

ISE를 RADIUS 서버로 사용하는 SWA Second Factor Authentication 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 토폴로지](#)

[컨피그레이션 단계](#)

[ISE 구성](#)

[SWA 컨피그레이션](#)

[다음을 확인합니다.](#)

[참조](#)

소개

이 문서에서는 Cisco ISE(Identity Service Engine)를 RADIUS 서버로 사용하는 Secure Web Appliance에서 2단계 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA의 기본 지식
- ISE의 인증 및 권한 부여 정책 컨피그레이션에 대한 지식
- 기본 RADIUS 지식.

Cisco에서는 다음과 같은 기능도 권장합니다.

- SWA(Secure Web Appliance) 및 Cisco ISE(Identity Service Engine) 관리 액세스
- ISE가 Active Directory 또는 LDAP에 통합됩니다.
- Active Directory 또는 LDAP가 사용자 이름 'admin'으로 구성되어 SWA 기본 'admin' 계정을 인증합니다.
- 호환 가능한 WSA 및 ISE 버전.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- SWA 14.0.2-012
- ISE 3.0.0.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SWA의 관리 사용자에게 대해 2차 요인 인증을 활성화하면 디바이스는 SWA에 구성된 자격 증명을 확인한 후 두 번째로 RADIUS 서버에 대한 사용자 자격 증명을 확인합니다.

네트워크 토폴로지



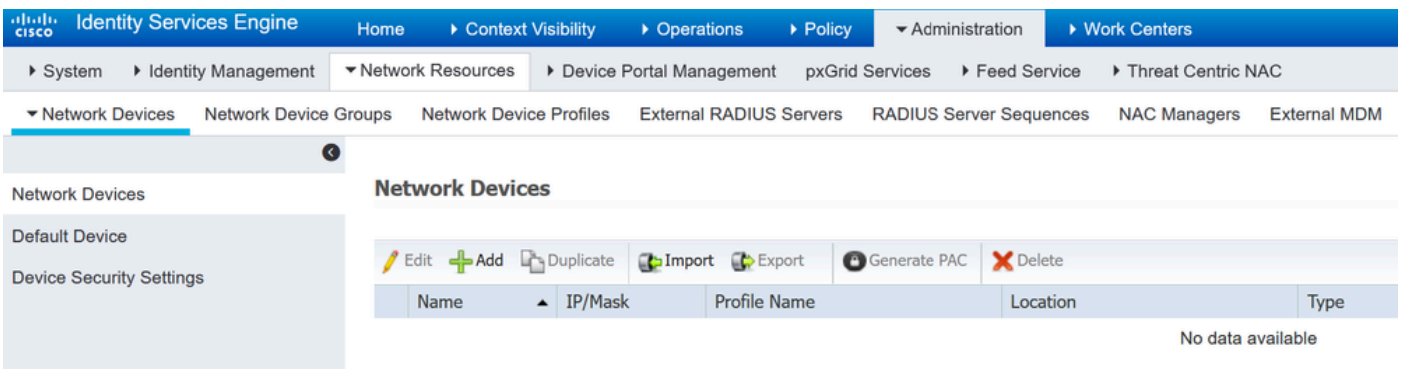
이미지 - 네트워크 토폴로지 다이어그램

관리 사용자는 자격 증명을 사용하여 포트 443의 SWA에 액세스합니다. SWA는 RADIUS 서버에서 2단계 인증을 위해 자격 증명을 확인합니다.

컨피그레이션 단계

ISE 구성

1단계. 새 네트워크 디바이스를 추가합니다. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > +Add(추가)로 이동합니다.



ISE에서 SWA를 네트워크 디바이스로 추가

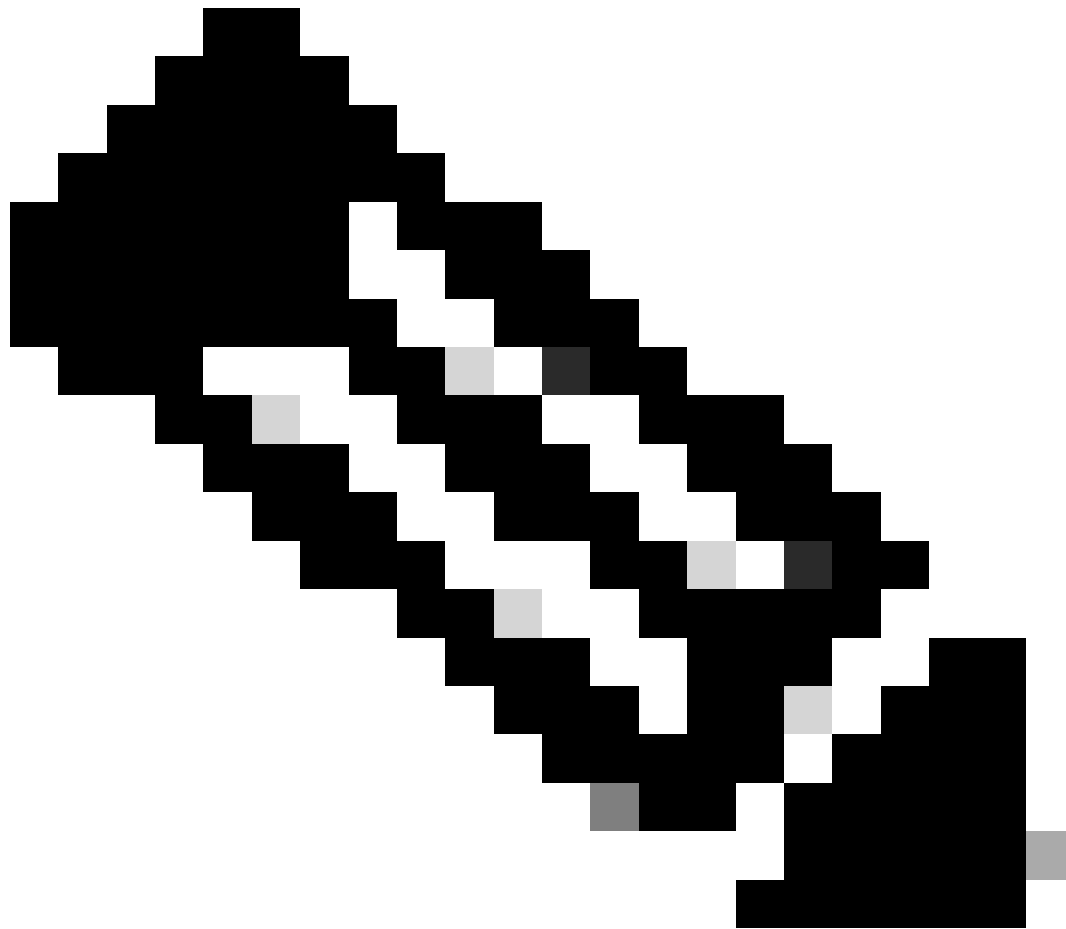
2단계. ISE에서 네트워크 디바이스를 구성합니다.

2.1단계. 네트워크 디바이스 객체에 Name을 할당합니다.

2.2단계. SWA IP 주소를 삽입합니다.

2.3단계. RADIUS 확인란을 선택합니다.

2.4단계. 공유 암호를 정의합니다.



참고: SWA를 구성하려면 나중에 동일한 키를 사용해야 합니다.

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

SWA 네트워크 디바이스 공유 키 구성

2.5단계. Submit(제출)을 클릭합니다.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: [REDACTED] Show

Use Second Shared Secret: ⓘ

[REDACTED] Show

CoA Port: 1700 Set To Default

RADIUS DTLS Settings ⓘ

DTLS Required: ⓘ

Shared Secret: radius/dtls ⓘ

CoA Port: 2083 Set To Default

Issuer CA of ISE Certificates for CoA: Select if required (optional) ⓘ

DNS Name: [REDACTED]

General Settings

Enable KeyWrap: ⓘ

* Key Encryption Key: [REDACTED] Show

* Message Authenticator Code Key: [REDACTED] Show

Key Input Format: ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Submit Cancel

네트워크 디바이스 컨피그레이션 제출

3단계. SWA에 구성된 사용자 이름과 일치하는 네트워크 액세스 사용자를 생성해야 합니다. Administration(관리) > Identity Management(ID 관리) > Identities(ID) > + Add(추가)로 이동합니다.

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

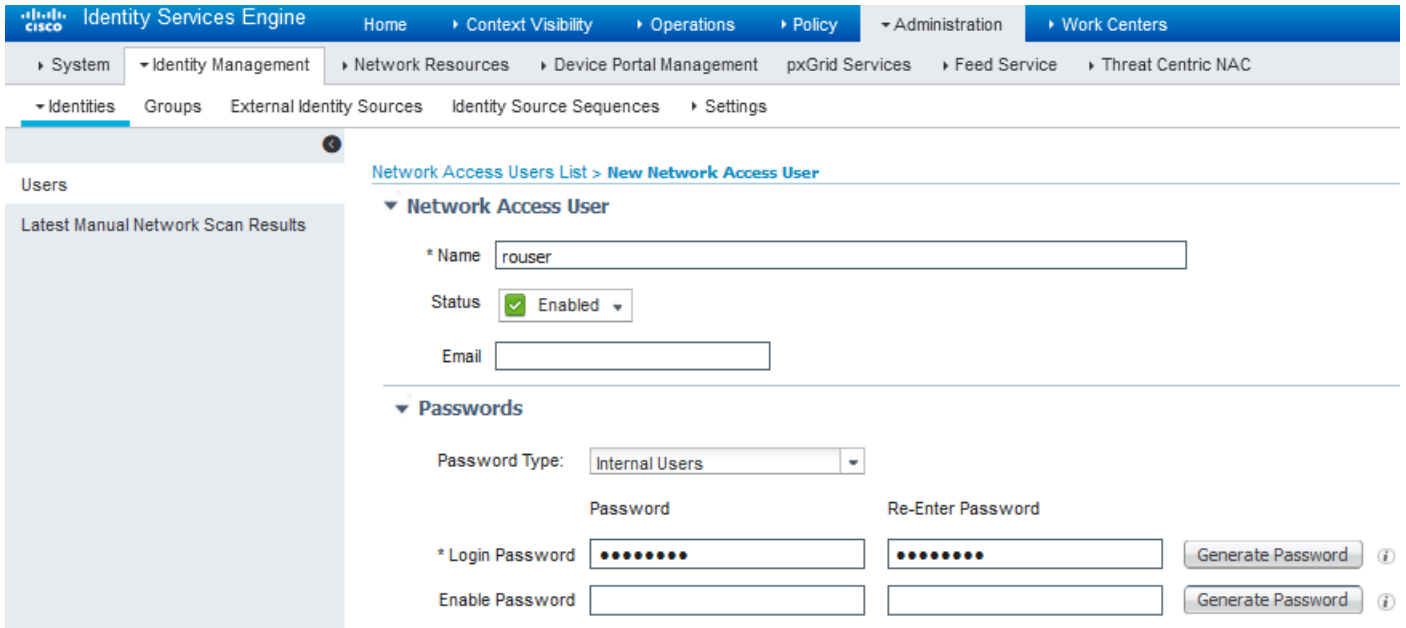
Network Access Users

Edit Add Change Status Import Export Delete Duplicate

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

ISE에서 로컬 사용자 추가

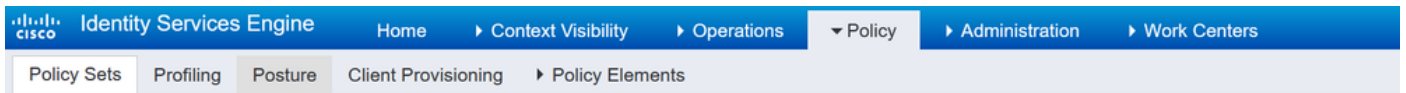
- 3.1단계. 이름을 할당합니다.
- 3.2단계. (선택 사항) 사용자의 이메일 주소를 입력합니다.
- 3.3단계. 비밀번호 설정.
- 3.4단계. 저장을 클릭합니다.



ISE에서 로컬 사용자 추가

4단계. SWA IP 주소와 일치하는 정책 집합을 생성합니다. 이는 이러한 사용자 자격 증명을 사용하여 다른 디바이스에 액세스하지 못하도록 하기 위한 것입니다.

Policy(정책) > Policy(정책)Sets(설정)로 이동하고 왼쪽 상단 모서리에 있는 + 아이콘을 클릭합니다.



Policy Sets

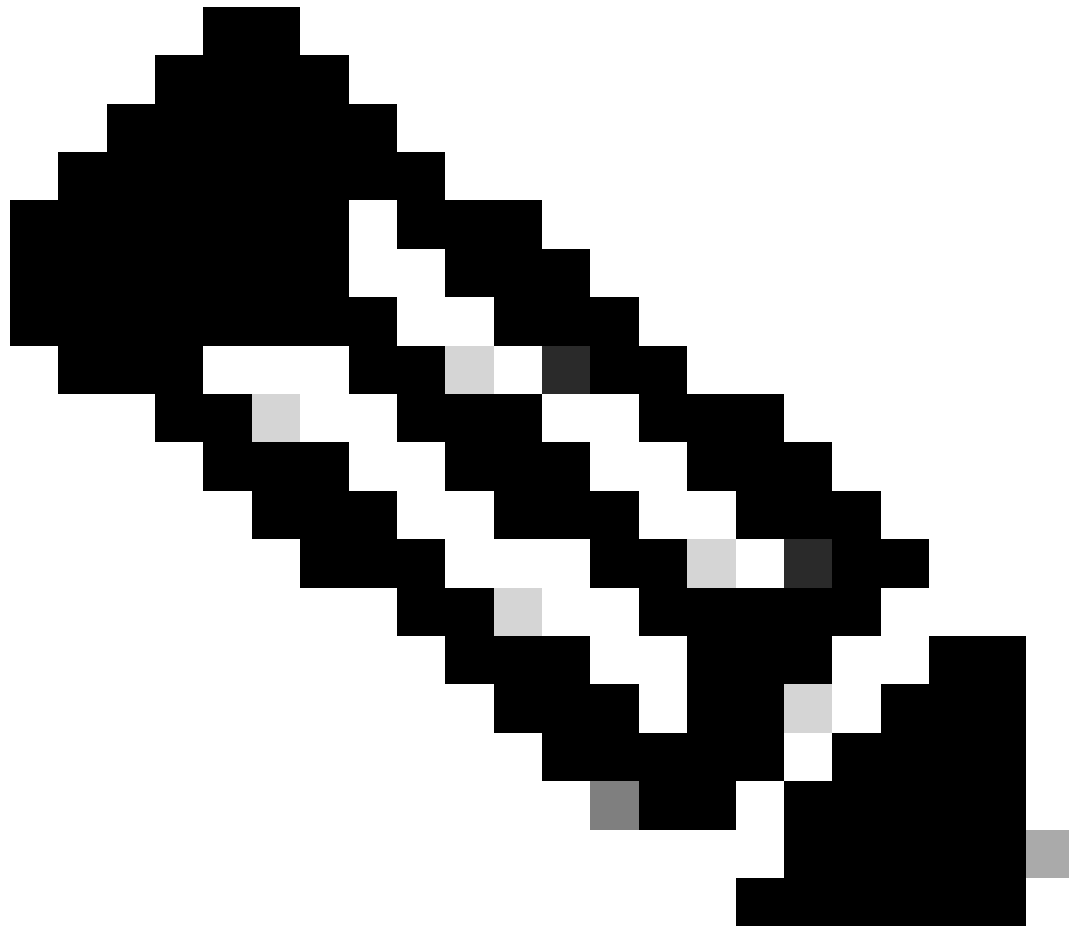
+	Status	Policy Set Name	Description	Conditions
Search				

ISE에 정책 집합 추가

4.1단계. 새 행이 정책 집합의 맨 위에 배치됩니다. 새 정책의 Name을 입력합니다.

4.2단계. RADIUS NAS-IP-Address 특성이 SWA IP 주소와 일치하도록 조건을 추가합니다.

4.3단계. 변경 사항을 유지하고 편집기를 종료하려면 사용을 클릭합니다.



참고: 이 예에서는 기본 네트워크 액세스 프로토콜 목록을 허용했습니다. 새 목록을 만들고 필요에 따라 목록을 좁힐 수 있습니다.

5단계. 새 정책 집합을 보려면 View(보기) 열에서 ">" 아이콘을 클릭합니다.

5.1단계. Authorization Policy(권한 부여 정책) 메뉴를 확장하고 + 아이콘을 클릭하여 인증된 모든 사용자에게 대한 액세스를 허용하는 새 규칙을 추가합니다.

5.2단계. 이름을 설정합니다.

5.3단계. AuthenticationStatus Equals AuthenticationPassed 특성을 가진 사전 네트워크 액세스와 일치하는 조건을 설정하고 Use를 클릭합니다.

SWA 컨피그레이션

1단계. SWA GUI에서 System Administration(시스템 관리)으로 이동하고 Users(사용자)를 클릭합니다.

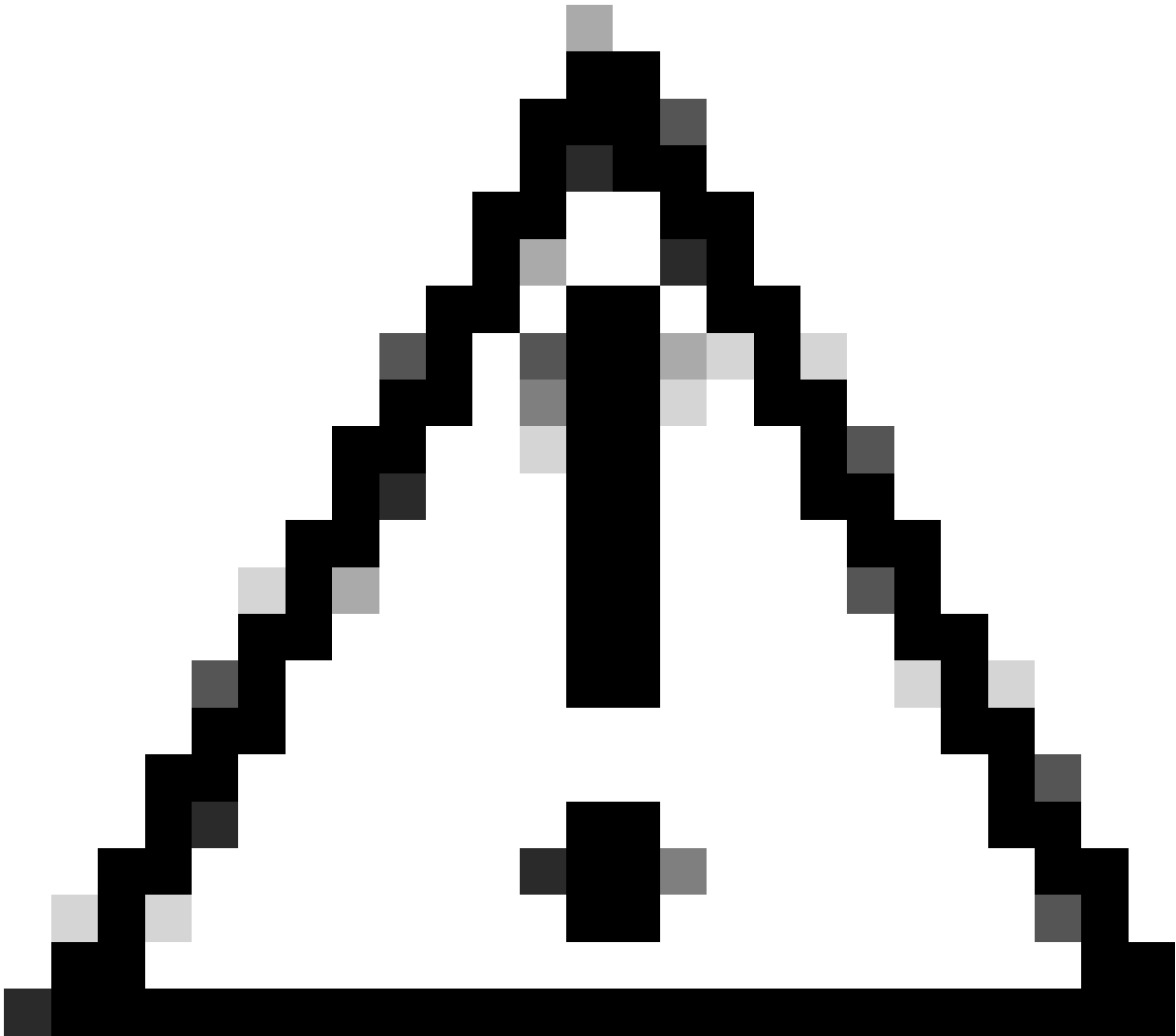
2단계. Second Factor Authentication Settings(2차 요인 인증 설정)에서 Enable(활성화)을 클릭합니다.

The screenshot displays the Cisco Secure Web Appliance (S100V) GUI. The top navigation bar shows 'System Administration' as the active tab. Below it, the 'Users' section is visible, featuring a table with columns for 'Accounts', 'User Name', 'Full Name', 'User Type', 'Account Status', 'Passphrase Expires', and 'Delete'. The 'admin' user is listed with an 'Active' status. Below the table are sections for 'Local User Account & Passphrase Settings', 'External Authentication', and 'Second Factor Authentication Settings'. The 'Second Factor Authentication Settings' section shows 'Two Factor Authentication is disabled.' and an 'Enable...' button, which is highlighted with a blue arrow.

SWA에서 두 번째 요소 인증 활성화

3단계. RADIUS Server Hostname(RADIUS 서버 호스트 이름) 필드에 ISE의 IP 주소를 입력하고 ISE 컨피그레이션의 2단계에서 구성된 Shared Secret(공유 암호)을 입력합니다.

4단계. Second Factor Enforcement를 활성화해야 하는 필수 사전 정의 역할을 선택합니다.



주의: SWA에서 2차 요인 인증을 활성화할 경우, 기본 'admin' 계정도 2차 요인 적용으로 활성화할 수 있습니다. ISE에서는 네트워크 액세스 사용자로 'admin'을 구성할 수 없으므로 ISE를 LDAP 또는 AD(Active Directory)와 통합하여 'admin' 자격 증명을 인증해야 합니다.



Users

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

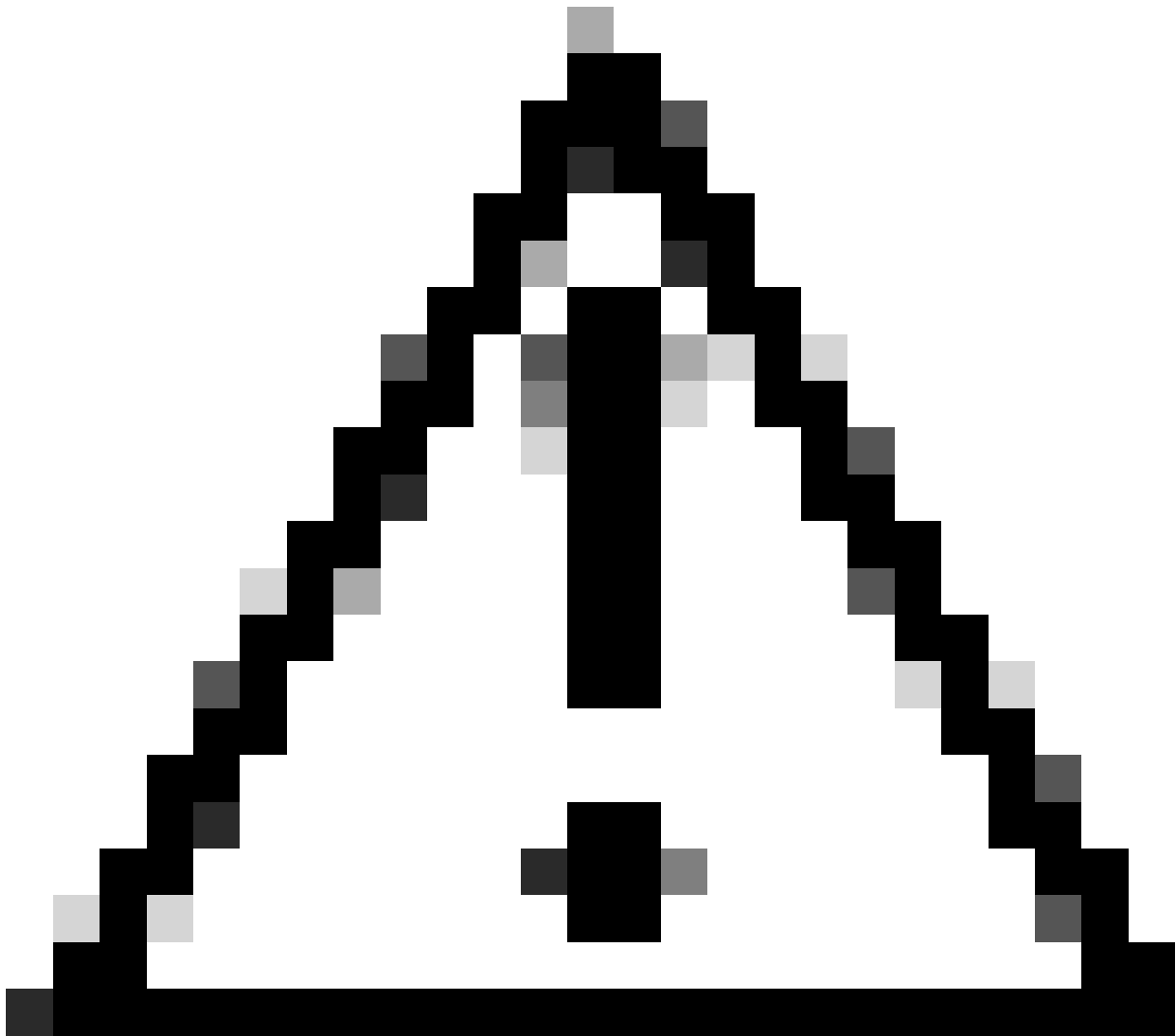
Local User Account & Passphrase Settings	
Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. <i>Additional rules configured...</i>
Edit Settings...	

External Authentication	
<i>External Authentication is disabled.</i>	
Enable...	

Second Factor Authentication Settings	
<i>Two Factor Authentication is disabled.</i>	
Enable...	



SWA에서 두 번째 요소 인증 활성화



주의: SWA에서 2차 요인 인증을 활성화할 경우, 기본 'admin' 계정도 2차 요인 적용으로 활성화할 수 있습니다. ISE에서는 네트워크 액세스 사용자로 'admin'을 구성할 수 없으므로 ISE를 LDAP 또는 AD(Active Directory)와 통합하여 'admin' 자격 증명을 인증해야 합니다.

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	Add Row
	<input type="text" value="10.106.38.150"/>	<input type="text" value="1812"/>	<input type="text" value="*****"/>	<input type="text" value="5"/>	PAP ▾	

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](#)

두 번째 요소 인증 구성

5단계: SWA에서 사용자를 구성하려면 Add User(사용자 추가)를 클릭합니다. 사용자 이름을 입력하고 원하는 역할에 필요한 사용자 유형을 선택합니다. Passphrase를 입력하고 Passphrase를 다시 입력합니다.

Users

Users

* 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.

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	

SWA의 사용자 컨피그레이션

6단계: Submit and Commit Changes(변경 사항 제출 및 커밋)를 클릭합니다.

다음을 확인합니다.

구성된 사용자 자격 증명으로 SWA GUI에 액세스합니다. 인증에 성공하면 보조 인증 페이지로 리디렉션됩니다. 여기서 ISE에 구성된 보조 인증 자격 증명을 입력해야 합니다.



Passcode:

Login

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

2차 요인 로그인 확인

참조

- [AsyncOS 14.0 for Cisco Secure Web Appliance 사용 설명서](#)
- [ISE 3.0 관리 설명서](#)
- [Secure Web Appliance용 ISE 호환성 매트릭스](#)
- [ISE GUI 및 CLI용 AD 통합 로그인](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.