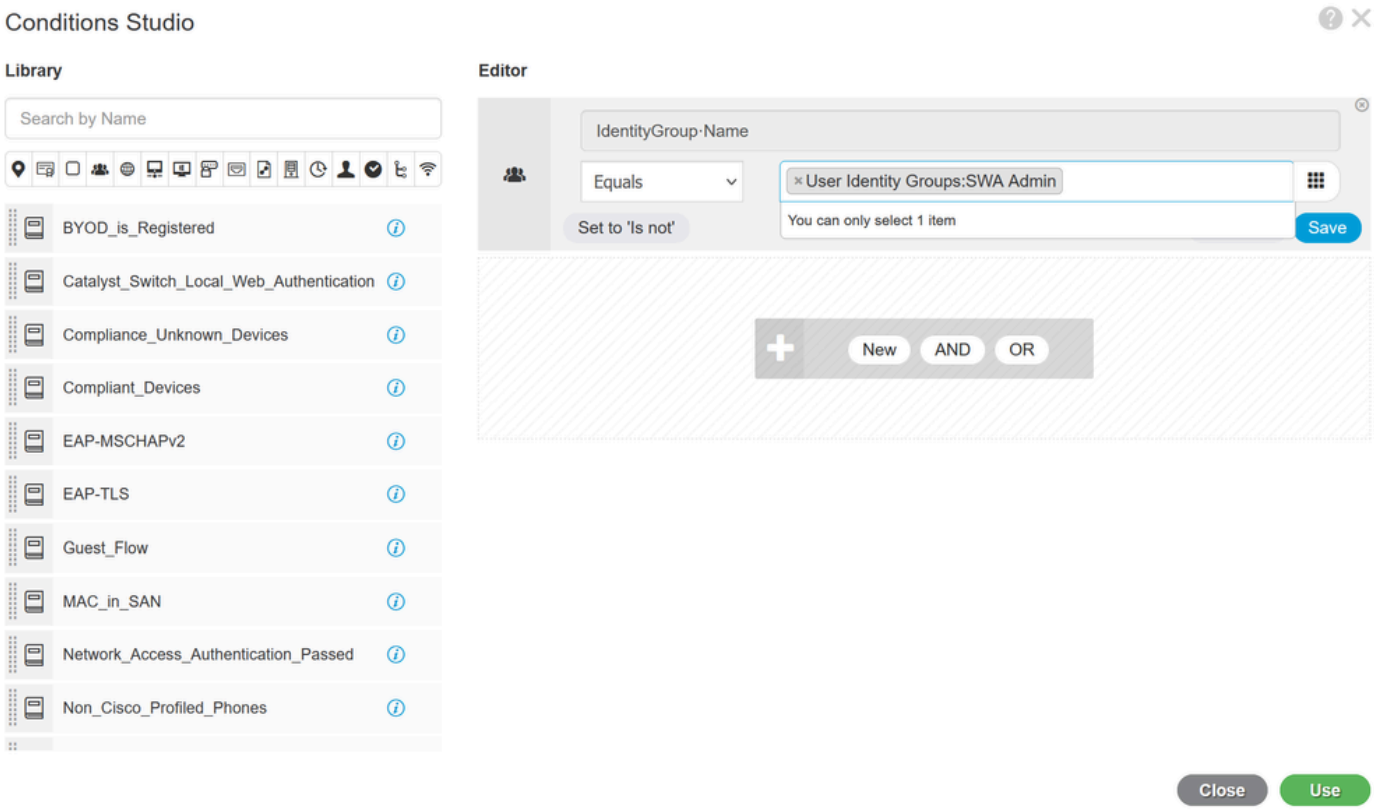
Select Identity Group as Condition

9.4. Scroll down and select **User Identity Groups: SWA Admin**.



Scroll Down abd Select Identity Group Name

9.5. Click **Use**.



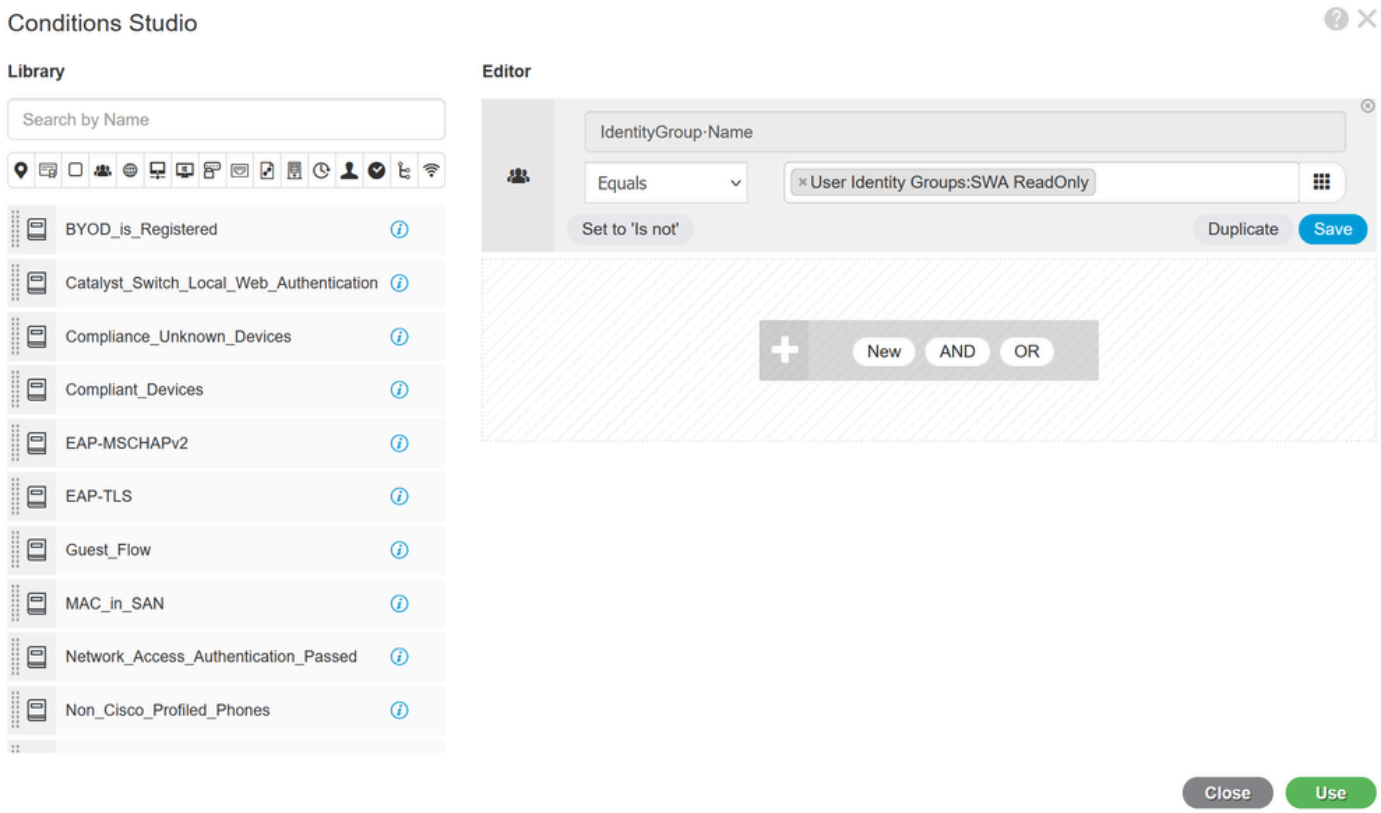
Select Authorization Policy for SWA Admin User Group

---

10. Click the + icon to add a second rule to allow access to the user with read-only rights.

10.1. Enter a Name.

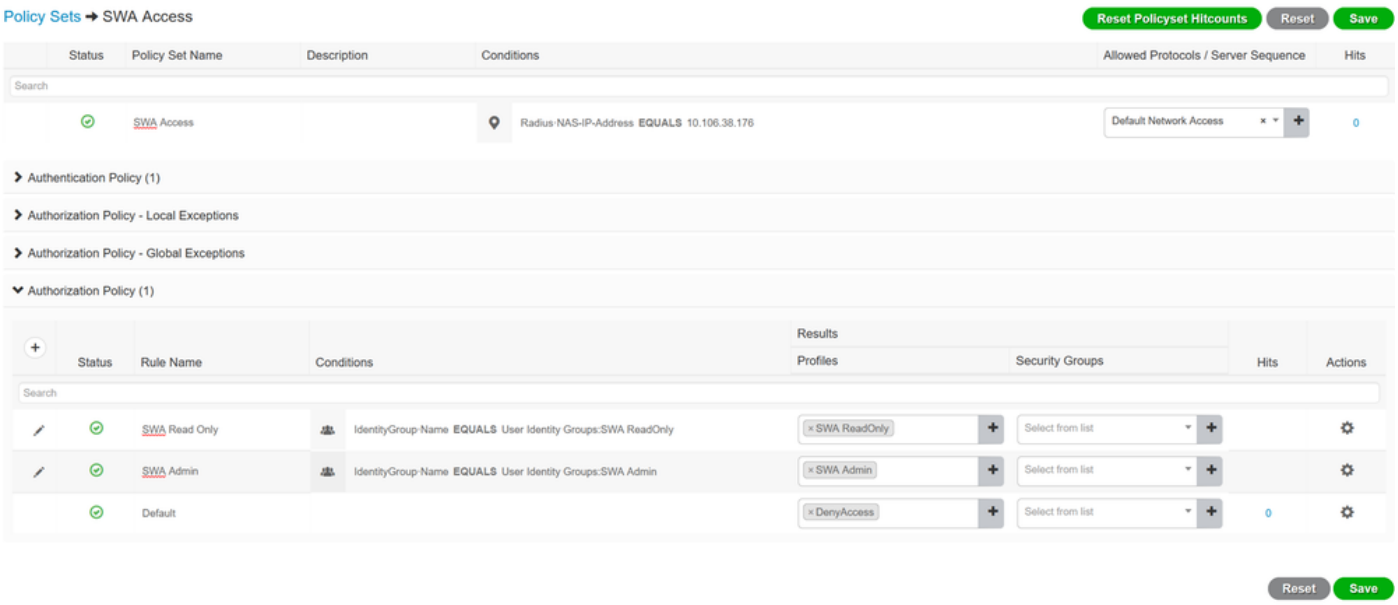
10.2. Set the conditions to match the **Dictionary Identity Group** with **Attribute Name Equals User Identity Groups: SWA ReadOnly** and click **Use**.



Select Authorization Policy for ReadOnly User Group

---

11. Set the **Authorization Profile** respectively for each rule and click **Save**.

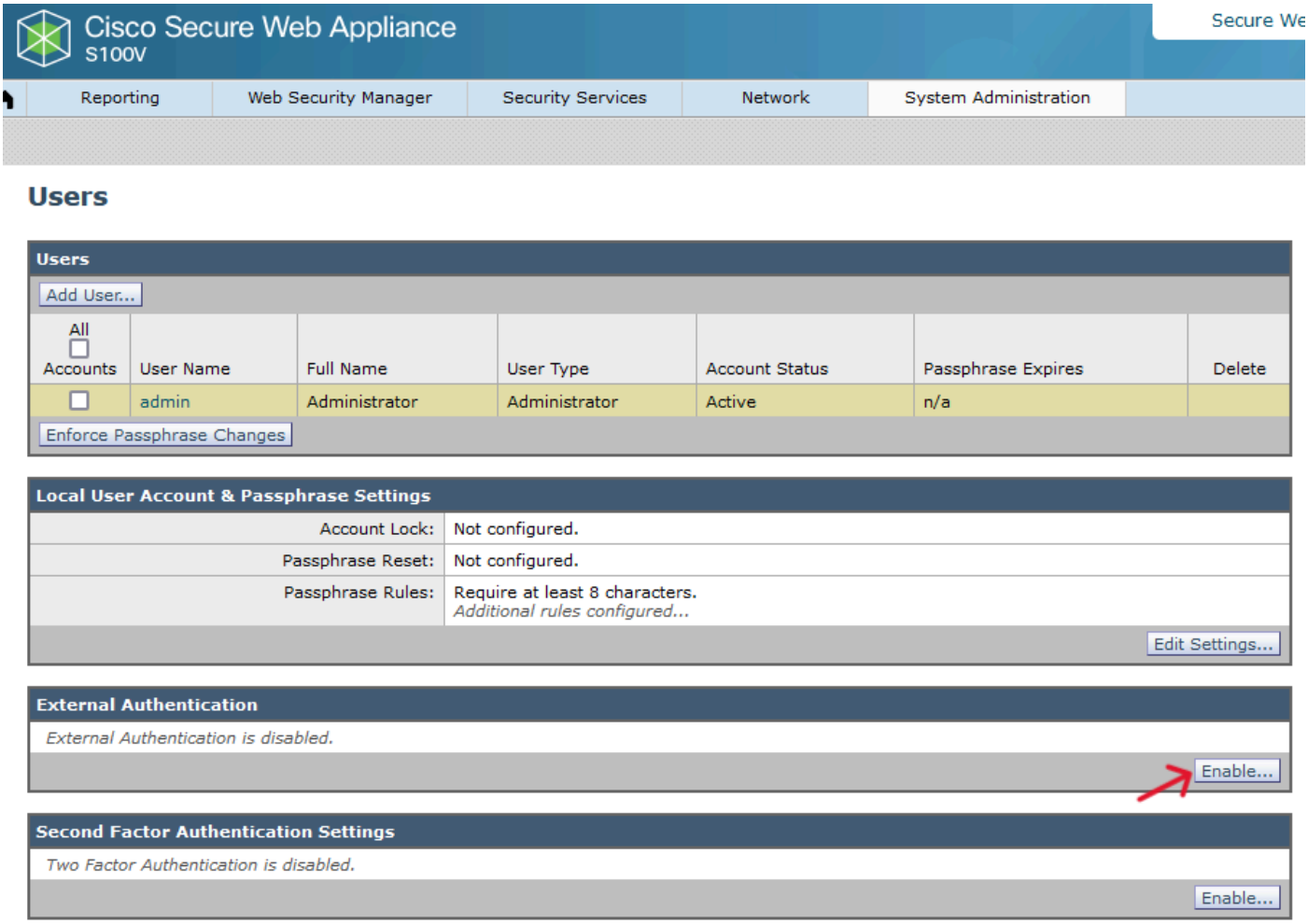


Select Authorization Profile

SWA Configuration

1. From the SWA GUI, choose **System Administration** and select **Users**.

2. Click **Enable** in **External Authentication**.



Enable External Authentication in SWA

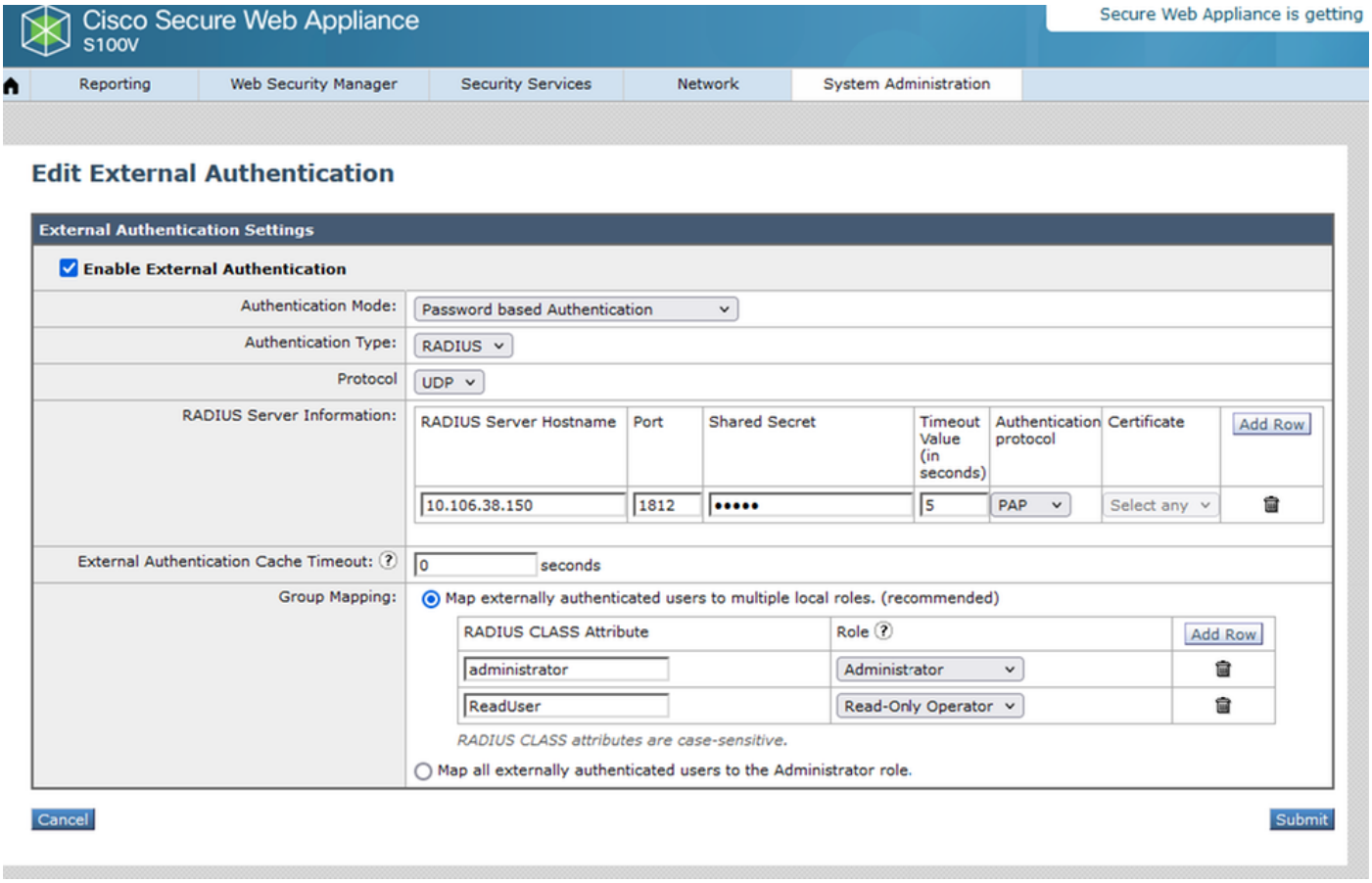
---

3. Enter the IP address or Fully Qualified Domain Name (FQDN) of the ISE in **RADIUS Server Hostname** field and enter the same **Shared Secret** that was configured in **Step 2**, ISE Configuration.

4. Select **Map externally authenticated users to multiple local roles** in **Group Mapping**.

4.1. Enter **Administrator** in the **RADIUS CLASS Attribute** field and select the **Role Administrator**.

4.2. Enter **ReadUser** in the **RADIUS CLASS Attribute** field and select the **Role Read-Only Operator**.

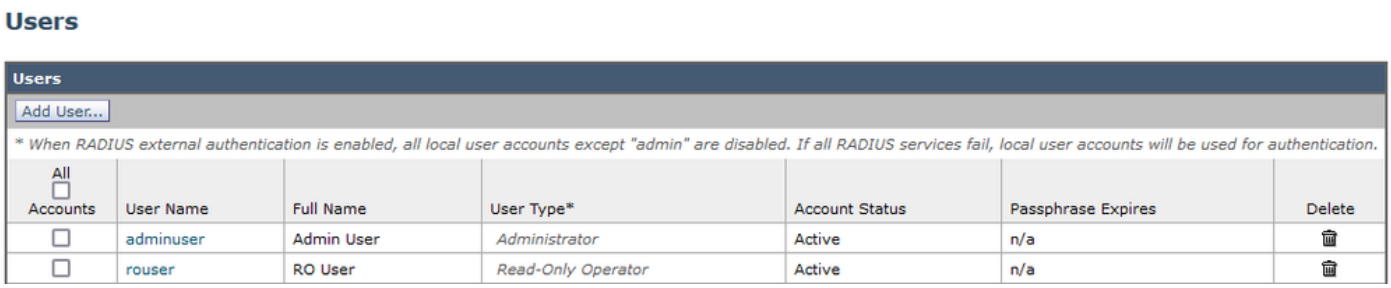


External Authentication Configuration for RADIUS Server

---

5. To configure **Users** in SWA, click **Add User**. Enter the **User Name** and select **User Type**, which is required for the desired role. Enter the **Passphrase** and **Retype Passphrase**, which is required for GUI access, if the appliance cannot connect to any external RADIUS server.

Note: If the appliance cannot connect to any external server, it tries to authenticate the user as a local user defined on the Secure Web Appliance.



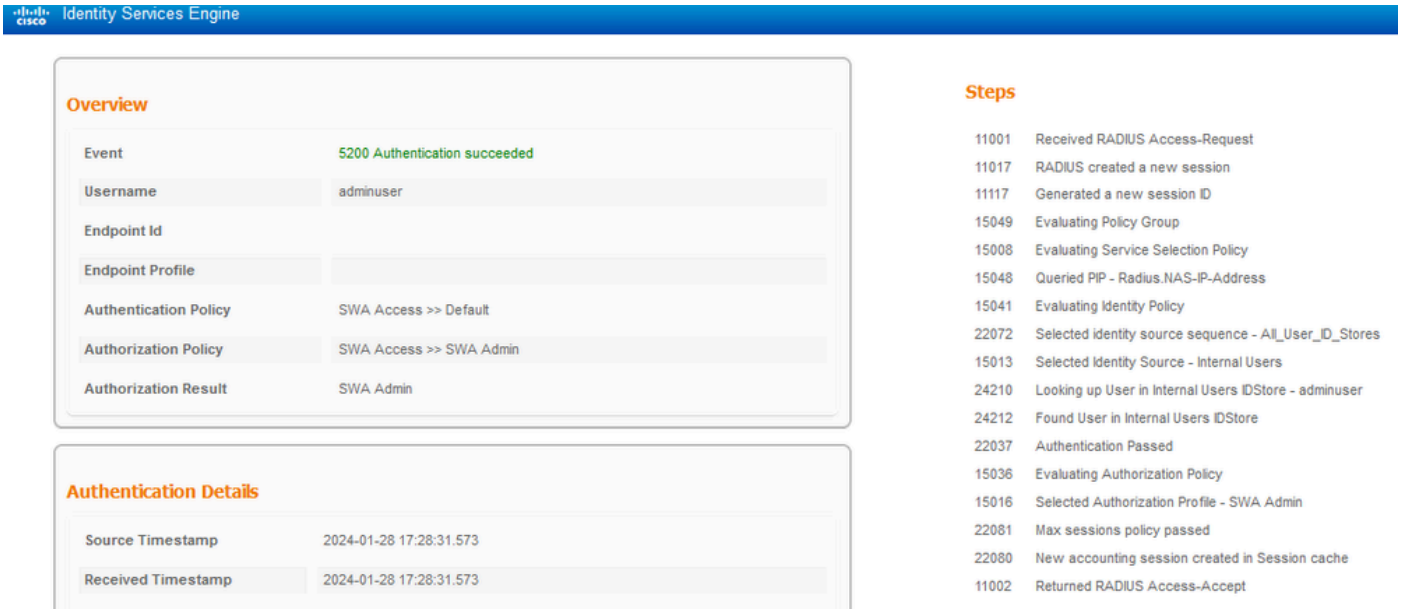
User configuration in SWA

---

6. Click **Submit** and **Commit** Changes.

Verify

Access the SWA GUI with the configured user credentials and check the live logs in ISE. To check the live logs in ISE navigate to **Operations > Live Logs**:



Verify User Login ISE

Related Content

- User Guide for AsyncOS 14.0 for Cisco Secure Web Appliance
- ISE 3.0 Admin Guide
- ISE Compatibility Matrix for Secure Web Appliance
- Cisco Technical Support & Downloads