

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 Information](#)

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 knowledge in Cisco Secure Web Appliance.
- Knowledge of authentication and authorization policies configuration on ISE.
- Basic RADIUS knowledge.

Cisco recommends that you also have:

- SWA and ISE administration access.
- Compatible WSA and ISE versions.

Components Used

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

- SWA 14.0.2-012
- ISE 3.0.0

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 external authentication configuration.

Network Topology



Network Topology Diagram

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

Configure

ISE Configuration

Step 1. Add a new Network Device. Navigate to **Administration > Network Resources > Network Devices > +Add**.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Network Resources' menu is further expanded to show 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', and 'External MDM'. The 'Network Devices' page is active, displaying a table with columns for 'Name', 'IP/Mask', 'Profile Name', 'Location', and 'Type'. The table is currently empty, with the text 'No data available' at the bottom right. The page also includes a sidebar with 'Network Devices', 'Default Device', and 'Device Security Settings' options, and a toolbar with 'Edit', 'Add', 'Duplicate', 'Import', 'Export', 'Generate PAC', and 'Delete' actions.

Add SWA as Network Device in ISE

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

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



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

Network Devices

Default Device

Device Security Settings

[Network Devices List > SWA](#)

Network Devices

* Name

Description

IP Address /

* Device Profile  Cisco

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Configure SWA Network Device Shared Key

Step 2.1. Click Submit.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret ⓘ

CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required ⓘ

Shared Secret ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA ⓘ

DNS Name

General Settings

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

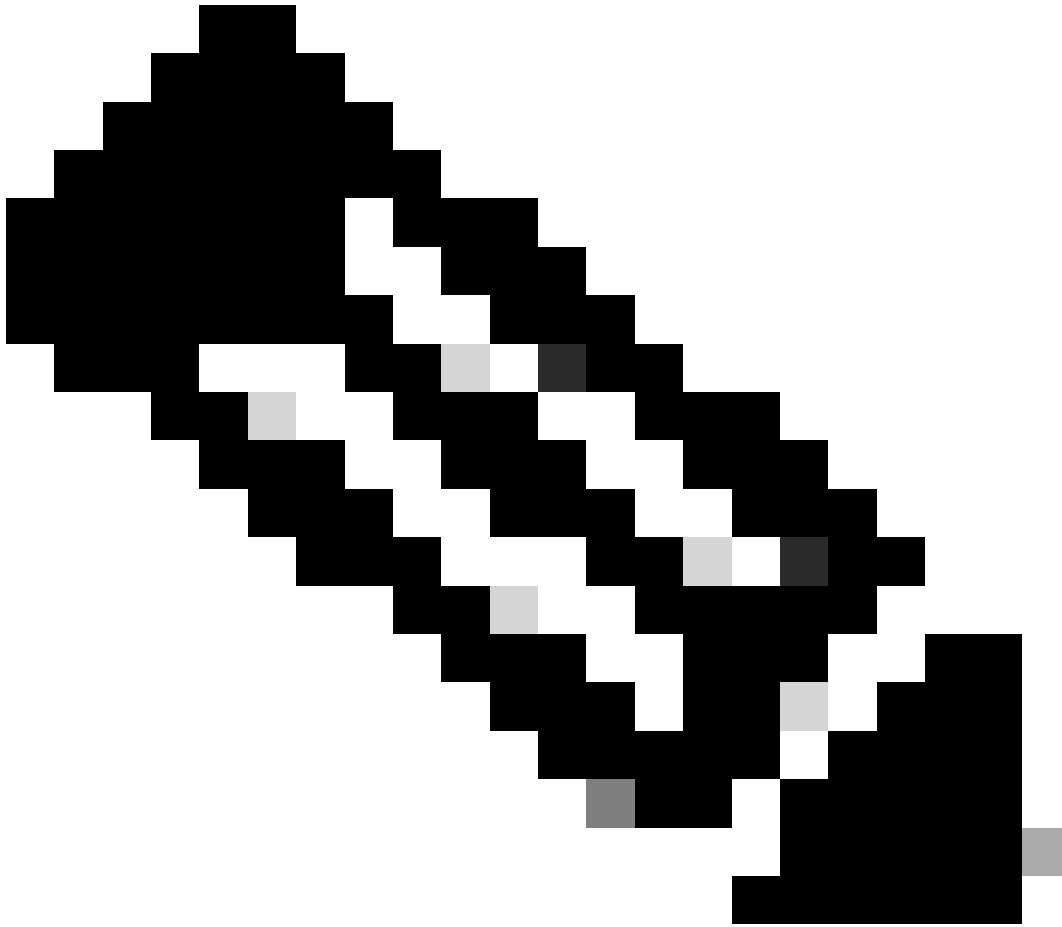
▶ TACACS Authentication Settings

▶ SNMP Settings

▶ Advanced TrustSec Settings

Submit Network Device Configuration

Step 3. Create the required User Identity Groups. Navigate to **Administration > Identity Management > Groups > User Identity Groups > + Add.**



Note: You need to configure different user groups to match different type of users.

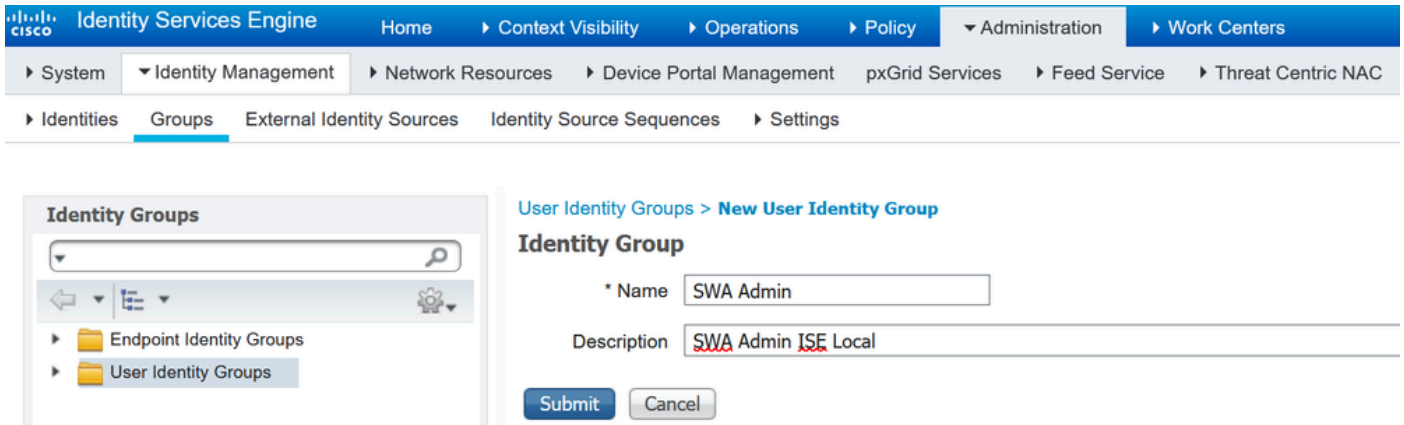
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Identity Management' menu is further expanded to show 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' menu item is selected.

The main content area is divided into two sections. On the left, the 'Identity Groups' section shows a search bar and a tree view with 'Endpoint Identity Groups' and 'User Identity Groups'. The 'User Identity Groups' section is active, displaying a table of existing groups.

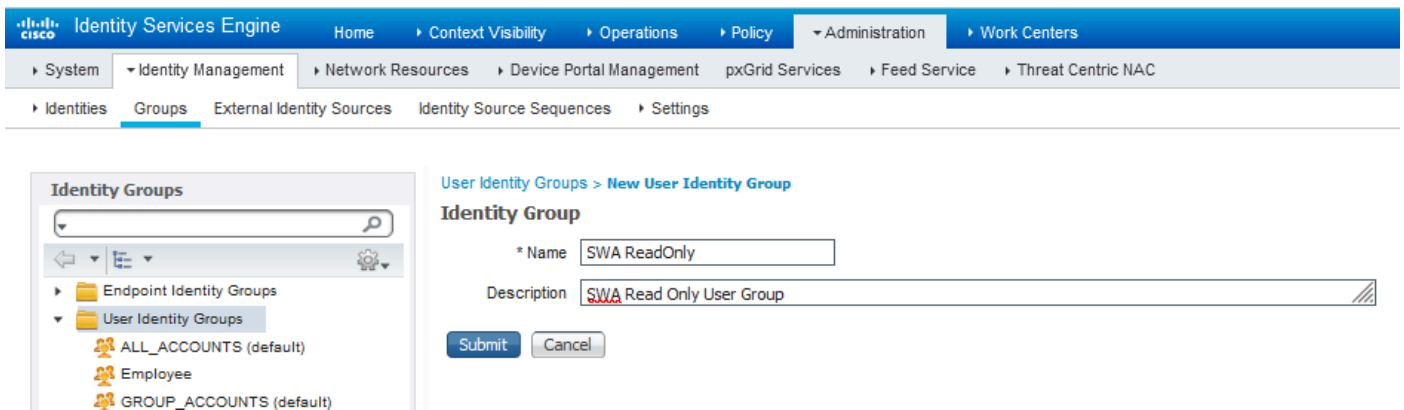
	Name	Description
<input type="checkbox"/>	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/>	Employee	Default Employee User Group
<input type="checkbox"/>	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/>	GuestType_Contractor (default)	Identity group mirroring the guest type

Add User Identity Group

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



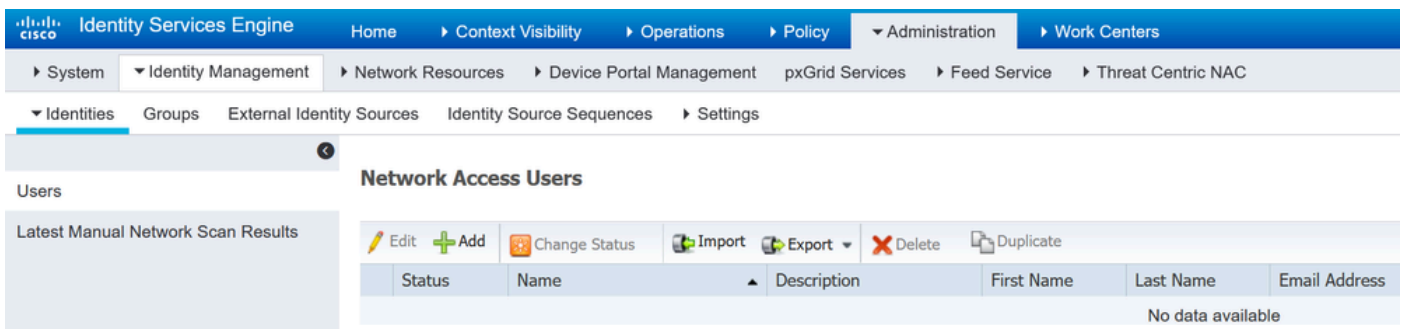
Add User Identity Group



Add User Identity Group for SWA Read Only Users

Step 5. You need to create Network access users that match with user name configured in SWA.

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



Add Local Users in ISE

Step 5.1. You need to create a **Network Access Users** with Administrator rights. Assign a name and password.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name

Status Enabled

Email

Passwords

Password Type:

Password Re-Enter Password

* Login Password

Add Admin User

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

User Groups

Step 5.2. Choose **SWA Admin** in the **User Groups** section.

Assign Admin Group to the Admin User

Step 5.3. You need to create a user with Read Only rights. Assign a name and password.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name

Status Enabled

Email

Passwords

Password Type:

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

Add Read Only User

Step 5.4. Choose **SWA ReadOnly** in the **User Groups** section.

Account Disable Policy

Disable account if date exceeds (yyyy-mm-dd)

User Groups

Submit

Cancel

Assign Read Only User group to the Read Only User

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

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

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

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Add Authorization Profile for Admin Users

Step 6.1. In the **Advanced Attributes Settings**, navigate to **Radius > Class--[25]** and enter the

Advanced Attributes Settings

Radius:Class = Administrator

Attributes Details

Access Type = ACCESS_ACCEPT

Class = Administrator

Submit Cancel

value **Administrator** and click **Submit**.

Add Authorization Profile for Admin Users

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

The screenshot shows the Cisco Identity Services Engine (ISE) interface for creating a new authorization profile. The breadcrumb trail is 'Authorization Profiles > New Authorization Profile'. The page title is 'Authorization Profile'. The form contains the following fields and options:

- * Name:** SWA ReadOnly
- Description:** (empty text field)
- * Access Type:** ACCESS_ACCEPT (dropdown menu)
- Network Device Profile:** Cisco (dropdown menu with a plus icon)
- Service Template:**
- Track Movement:** ⓘ
- Passive Identity Tracking:** ⓘ

Add Authorization Profile for Read Only Users

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

The screenshot shows the 'Advanced Attributes Settings' and 'Attributes Details' sections of the ISE configuration. The 'Advanced Attributes Settings' section shows a table with one row: 'Radius:Class' is set to 'ReadUser'. The 'Attributes Details' section shows the following configuration:

- Access Type = ACCESS_ACCEPT
- Class = ReadUser

At the bottom of the configuration, there are two buttons: 'Submit' and 'Cancel'.

Add Authorization Profile for Read Only Users

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

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

Policy Sets

+	Status	Policy Set Name	Description	Conditions
Search				

Add Policy Set in ISE

Step 8.1. A new line is placed at the top of your **Policy Sets**.

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

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

Conditions Studio

Library

Search by Name

- Catalyst_Switch_Local_Web_Authentication
- Switch_Local_Web_Authentication
- Switch_Web_Authentication
- Wired_802.1X
- Wired_MAB
- Wireless_802.1X
- Wireless_Access
- Wireless_MAB
- WLC_Web_Authentication

Editor

Radius-NAS-IP-Address

Equals 10.106.38.176

Set to 'Is not' Duplicate Save

+ New AND OR

Close Use

Add Policy to Map SWA Network Device

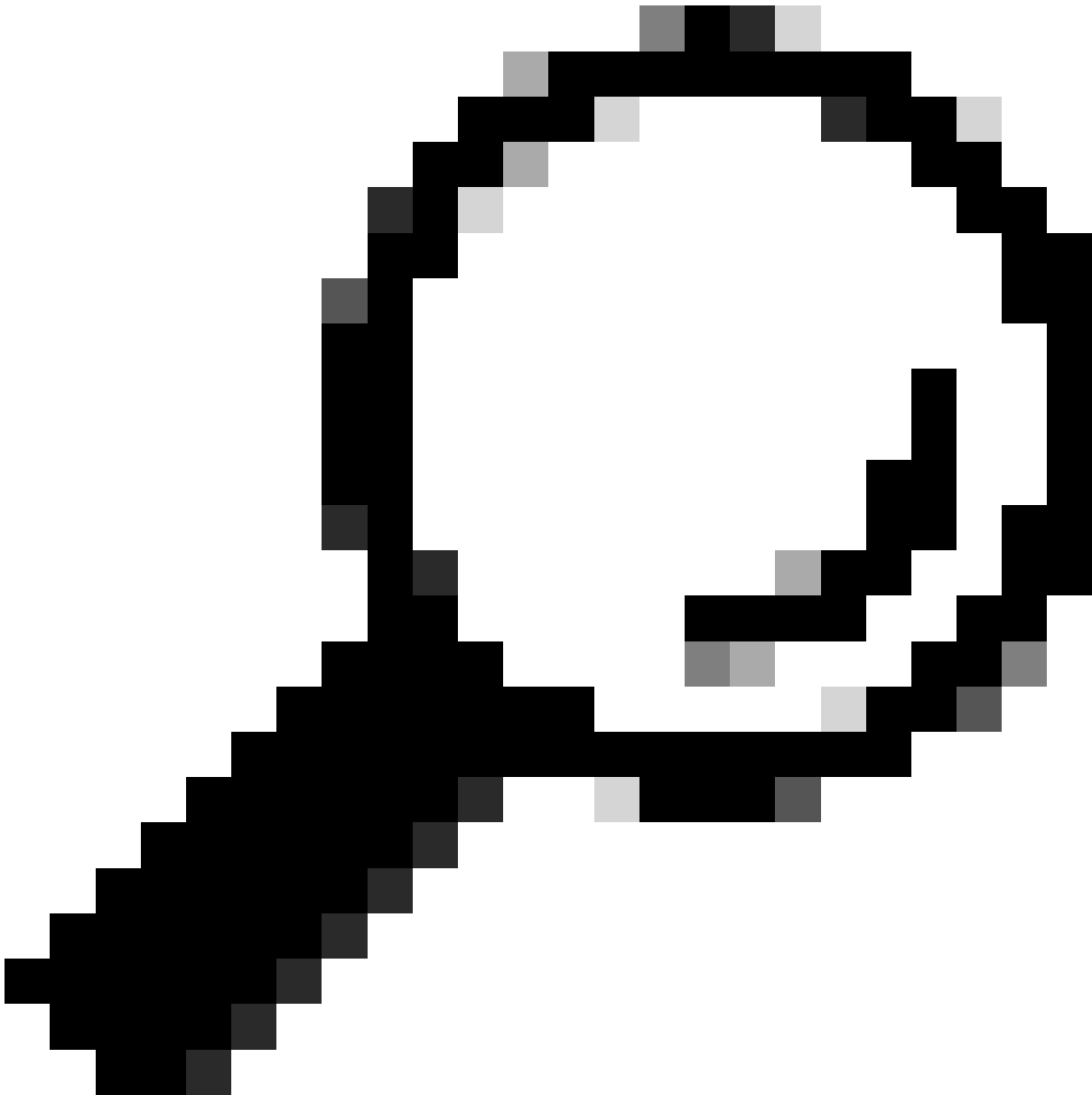
Step 8.2. Click **Save**.

Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search								
	✓	SWA Access		Radius-NAS-IP-Address EQUALS 10.106.38.176	Default Network Access x +		⚙	➔
	✓	Default	Default policy set		Default Network Access x +	0	⚙	➔

Reset Policyset Hitcounts Reset Save

Reset Save

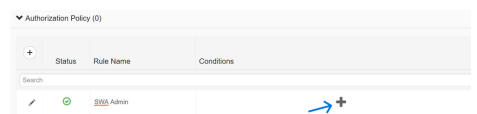


Tip: In this article, the Default Network Access Protocols list is allowed. You can create a new list and narrow down as needed.

Step 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 the access to the user with admin rights.

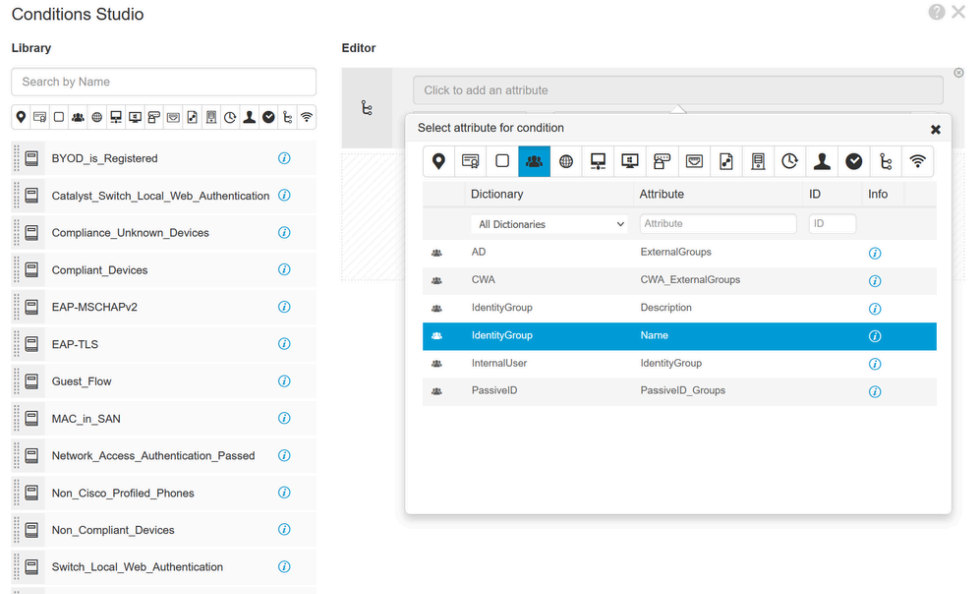
Set a name.

Step 9.1. To create a condition to match Admin user group, click + icon.



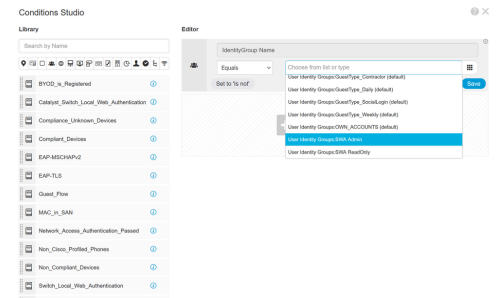
Add Authorization Policy Condition

Step 9.2. Set the conditions to match the **Dictionary Identity Group** with **Attribute Name Equals User**



Identity Groups: SWA admin.

Select Identity Group as Condition



Step 9.3. Scroll down and select User Identity Groups: SWA admin.

Scroll Down and Select Identity Group Name



Step 9.4. Click Use.

Conditions Studio



Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Compliant_Devices

EAP-MSCHAPv2

EAP-TLS

Guest_Flow

MAC_in_SAN

Network_Access_Authentication_Passed

Non_Cisco_Profiling_Phones

Editor

IdentityGroup-Name

Equals

× User Identity Groups:SWA Admin

Set to 'Is not'

You can only select 1 item

Save

+ New AND OR

Close

Use

Select Authorization Policy for SWA Admin User Group

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

Set a name.

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

Conditions Studio



Library

Search by Name

BYOD_is_Registered

Catalyst_Switch_Local_Web_Authentication

Compliance_Unknown_Devices

Compliant_Devices

EAP-MSCHAPv2

EAP-TLS

Guest_Flow

MAC_in_SAN

Network_Access_Authentication_Passed

Non_Cisco_Profiling_Phones

Editor

IdentityGroup-Name

Equals

× User Identity Groups:SWA ReadOnly

Set to 'Is not'

Duplicate

Save

+ New AND OR

Close

Use

Select Authorization Policy for ReadOnly User Group

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

Policy Sets → SWA Access Reset Policyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	SWA Access		Radius-NAS-IP-Address EQUALS 10.106.38.176	Default Network Access x +	0

Authentication Policy (1)
Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy (1)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
✎	✓	SWA Read Only	IdentityGroup-Name EQUALS User Identity Groups:SWA ReadOnly	SWA ReadOnly +	Select from list +		⚙
✎	✓	SWA Admin	IdentityGroup-Name EQUALS User Identity Groups:SWA Admin	SWA Admin +	Select from list +		⚙
	✓	Default		DenyAccess +	Select from list +	0	⚙

Reset Save

Select Authorization Profile

SWA Configuration

Step 1. From SWA GUI navigate to **System Administration** and click **Users**.

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



Users

Users

[Add User...](#)

<input type="checkbox"/> All Accounts	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	

[Enforce Passphrase Changes](#)

Local User Account & Passphrase Settings

Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. Additional rules configured...

[Edit Settings...](#)

External Authentication

External Authentication is disabled.

[Enable...](#)

Second Factor Authentication Settings

Two Factor Authentication is disabled.

[Enable...](#)

Enable External Authentication in SWA

Step 3. Enter IP address or FQDN of the ISE in **RADIUS Server Hostname** field and enter the same Shared Secret that is configured in the Step 2, ISE Configuration.

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

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

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



Edit External Authentication

External Authentication Settings

Enable External Authentication

Authentication Mode: Password based Authentication

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:							Add Row
RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Certificate		
10.106.38.150	1812	*****	5	PAP	Select any		

External Authentication Cache Timeout: 0 seconds

Group Mapping:

Map externally authenticated users to multiple local roles. (recommended)

RADIUS CLASS Attribute	Role	Add Row
administrator	Administrator	
ReadUser	Read-Only Operator	

RADIUS CLASS attributes are case-sensitive.

Map all externally authenticated users to the Administrator role.

Cancel Submit

External Authentication Configuration for RADIUS Server

Step 5: To configure **Users** in SWA, click **Add User**. Enter **User Name** and select **User Type** required for the desired role. Enter **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.

Users

Users						
Add User..						
<small>* When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.</small>						
<input type="checkbox"/> All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	adminuser	Admin User	Administrator	Active	n/a	
<input type="checkbox"/>	rouser	RO User	Read-Only Operator	Active	n/a	

User configuration in SWA

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

Verify

Access 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**:

Overview

Event	5200 Authentication succeeded
Username	adminuser
Endpoint Id	
Endpoint Profile	
Authentication Policy	SWA Access >> Default
Authorization Policy	SWA Access >> SWA Admin
Authorization Result	SWA Admin

Authentication Details

Source Timestamp	2024-01-28 17:28:31.573
Received Timestamp	2024-01-28 17:28:31.573

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Radius.NAS-IP-Address
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore - adminuser
24212	Found User in Internal Users IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15016	Selected Authorization Profile - SWA Admin
22081	Max sessions policy passed
22080	New accounting session created in Session cache
11002	Returned RADIUS Access-Accept

Verify User Login ISE

Related Information

- [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](#)