

# Configure SWA Second Factor Authentication with ISE as a RADIUS Server

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

### [Network Topology](#)

### [Configuration Steps](#)

[ISE Configuration](#)

[SWA Configuration](#)

### [Verify](#)

### [References](#)

---

## Introduction

This document describes how to configure second factor authentication on Secure Web Appliance with Cisco Identity Service Engine as a RADIUS server.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge in SWA.
- Knowledge of authentication and authorization policies configuration on ISE.
- Basic RADIUS knowledge.

Cisco recommends that you also have:

- Secure Web Appliance (SWA) and Cisco Identity Service Engine (ISE) administration access.
- Your ISE is integrated to Active Directory or LDAP.
- Active Directory or LDAP is configured with a username 'admin' to authenticate SWA default 'admin' account.
- 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 second factor authentication for administrative users on SWA, the device verifies the user credential with the RADIUS server for the second time after verify credentials configured in SWA.

## Network Topology



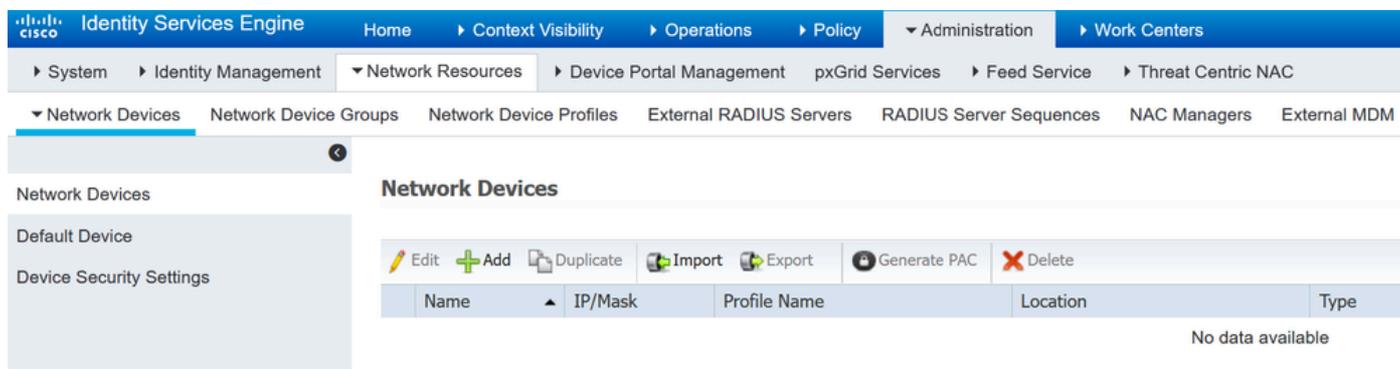
Image- Network Topology Diagram

Administrative users access SWA on port 443 with their credentials. SWA verifies the credentials with the RADIUS server for second factor authentication.

## Configuration Steps

### ISE Configuration

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



Add SWA as Network Device in ISE

**Step 2.** Configure Network device in ISE.

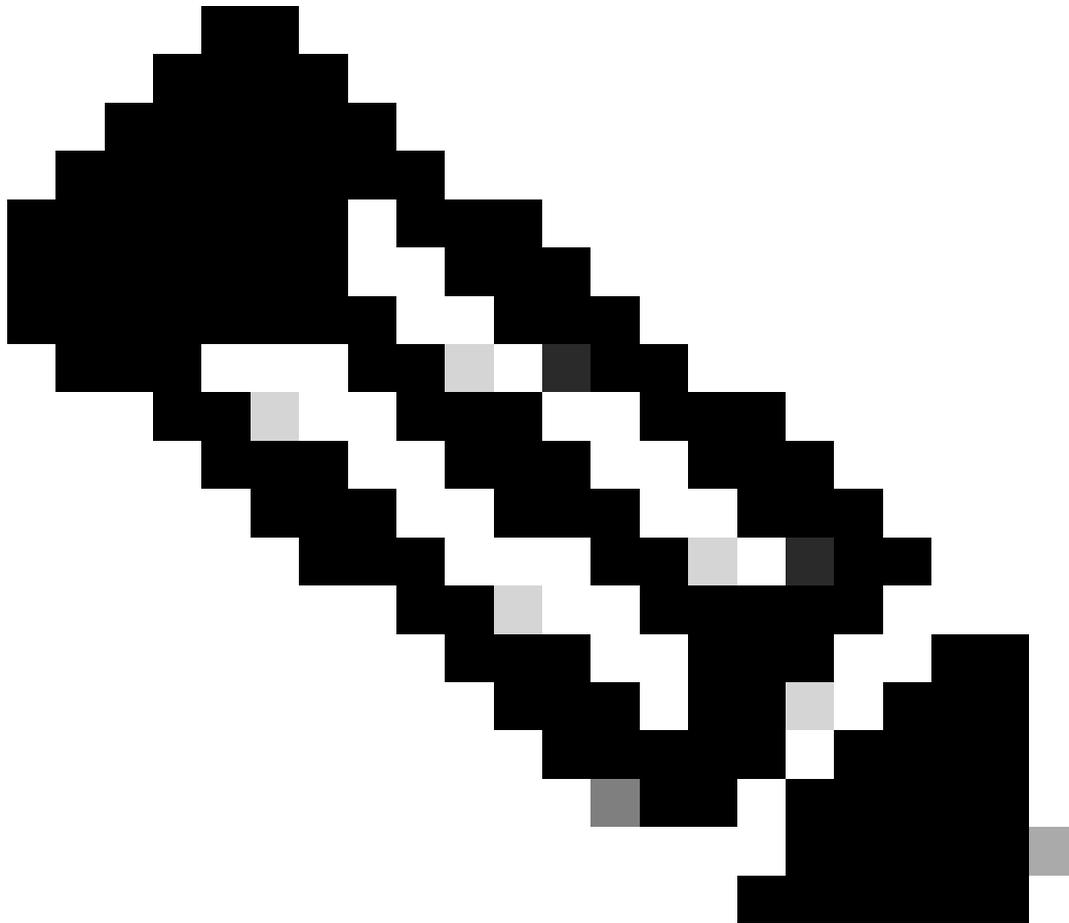
**Step 2.1.** Assign a **Name** to the network device object.

**Step 2.2.** Insert the SWA **IP address**.

**Step 2.3.** Check the RADIUS checkbox.

**Step 2.4.** Define a Shared Secret.

---



**Note:** The same key must be used later to configure the SWA.

---

Network Devices

Default Device

Device Security Settings

[Network Devices List > SWA](#)

### Network Devices

\* Name

Description

IP Address  \* IP :  /

\* 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 2.5.** 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.** You need to create **Network Access Users** that match with user name configured in SWA. Navigate to **Administration > Identity Management > Identities > + Add.**

Identity Services Engine Administration > Work Centers > Administration > Identity Management > Identities > Network Access Users

Users

Latest Manual Network Scan Results

**Network Access Users**

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address
No data available					

Add Local Users in ISE

**Step 3.1.** Assign a **Name**.

**Step 3.2.** (Optional) Enter the Email address of the user.

**Step 3.3.** Set **Password**.

**Step 3.4.** Click **Save**.

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 a local User in ISE

**Step 4.** Create policy set 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.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Policy Sets | Profiling | Posture | Client Provisioning | Policy Elements

**Policy Sets**

+	Status	Policy Set Name	Description	Conditions
Search				

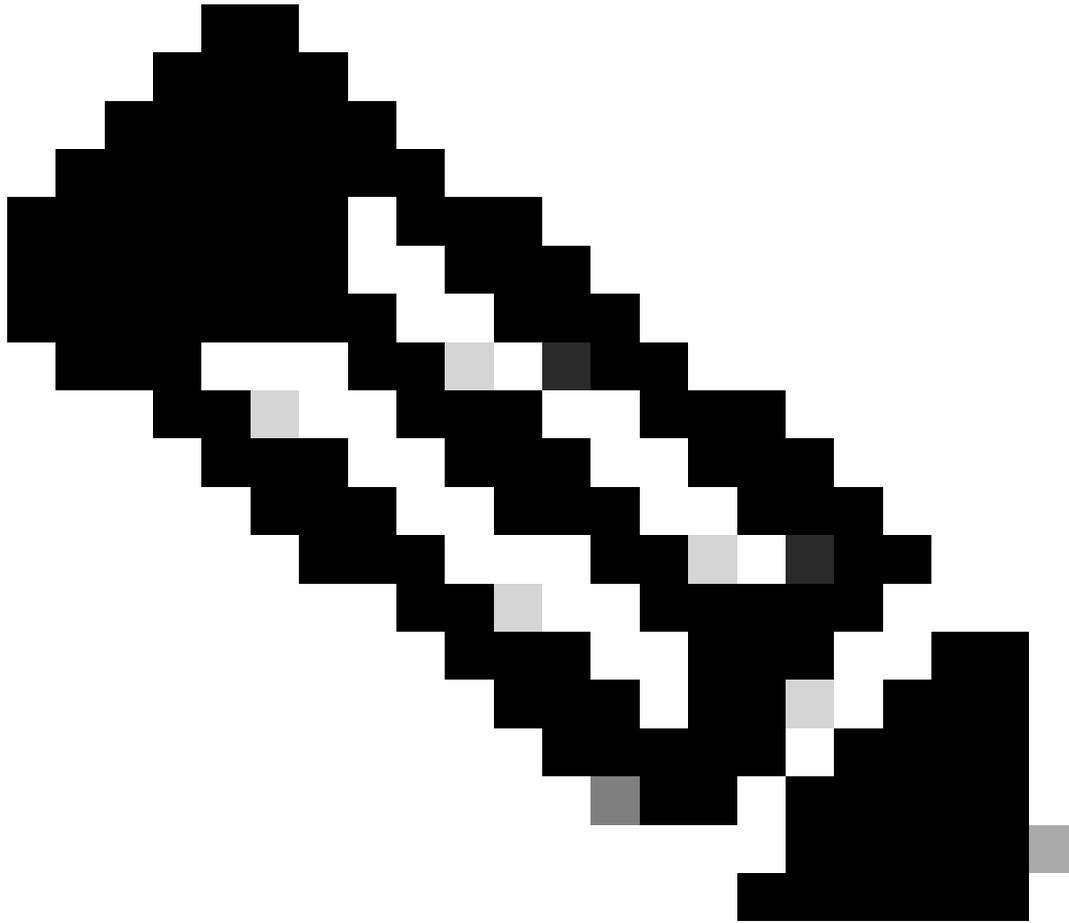
Add Policy Set in ISE

**Step 4.1.** A new line is placed at the top of your **Policy Sets**. Enter Name for new policy.

**Step 4.2.** Add a condition for **RADIUS NAS-IP-Address** attribute to match the SWA IP address.

**Step 4.3.** Click **Use** to keep the changes and exit the editor.





**Note:** This example allowed the Default Network Access Protocols list. You can create a new list and narrow it down as needed.

---

**Step 5.** To view the new **Policy Sets**, click the ">" icon in the **View** column.

**Step 5.1.** Expand the Authorization Policy menu and click the + icon to add a new rule to allow the access to all authenticated users.

**Step 5.2.** Set a name.

**Step 5.3.** Set the conditions to match the Dictionary **Network Access** with Attribute **AuthenticationStatus Equals AuthenticationPassed** and click **Use**.



# SWA Configuration

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

**Step 2.** Click **Enable** in **Second Factor Authentication Settings**.

The screenshot shows the Cisco Secure Web Appliance (S100V) GUI. The navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The 'Users' section contains a table with the following data:

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

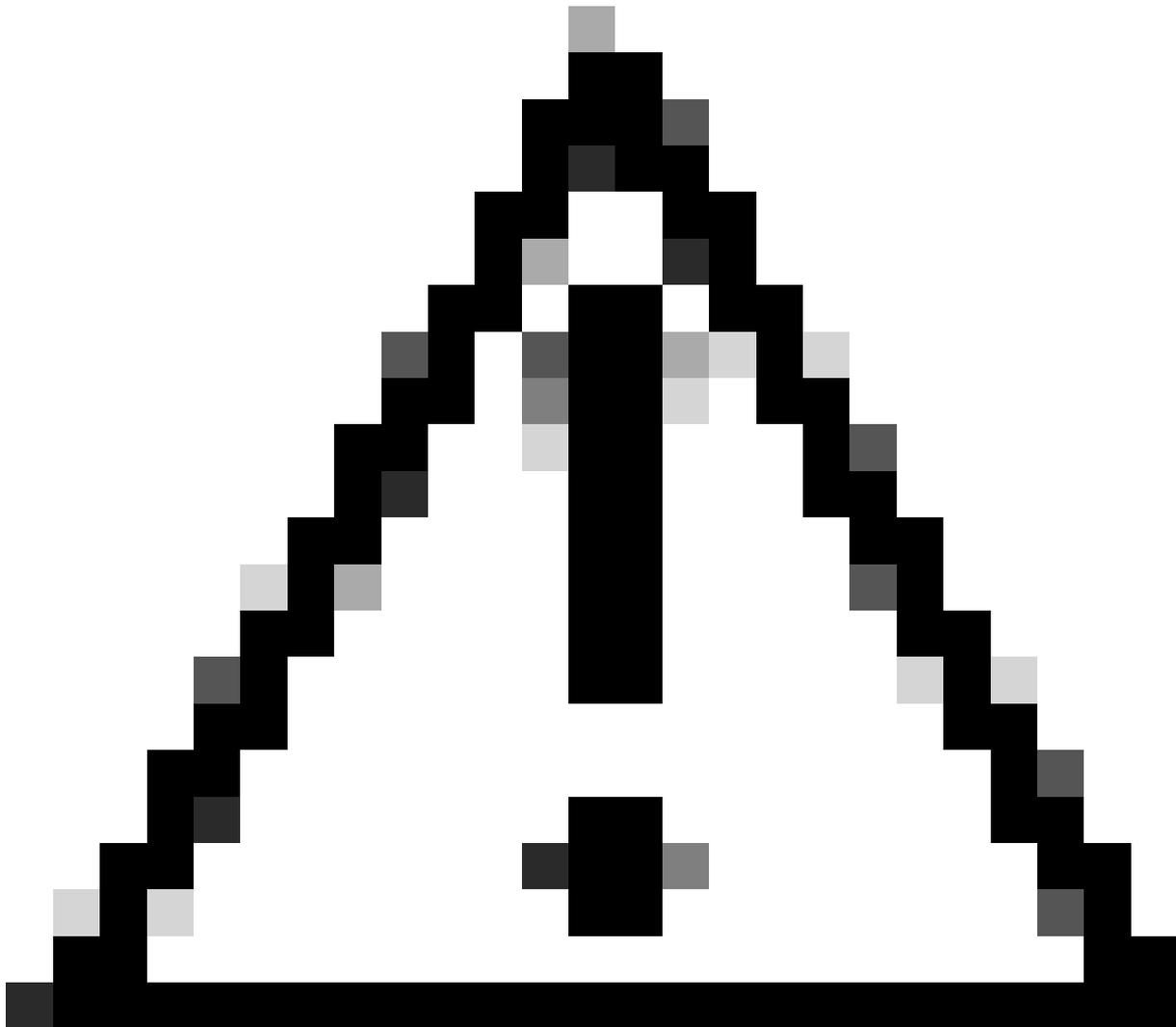
Below the table are three settings panels:

- 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... (indicated by a blue arrow)

*Enable Second Factor Authentication in SWA*

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

**Step 4.** Select required **Predefined Roles** which you need Second Factor enforcement to be enabled.



**Caution:** If you enable second factor authentication in SWA, default 'admin' account also be enabled with Second Factor enforcement. You have to integrate ISE with LDAP or Active Directory (AD) to authenticate 'admin' credentials as ISE does not allow you to configure 'admin' as a Network Access User.

---



## Users

Users						
<a href="#">Add User...</a>						
<input type="checkbox"/>	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	
<a href="#">Enforce Passphrase Changes</a>						

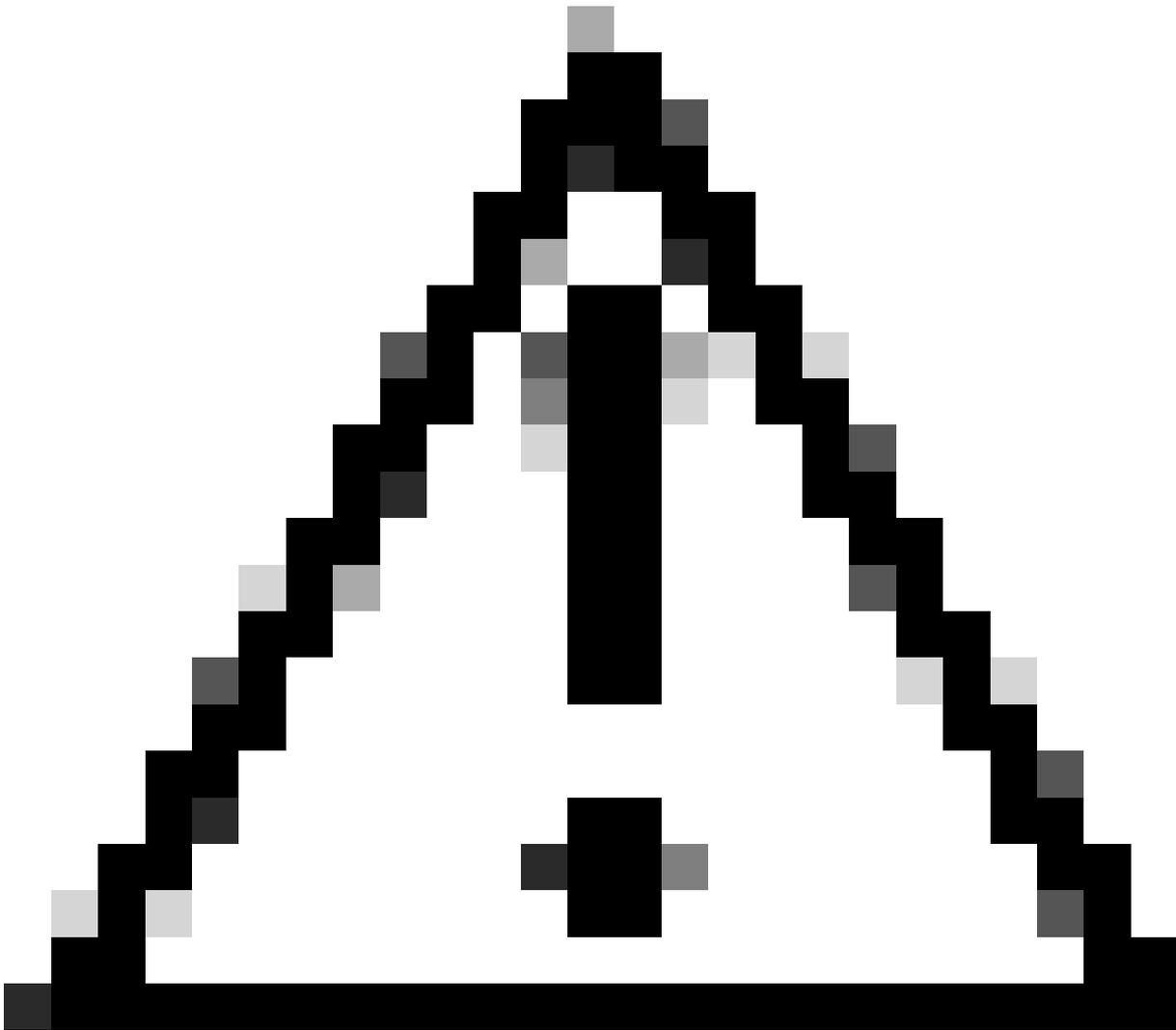
Local User Account & Passphrase Settings	
Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. <i>Additional rules configured...</i>
<a href="#">Edit Settings...</a>	

External Authentication
<i>External Authentication is disabled.</i>
<a href="#">Enable...</a>

Second Factor Authentication Settings
<i>Two Factor Authentication is disabled.</i>
<a href="#">Enable...</a>



Enable Second Factor Authentication in SWA



**Caution:** If you enable second factor authentication in SWA, default 'admin' account also be enabled with Second Factor enforcement. You have to integrate ISE with LDAP or Active Directory (AD) to authenticate 'admin' credentials as ISE does not allow you to configure 'admin' as a Network Access User.

---

## Second Factor Authentication

**Second Factor Authentication Settings**

**Enable Second Factor Authentication**

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:	RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	<a href="#">Add Row</a>
	<span style="border: 1px solid #ccc; padding: 2px;">10.106.38.150</span>	<span style="border: 1px solid #ccc; padding: 2px;">1812</span>	<span style="border: 1px solid #ccc; padding: 2px;">*****</span>	<span style="border: 1px solid #ccc; padding: 2px;">5</span>	<span style="border: 1px solid #ccc; padding: 2px;">PAP</span>	

**User Role Privileges**

Configure user roles for Second Factor Authentication

Second Factor Authentication is enforced to:

Predefined Roles

- Administrator
- Operator
- Read-Only Operator
- Guest

**Two Factor Login Page**

Appearance:

Current Logo:

Use Current Logo

Upload Custom Logo from Local Computer: Browse... No file selected.

Company Name:   
(Max 150 characters only)

Custom text Information:   
(Max 500 characters only)

Login help Information:   
(Examples: For login trouble Please contact, Contact Name ,123-1234-123,admin@example.com or help URL. Note:Max 500 characters only)

[View Existing Two Factor Login Page](#)

Cancel
Submit

Configure Second Factor Authentication

**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**.

### Users

**Users**

Add User...

\* 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.

<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. After successful authentication, you get redirected to secondary authentication page. Here, you need to enter the secondary authentication credentials configured in ISE.



Passcode:

Login

Copyright © 2003-2022 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

*Verify Second Factor Login*

## References

- [User Guide for AsyncOS 14.0 for Cisco Secure Web Appliance](#)
- [ISE 3.0 Admin Guide](#)
- [ISE Compatibility Matrix for Secure Web Appliance](#)
- [Integrate AD for ISE GUI and CLI Log in](#)