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 |
| <u>Verify</u> |
| 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 Directlory 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.**

| dentity Services Engine | Home Conte | xt Visibility 🔹 🕨 | Operations | Policy | istration V | Vork Centers | |
|------------------------------------|---------------------|-----------------------------|--------------------|------------------|-----------------|------------------|--------------|
| System Identity Management | ✓ Network Resources | Device Port | tal Management | pxGrid Services | Feed Service | Threat Centric N | AC |
| ▼ Network Devices Network Device 0 | Groups Network De | vice Profiles E | External RADIUS Se | ervers RADIUS Se | erver Sequences | NAC Managers | External MDM |
| 0 | | | | | | | |
| Network Devices | Network Devi | ces | | | | | |
| Default Device | | | | | | | |
| Device Security Settings | 🥖 Edit 🛛 🕂 Add | Duplicate | Export | Generate PAG | C 🗙 Delete | | |
| , , | Name | IP/Mask | Profile Nam | ne | Location | | Туре |
| | | | | | | No data a | vailable |
| | | | | | | | |



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 | Network Devices List > SWA |
|--|---|
| Default Device Device Security Settings | Name SWA Description |
| | IP Address • IP : 10.106.38.176 / 32 |
| | * Device Profile Cisco • • Model Name • Software Version • * Network Device Group Location All Locations • Set To Default IPSEC No • Set To Default Device Type All Device Types • Set To Default |
| | RADIUS Authentication Settings |
| | RADIUS UDP Settings |
| | Protocol RADIUS |
| | * Shared Secret Show |

Configure SWA Network Device Shared Key

Step 2.5. Click Submit.

| | RADIUS Authentication Settings |
|-----|---|
| | |
| | RADIUS UDP Settings |
| | Protocol RADIUS |
| | * Shared Secret Show |
| | Use Second Shared Secret 🔲 🕡 |
| | Show |
| | CoA Port 1700 Set To Default |
| | RADIUS DTLS Settings () |
| | DTLS Required 🔲 🕡 |
| | Shared Secret radius/dtls (i) |
| | CoA Port 2083 Set To Default |
| | Issuer CA of ISE Certificates for CoA Select if required (optional) |
| | DNS Name |
| | |
| | General Settings |
| | Enable KeyWrap 🗌 🕡 |
| | * Key Encryption Key Show |
| | * Message Authenticator Code Key Show |
| | Key Input Format ASCII HEXADECIMAL |
| | |
| | TACACS Authentication Settings |
| | SNMP Settings |
| | Advanced TrustSec Settings |
| Sul | Omit Cancel |

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.**

| dentity Services Engine | Home → Context Visibility → O | perations Policy Administratio | n Work Centers |
|------------------------------------|---------------------------------------|-------------------------------------|------------------------------------|
| System Identity Management | Network Resources Device Portal | Management pxGrid Services + Feed | Service |
| ◄ Identities Groups External Ident | ity Sources Identity Source Sequences | Settings | |
| 0 | | | |
| Users | Network Access Users | | |
| Latest Manual Network Scan Results | 🖋 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.

| dentity Services Engine | Home | ility • Operations | Policy + Adr | ministration | Work Centers | |
|---|---|---|-----------------|----------------|----------------------------------|-------------------------|
| + System - Identity Managemen | t + Network Resources + De | evice Portal Management | pxGrid Services | Feed Servi | ce 🔸 Threat Cent | ric NAC |
| - Identities Groups External I | dentity Sources Identity Source | Sequences + Settings | 5 | | | |
| Users Latest Manual Network Scan Results | Network Access Users L Network Access Network Access * Name rouser Status Enai | ist > New Network Acces User Died 👻 | ss User | | | |
| | ▼ Passwords | | - | | | |
| | Password Type: | Internal Users | • | | | |
| | | Password | Re-E | Enter Password | | |
| | * Login Password | ••••• | •• | ••••• | | Generate Password) (i) |
| | Enable Password | 1 | | | | Generate Password (j) |

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.

| uluilu cisco | Identit | / Services | Engine | Home | ▸ Conte | ext Visibility | ▸ Operations | ▼Policy | Administration | Work Centers |
|-----------------|---------|------------|------------|-----------------|---------|----------------|--------------|---------|----------------|--------------|
| Polic | y Sets | Profiling | Posture | Client Provisio | oning | Policy Element | nts | | | |
| Polic | y Set | 6 | | | | | | | | |
| + | S | tatus | Policy Set | t Name | | Description | | Condi | tions | |
| Sear | ch | | | | | | | | | |

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.

Conditions Studio

| Librar | у | |
|----------|--|-------------|
| Sear | rch by Name | |
| Q | □ ▲ ⊕ 🖵 🗳 🕾 🖾 🕑 🗜 🥸 🕹 🜑 | ະ ຈີ |
| | Catalyst_Switch_Local_Web_Authentication | () |
| | Switch_Local_Web_Authentication | () |
| | Switch_Web_Authentication | <i>(i)</i> |
| | Wired_802.1X | <i>(i</i>) |
| | Wired_MAB | <i>(i</i>) |
| | Wireless_802.1X | <i>(i</i>) |
| | Wireless_Access | <i>(i</i>) |
| | Wireless_MAB | <i>()</i> |
| | WLC_Web_Authentication | 1 |

| ditor | | | | 0 |
|-------|-----------------|-----------|---------------|------|
| | Radius NAS- | IP-Addres | 55 | |
| • | Equals | ~ | 10.106.38.176 | |
| | Set to 'Is not' | | Duplicate | Save |
| | | | | |
| | | | + New AND OR | |
| | | | | |
| | | | | |

Close Use

Reset Save

Add Policy to Map SWA Network Device

Step 4.4. Click Save.

| Policy | Sets | | | | | Re | eset Policys | et Hitcount | s Reset | Save |
|--------|---------|-----------------|--------------------|------|--|--------------------------------|--------------|-------------|---------|------|
| + | Status | Policy Set Name | Description | Cond | ditions | Allowed Protocols / Server Sec | quence | Hits | Actions | View |
| Search | | | | | | | | | | |
| / | \odot | SWA Access | | 0 | Radius-NAS-IP-Address EQUALS 10.106.38.176 | Default Network Access × | - + | | ٥ | > |
| | ø | Default | Default policy set | | | Default Network Access × | • + | 0 | ٥ | > |

Policy Save



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**.

Conditions Studio

| Librar | У | |
|----------|--|-------------------|
| Sear | rch by Name | |
| Q | | <mark>६</mark> ङ् |
| | BYOD_is_Registered | 1 |
| | $\label{eq:catalyst_Switch_Local_Web_Authenticati} \\ \text{on}$ | <i>(i</i>) |
| | Compliance_Unknown_Devices | 1 |
| | Compliant_Devices | <i>i</i> |
| | Guest_Flow | <i>i</i>) |
| | Network_Access_Authentication_Passed | 1 |
| | Non_Cisco_Profiled_Phones | <i>i</i> |
| | Non_Compliant_Devices | <i>i</i>) |
| | Switch_Local_Web_Authentication | <i>i</i>) |
| | Switch_Web_Authentication | <i>i</i> |
| | Wired_802.1X | <i>i</i> |
| | Wired_MAB | <i>i</i>) |
| | Wireless_802.1X | <i>i</i> |
| | Wireless_MAB | <i>(i</i>) |
| | WLC_Web_Authentication | <i>i</i>) |

| Network Acc | cess-Aut | henticationStatus | | |
|-----------------|--------------------------|----------------------------|-------------------------------|-------------------------------|
| Equals | ~ | AuthenticationPassed | * | |
| Set to 'Is not' | | | Duplicate | Save |
| 5 | Equals et to 'Is not' | Equals v et to 'ls not' | Equals v AuthenticationPassed | Equals AuthenticationPassed |

Close Use

Reset Save

Select Authorization Condition

Step 6. Set the default PermitAccess as Authorization Profile and click Save.

| Policy Se | ts → SV | VA Access | | | | | | | | | | | | | Res | et Policys | et Hitcoun | s Res | save |
|-----------|-------------|--------------------------|----------------|-------------------|--------|---------------|-----------------|------------|--|-----|--|--------|-----------|---|------------------|---------------|-------------|------------|---------|
| | Status | Policy Set Name | Description | Condit | itions | 5 | | | | | | | | | AJ | lowed Prot | ocols / Ser | er Sequenc | e Hits |
| Search | | | | | | | | | | | | | | | | | | | |
| | 0 | SUG Access | | ۰ | Radius | dus NAS-P-Add | ress EQUALS 10. | 106.38.176 | | | | | | | | Default Netwo | ork Access | ** + | |
| ✓ Auther | tication P | olicy (1) | | | | | | | | | | | | | | | | | |
| ٠ | Status | Rule Name | Conditions | | | | | | | | | | | | Use | | | Hits | Actions |
| Search | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | ŧ . | | | | | | | | | |
| | ~ | | | | | | | | | | | | | | Al_User_D_Stores | | ** | | |
| | ۲ | Default | | | | | | | | | | | | | > Options | | | 6 | • |
| > Author | ization Pol | licy - Local Exceptions | | | | | | | | | | | | | | | | | |
| > Author | ization Pol | licy - Global Exceptions | | | | | | | | | | | | | | | | | |
| ✓ Author | zation Pol | licy (2) | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | Resu | ts | | | | | | |
| ٠ | Status | Rule Name | Conditions | | | | | | | | | Profil | es | | Security Groups | | | Hits | Actions |
| Search | | | | | | | | | | | | | | | | | | | |
| 1 | 0 | Stora Users | Network_Access | s_Authentication_ | Passed | sed | | | | | | Pe | rm&Access | + | Select from list | | - + | 5 | ۰ |
| | ø | Default | | | | | | | | | | × De | myAccess | + | Select from list | | | • | ٥ |
| | | | | | | | | | | | | | | | | | | | |

SWA Configuration

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

Step 2. Click Enable in Second Factor Authentication Settings.

| Į | Cisco Sec | cure Web Appliance | | | | Secure We |
|---|-----------|----------------------|-------------------|---------|-----------------------|-----------|
| ١ | Reporting | Web Security Manager | Security Services | Network | System Administration | |
| | | | | | | |

Users

| Users | | | | | | | | | | | |
|-------------------|-----------------------------|------------------|---------------|--|----------------|--------------------|--------------|--|--|--|--|
| Add User | | | | | | | | | | | |
| All Accounts | User Name | Full Name | | User Type | Account Status | Passphrase Expires | Delete | | | | |
| | admin | Administrator | | Administrator | Active | n/a | | | | | |
| Enforce Pa | assphrase Changes | | | | | | | | | | |
| Local User | r Account & Passp | hrase Settings | | | | | | | | | |
| | | Account Lock: | Not c | onfigured. | | | | | | | |
| Passphrase Reset: | | | | Not configured. | | | | | | | |
| | P | assphrase Rules: | Requ Addit | ire at least 8 characters. ional rules configured | | | | | | | |
| | | | | | | E | dit Settings | | | | |
| External A | Authentication | | | | | | | | | | |
| External A | uthentication is disa | bled. | | | | | | | | | |
| | | | | | | | Enable | | | | |
| Second Fa | ictor Authenti <u>catio</u> | on Settings | | | | | | | | | |
| Two Facto | r Authentication is di | isabled. | | | | | 1 | | | | |
| | | | | | | | Enable | | | | |

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.

| Cisco Seo s100v | cure Web Appliance | | | | Secure We |
|--------------------|----------------------|-------------------|---------|-----------------------|-----------|
| Reporting | Web Security Manager | Security Services | Network | System Administration | |
| Reporting | Web Security Manager | Security Services | Network | System Administration | |

Users

| Users | | | | | | |
|-----------------|-------------------|---------------|---------------|----------------|--------------------|--------|
| Add User. | | | | | | |
| All Accounts | User Name | Full Name | User Type | Account Status | Passphrase Expires | Delete |
| | admin | Administrator | Administrator | Active | n/a | |
| Enforce Pa | assphrase 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 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 v | | | | | | | |
| RADIUS Server Information: | RADIUS Server Hostname | RADIUS Server Hostname Port Shared Secret Timeout Value Authentication Add Row Add Row | | | | | | |
| | 10.106.38.150 | 1812 | ••••• | ••• | 5 | | PAP v | Ŵ |
| 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: CISCO. 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) | | | li. | | | | |
| Login help Information: | (Examples:For login trouble Plea characters only) | ase contact, | , Contact | ///. Name ,123-1234-123,au | dmin@exa | ample.co | om or help URL. N | lote:Max 500 |
| | | | | | | View Ex | isting 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 | Add User | | | | | | | |
| * When RADI | * 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. | | | | | | | |
| | | | | | | | | |
| Accounts | User Name | Full Name | User Type* | Account Status | Passphrase Expires | Delete | | |
| | adminuser | Admin User | Administrator | Active | n/a | Ŵ | | |
| | rouser | RO User | Read-Only Operator | Active | n/a | ŵ | | |

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: | |
|--|--|
| Copyright © 2003-2022 Cisco Systems, Inc. All rights reserved. Privacy Statement | |

Verify Second Factor Login

References

- <u>User Guide for AsyncOS 14.0 for Cisco Secure Web Appliance</u>
 <u>ISE 3.0 Admin Guide</u>
- ISE Compatibility Matrix for Secure Web Appliance
 Integrate AD for ISE GUI and CLI Log in