

ISE를 RADIUS 서버로 사용하는 SWA 외부 인증 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 토폴로지](#)

[구성](#)

[ISE 구성](#)

[SWA 컨피그레이션](#)

[다음을 확인합니다.](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ISE를 RADIUS 서버로 사용 하여 SWA (Secure Web Access)에 외부 인증을 구성 하는 단계에 대해 설명 합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Web Appliance에 대한 기본 지식
- ISE의 인증 및 권한 부여 정책 컨피그레이션에 대한 지식
- 기본 RADIUS 지식.

Cisco에서는 다음과 같은 기능도 권장합니다.

- SWA 및 ISE 관리 액세스.
- 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 관리자 사용자에게 외부 인증을 활성화하면 디바이스는 외부 인증 컨피그레이션에 지정된 대로 LDAP(Lightweight Directory Access Protocol) 또는 RADIUS 서버를 사용하여 사용자 자격 증명을 확인합니다.

네트워크 토폴로지



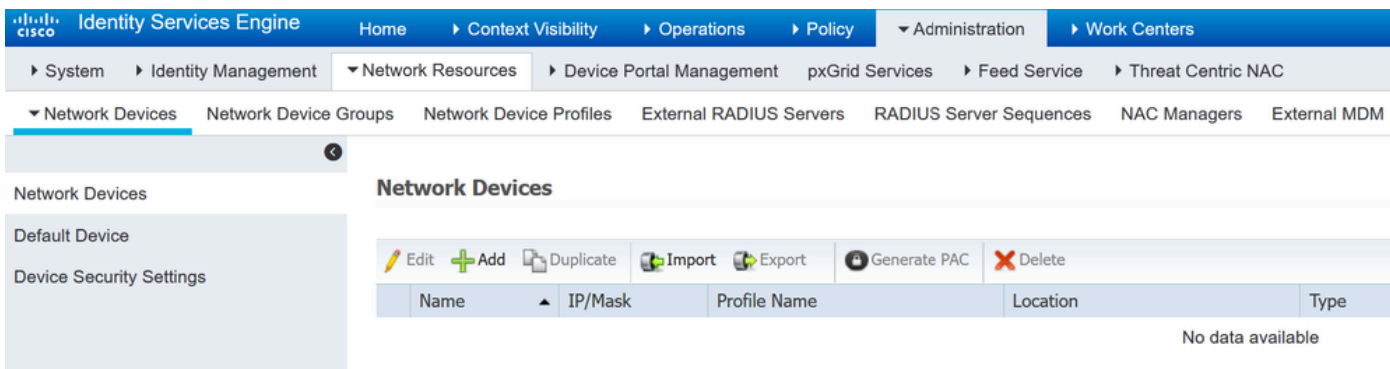
네트워크 토폴로지 다이어그램

관리 사용자는 자격 증명을 사용하여 포트 443의 SWA에 액세스합니다. SWA는 RADIUS 서버로 자격 증명을 확인합니다.

구성

ISE 구성

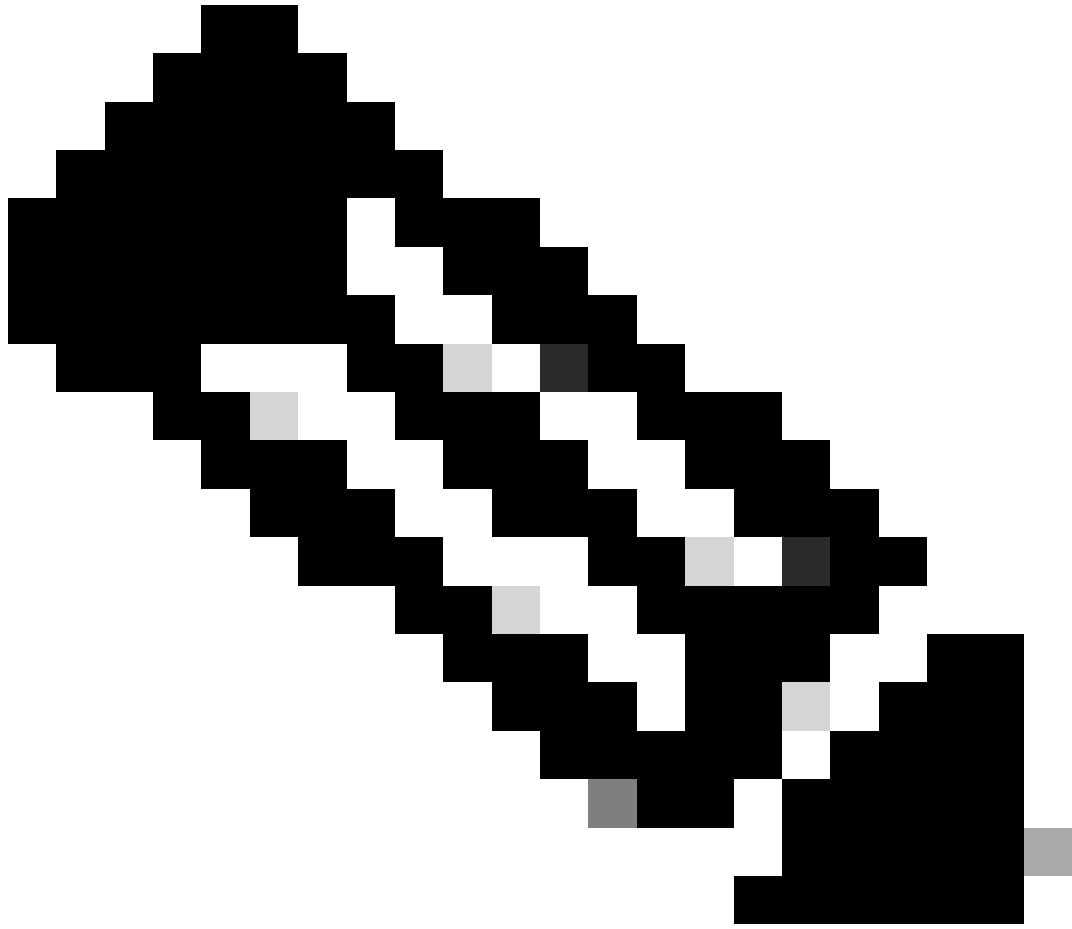
1단계. 새 네트워크 디바이스를 추가합니다. Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) > +Add(추가)로 이동합니다.



ISE에서 SWA를 네트워크 디바이스로 추가

2단계. 네트워크 디바이스 객체에 Name을 지정하고 SWA IP 주소를 삽입합니다.

RADIUS 확인란을 선택하고 공유 암호를 정의합니다.



참고: SWA에서 RADIUS 서버를 구성하려면 나중에 동일한 키를 사용해야 합니다.

Network Devices

Default Device

Device Security Settings

Network Devices List > SWA

Network Devices

* Name

Description

IP Address /

* Device Profile

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

2.1단계. Submit(제출)을 클릭합니다.

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

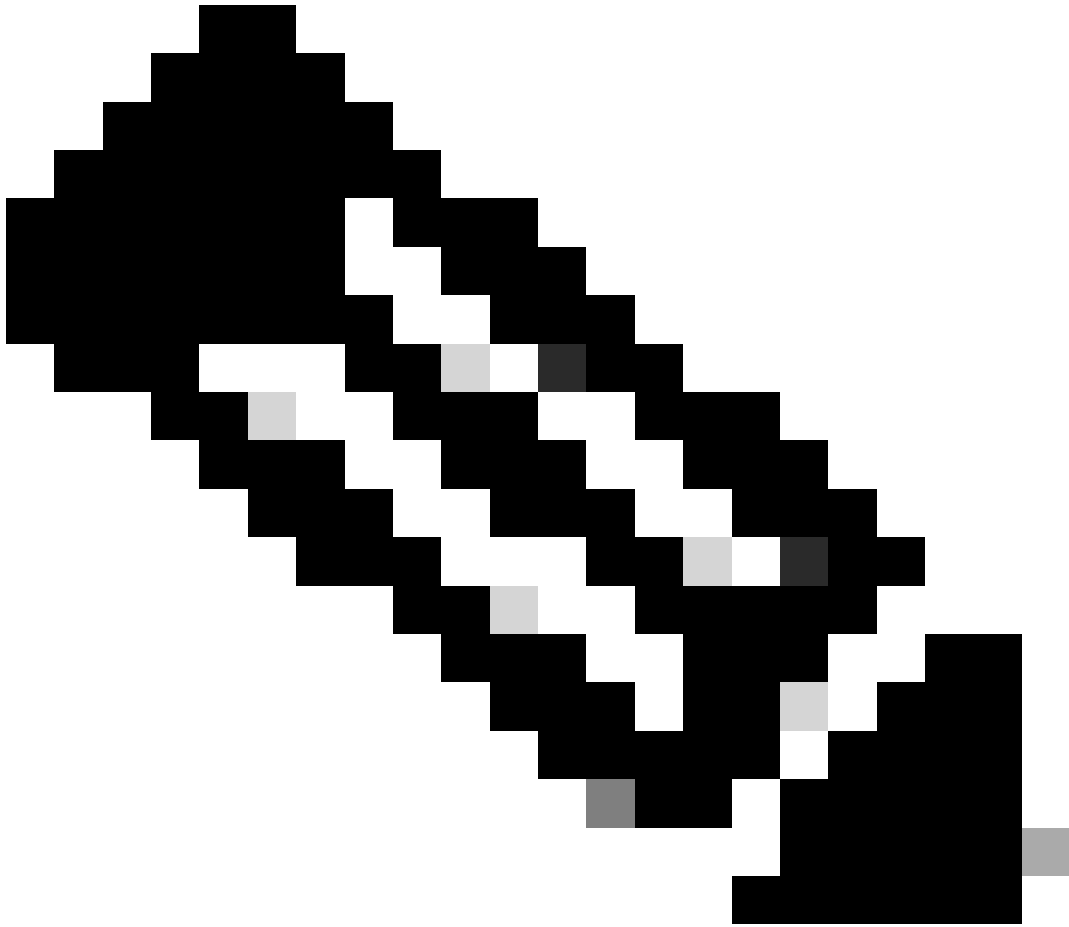
▶ TACACS Authentication Settings

▶ SNMP Settings

▶ Advanced TrustSec Settings

네트워크 디바이스 컨피그레이션 제출

3단계. 필요한 사용자 ID 그룹을 생성합니다. Administration(관리) > Identity Management(ID 관리) > Groups(그룹) > User Identity Groups(사용자 ID 그룹) > + Add(추가)로 이동합니다.



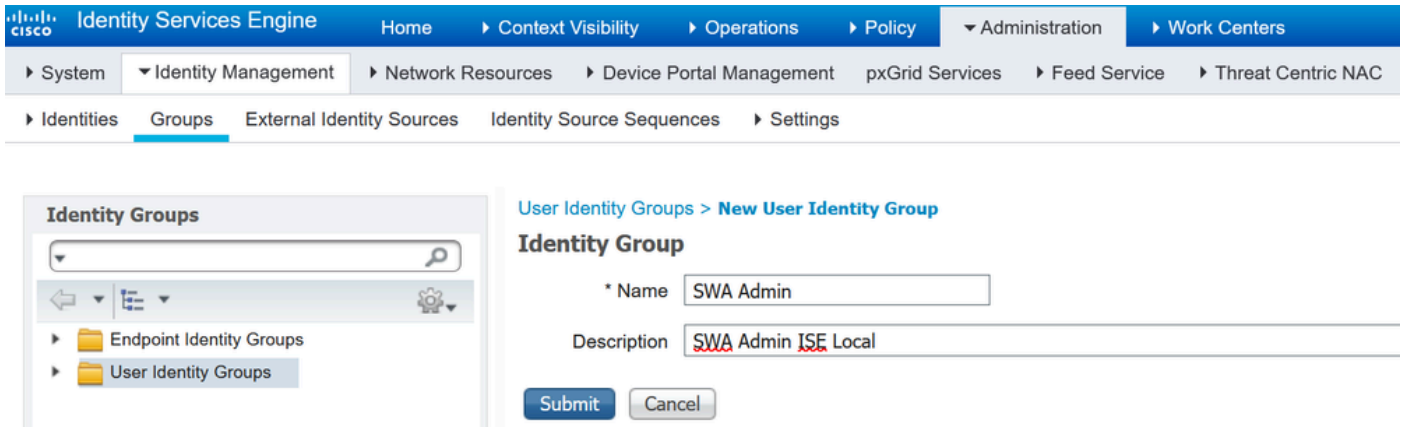
참고: 서로 다른 사용자 유형을 매칭하려면 서로 다른 사용자 그룹을 구성해야 합니다.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded to show '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 is selected, and the 'User Identity Groups' page is displayed. The page has a search bar and a list of user identity groups. The list includes:

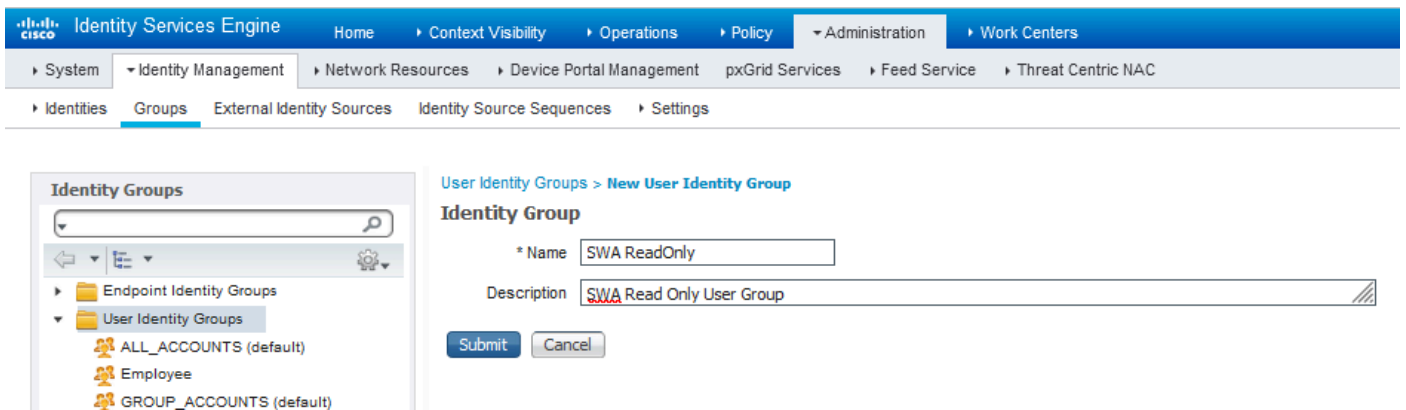
Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor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

사용자 ID 그룹 추가

4단계. 입력 그룹 이름, 설명(선택 사항) 및 제출. 각 그룹에 대해 이 단계를 반복합니다. 이 예에서는 Administrator 사용자를 위한 그룹을 만들고 읽기 전용 사용자를 위한 그룹을 만듭니다.



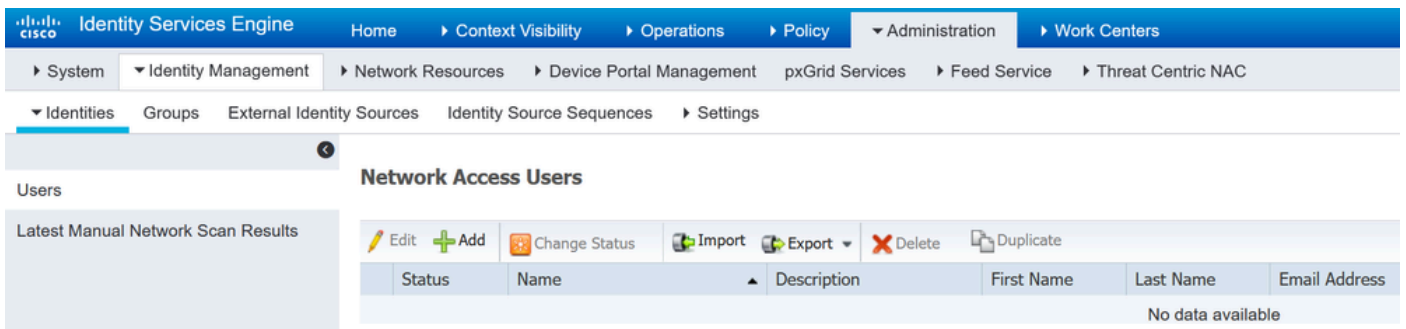
사용자 ID 그룹



추가SWA 읽기 전용 사용자에 대한 사용자 ID 그룹 추가

5단계. SWA에 구성된 사용자 이름과 일치하는 네트워크 액세스 사용자를 생성해야 합니다.

Network Access Users(네트워크 액세스 사용자)를 생성하고 해당 대응 그룹에 추가합니다. Administration(관리) > Identity Management(ID 관리) > Identities(ID) > + Add(추가)로 이동합니다.



ISE에서 로컬 사용자 추가

5.1단계. 관리자 권한이 있는 네트워크 액세스 사용자를 생성해야 합니다. 이름과 암호를 지정합니다.

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

관리자 사용자 추가

5.2단계. User Groups(사용자 그룹) 섹션에서 SWA Admin(SWA 관리자)을 선택합니다.

Account Disable Policy

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

User Groups

Admin User(관리자 사용자)에 관리자 그룹 할당

5.3단계. 읽기 전용 권한이 있는 사용자를 만들어야 합니다. 이름과 암호를 지정합니다.

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: rouser

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: * Login Password

Re-Enter Password:

Enable Password:

Generate Password (i)

Generate Password (i)

읽기 전용 사용자 추가

5.4단계. User Groups(사용자 그룹) 섹션에서 SWA ReadOnly를 선택합니다.

Account Disable Policy

Disable account if date exceeds 2024-03-28 (yyyy-mm-dd)

User Groups

SWA ReadOnly

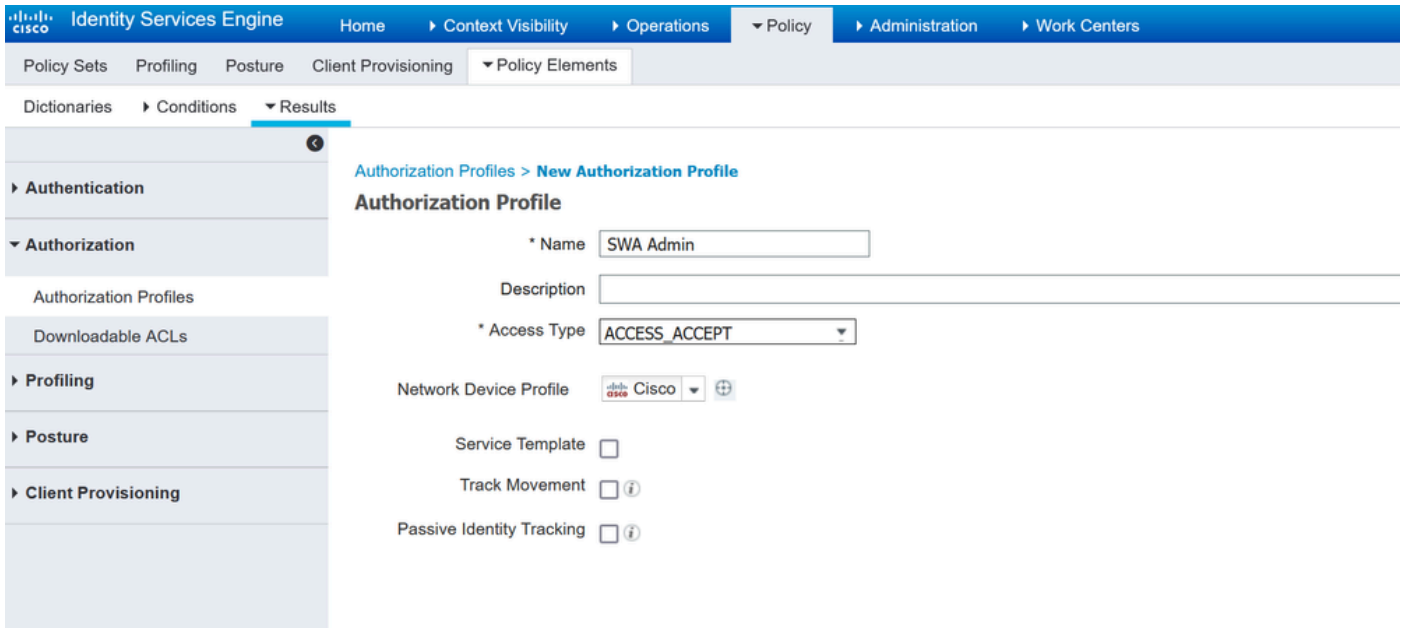
Submit Cancel

읽기 전용 사용자에게 읽기 전용 사용자 그룹 할당

6단계. 관리자 사용자에게 권한 부여 프로파일을 생성합니다.

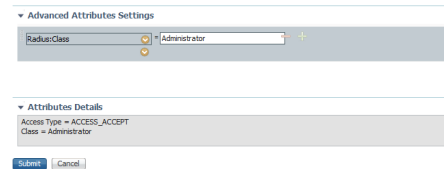
Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일) > +Add(추가)로 이동합니다.

권한 부여 프로파일의 이름을 정의하고 Access Type(액세스 유형)이 ACCESS_ACCEPT로 설정되었는지 확인합니다.



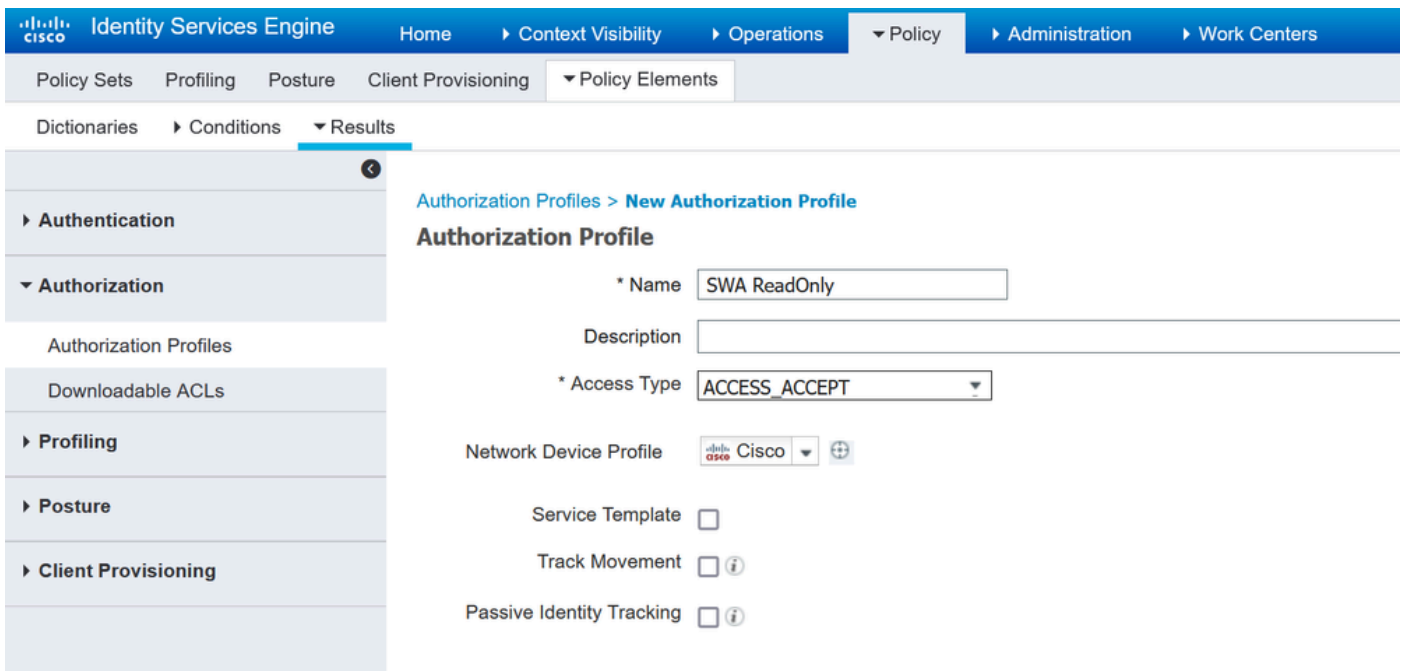
관리자 사용자에게 대한 권한 부여 프로파일 추가

6.1단계. Advanced Attributes Settings(고급 특성 설정)에서 Radius > Class(클래스)—[25]로 이동하고 Administrator(관리자) 값을 입력한 다음 Submit(제출)을 클릭합니다. Add Authorization Profile



for Admin Users(관리자 사용자를 위한 권한 부여 프로파일 추가)를 클릭합니다

7단계. 6단계를 반복하여 읽기 전용 사용자에게 대한 권한 부여 프로파일을 생성합니다.



읽기 전용 사용자에게 대한 권한 부여 프로파일 추가

7.1단계. 이번에는 Administrator 대신 ReadUser 값을 사용하여 Radius:Class를 만듭니다.

Advanced Attributes Settings

Radius:Class = ReadUser

Attributes Details

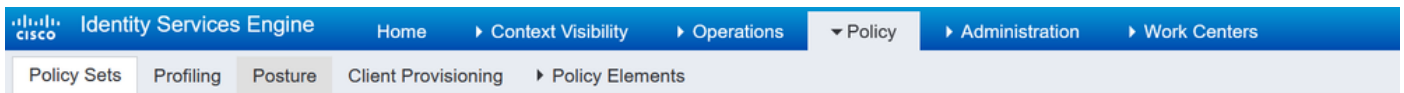
Access Type = ACCESS_ACCEPT
Class = ReadUser

Submit Cancel

읽기 전용 사용자에게 대한 권한 부여 프로파일 추가

8단계. 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

8.1단계. 새 행이 정책 집합의 맨 위에 배치됩니다.

새 정책의 이름을 지정하고 RADIUS NAS-IP-Address 특성이 SWA IP 주소와 일치하도록 조건을 추가합니다.

변경 사항을 유지하고 편집기를 종료하려면 사용을 클릭합니다.

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

SWA 네트워크 디바이스를 매핑하기 위한 정책 추가

8.2단계. 저장을 클릭합니다.

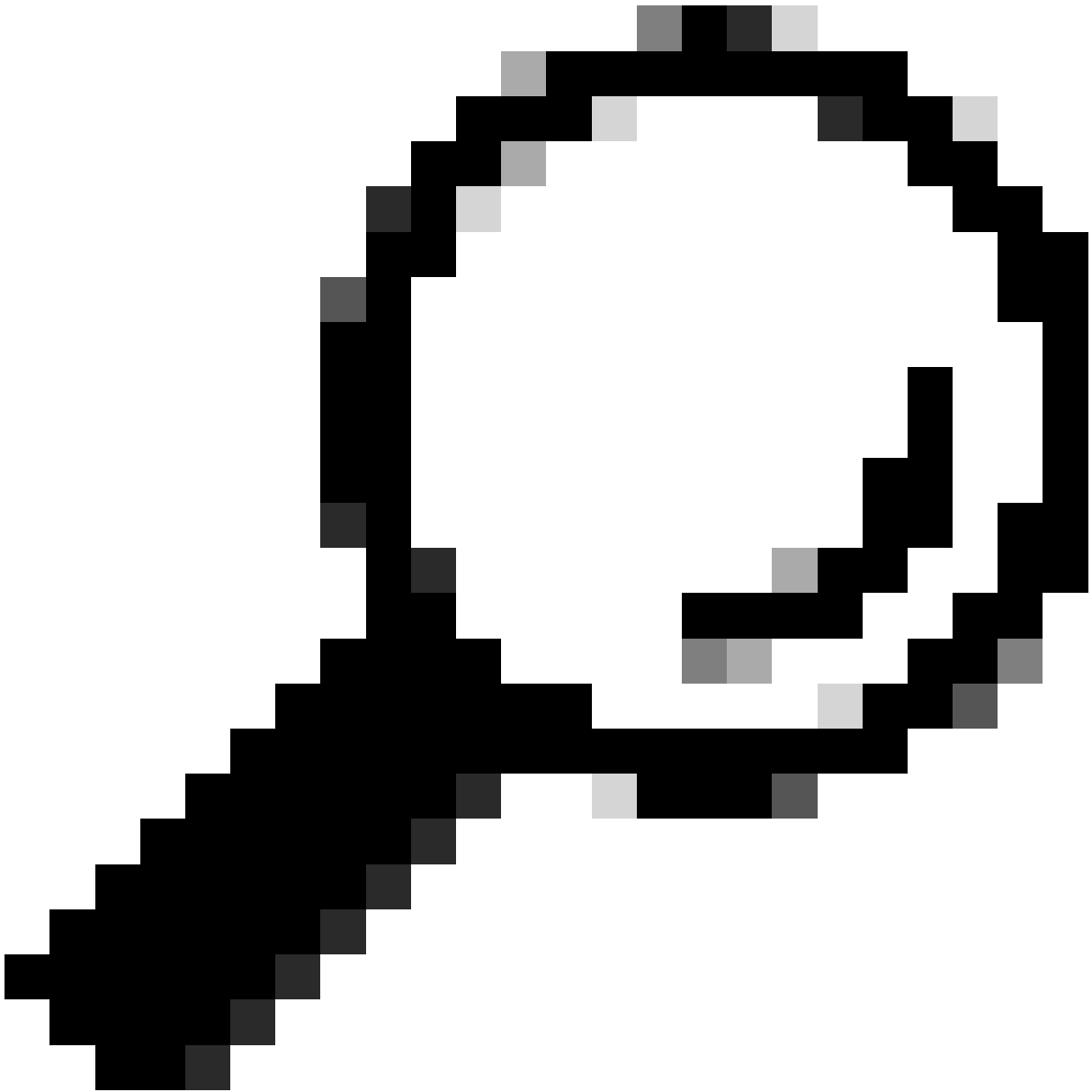
Policy Sets

Reset Policyset Hitcounts Reset Save

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

Reset Save

정책 저장



팁: 이 문서에서는 기본 네트워크 액세스 프로토콜 목록을 사용할 수 있습니다. 새 목록을 만들고 필요에 따라 범위를 좁힐 수 있습니다.

9단계. 새 정책 집합을 보려면 View(보기) 열에서 > 아이콘을 클릭합니다. Authorization Policy(권한 부여 정책) 메뉴를 확장하고 + 아이콘을 클릭하여 관리자 권한이 있는 사용자에게 대한 액세스를 허용하는 새 규칙을 추가합니다.

이름을 설정합니다.

9.1단계. 관리자 사용자 그룹과 일치하는 조건을 생성하려면 + 아이콘을 누릅니다.

▼ Authorization Policy (0)

	Status	Rule Name	Conditions
<input type="text" value="Search"/>			
		SWA Admin	

Add Authorization Policy Condition

9.2단계. Attribute Name Equals User Identity Groups(사용자 ID 그룹과 속성 이름 같음)와 Dictionary Identity Group(사전 ID 그룹)을 일치시키는 조건을 설정합니다. SWA admin(SWA 관리자)

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
- Non_Compliant_Devices
- Switch_Local_Web_Authentication

Editor

Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
AD	ExternalGroups		i
CWA	CWA_ExternalGroups		i
IdentityGroup	Description		i
IdentityGroup	Name		i
InternalUser	IdentityGroup		i
PassiveID	PassiveID_Groups		i

Close Use

Select Identity Group as Condition(조건으로 ID 그룹 선택)

9.3단계. 아래로 스크롤하여 User Identity Groups: SWA admin을 선택합니다.

아래로

Conditions Studio



Library

Search by Name

BYOD_is_Registered (i)

Catalyst_Switch_Local_Web_Authentication (i)

Compliance_Unknown_Devices (i)

Compliant_Devices (i)

EAP-MSCHAPv2 (i)

EAP-TLS (i)

Guest_Flow (i)

MAC_in_SAN (i)

Network_Access_Authentication_Passed (i)

Non_Cisco_Profiled_Phones (i)

Non_Compliant_Devices (i)

Switch_Local_Web_Authentication (i)

Editor

IdentityGroup-Name

Equals

Set to 'Is not'

Choose from list or type

- User Identity Groups:GuestType_Contractor (default)
- User Identity Groups:GuestType_Daily (default)
- User Identity Groups:GuestType_SocialLogin (default)
- User Identity Groups:GuestType_Weekly (default)
- User Identity Groups:OWN_ACCOUNTS (default)
- User Identity Groups:SWA Admin**
- User Identity Groups:SWA ReadOnly

Save

Close Use

스크롤하여 Select Identity Group Name(ID 그룹 이름 선택)을 선택합니다

9.4단계. Use(사용)를 클릭합니다.

Conditions Studio



Library

Search by Name

BYOD_is_Registered (i)

Catalyst_Switch_Local_Web_Authentication (i)

Compliance_Unknown_Devices (i)

Compliant_Devices (i)

EAP-MSCHAPv2 (i)

EAP-TLS (i)

Guest_Flow (i)

MAC_in_SAN (i)

Network_Access_Authentication_Passed (i)

Non_Cisco_Profiled_Phones (i)

Editor

IdentityGroup-Name

Equals

Set to 'Is not'

* User Identity Groups:SWA Admin

You can only select 1 item

Save

+ New AND OR

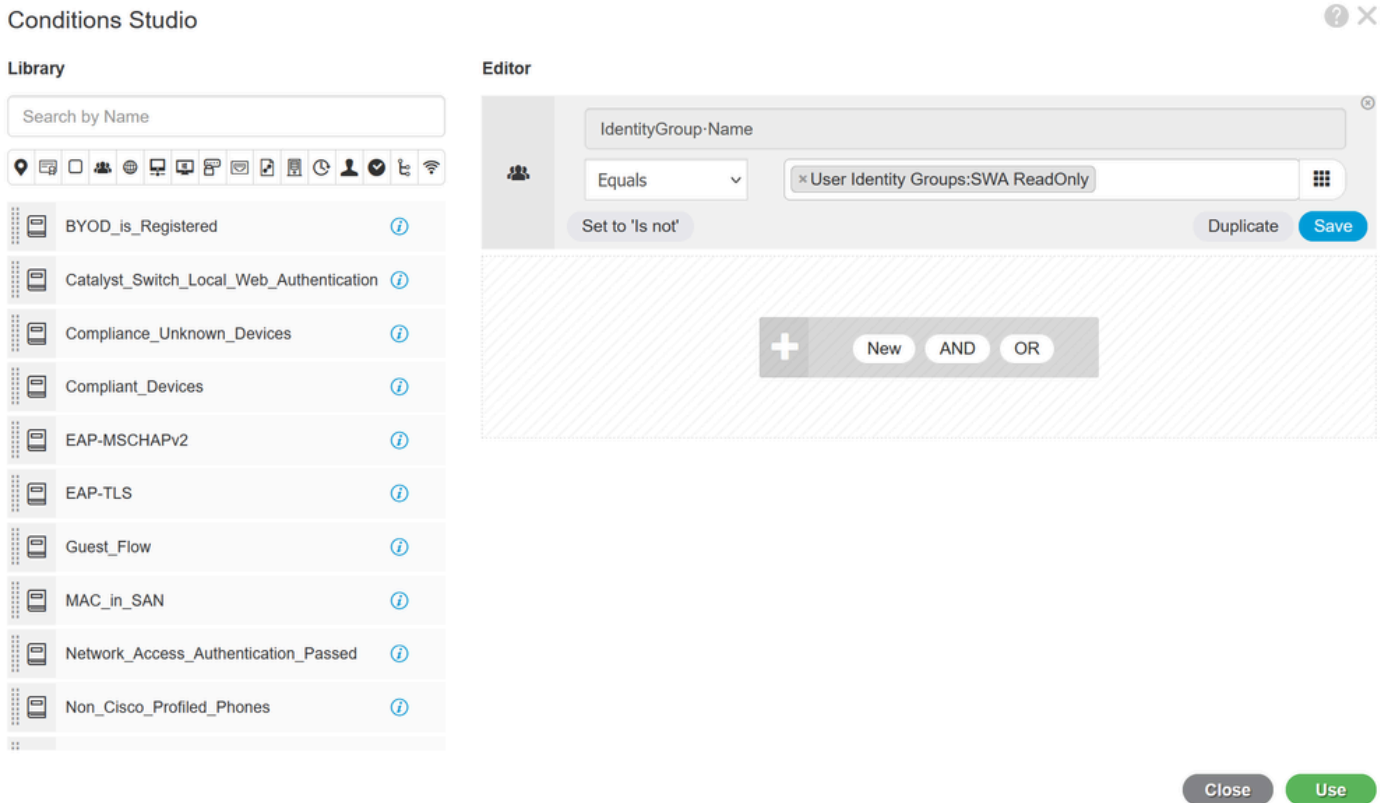
Close Use

SWA 관리자 사용자 그룹에 대한 권한 부여 정책 선택

10단계. 읽기 전용 권한을 가진 사용자에게 액세스를 허용하는 두 번째 규칙을 추가하려면 + 아이콘을 클릭합니다.

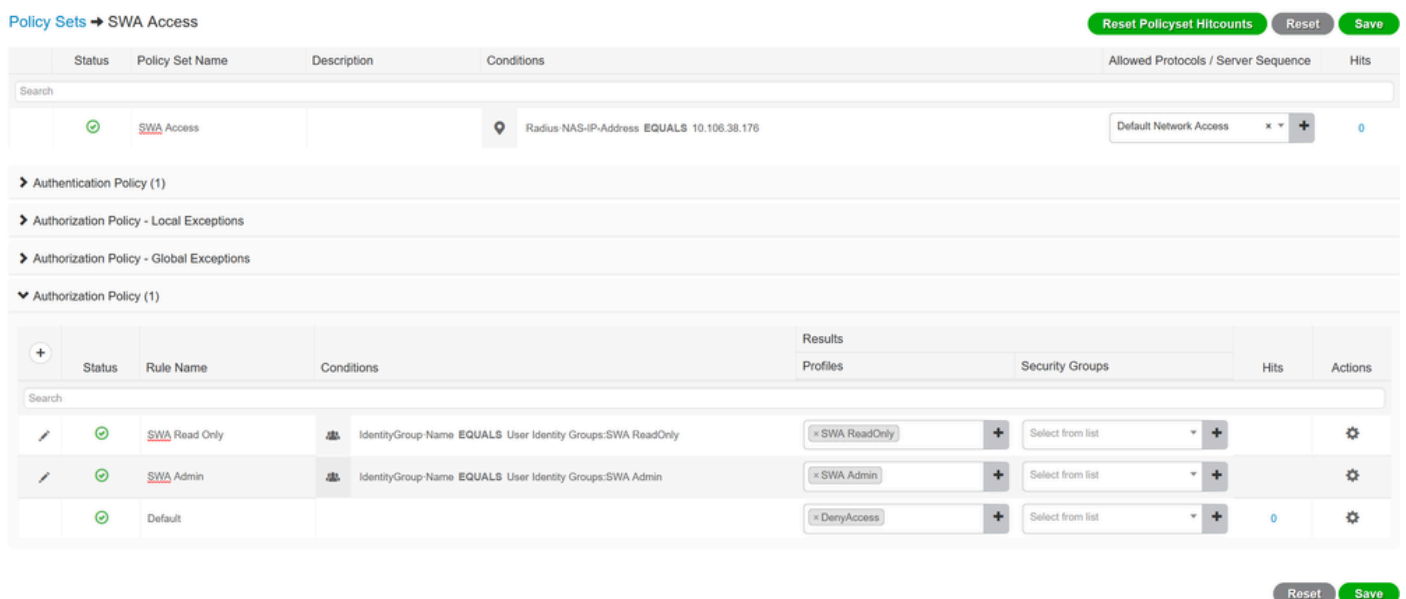
이름을 설정합니다.

Attribute Name Equals User Identity Groups: SWA ReadOnly(특성 이름이 User Identity Groups: SWA 읽기 전용)인 Dictionary Identity Group(사전 ID 그룹)과 일치하는 조건을 설정하고 Use(사용)를 클릭합니다.



읽기 전용 사용자 그룹에 대한 권한 부여 정책 선택

11단계. 각 규칙에 대해 Authorization Profile을 각각 설정하고 Save를 클릭합니다.



SWA 컨피그레이션

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

2단계. 외부 인증에서 활성화를 클릭합니다.

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 sections for 'Local User Account & Passphrase Settings', 'External Authentication', and 'Second Factor Authentication Settings'. The 'External Authentication' section shows 'External Authentication is disabled.' and an 'Enable...' button, which is highlighted with a red arrow.

SWA에서 외부 인증 활성화

3단계. RADIUS Server Hostname(RADIUS 서버 호스트 이름) 필드에 ISE의 IP 주소 또는 FQDN을 입력하고 2단계 ISE Configuration(ISE 컨피그레이션)에서 구성된 동일한 공유 암호를 입력합니다.

4단계. Map externally authenticated users to multiple local roles in Group Mapping(그룹 매핑에서 외부 인증 사용자를 여러 로컬 역할에 매핑)을 선택합니다.

4.1단계. RADIUS CLASS Attribute 필드에 Administrator를 입력하고 Role Administrator를 선택합니다.

4.2단계. RADIUS CLASS Attribute 필드에 ReadUser를 입력하고 Role Read-Only Operator를 선택합니다.



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

RADIUS 서버에 대한 외부 인증 컨피그레이션

5단계: SWA에서 사용자를 구성하려면 Add User(사용자 추가)를 클릭합니다. 사용자 이름을 입력하고 원하는 역할에 필요한 사용자 유형을 선택합니다. Passphrase를 입력하고 Retype Passphrase(어플라이언스가 외부 RADIUS 서버에 연결할 수 없는 경우 GUI 액세스에 필요)를 입력합니다.

참고: 어플라이언스가 외부 서버에 연결할 수 없는 경우 Secure Web Appliance에 정의된 로컬 사용자로 사용자를 인증하려고 시도합니다.

Users

Users						
<input type="button" value="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	

SWA의 사용자 컨피그레이션

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

다음을 확인합니다.

구성된 사용자 자격 증명으로 SWA GUI에 액세스하고 ISE의 라이브 로그를 확인합니다. ISE에서

라이브 로그를 확인하려면 Operations(운영) > Live Logs(라이브 로그)로 이동합니다.

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

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

Authentication Details

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

사용자 로그인 ISE 확인

관련 정보

- [AsyncOS 14.0 for Cisco Secure Web Appliance 사용 설명서](#)
- [ISE 3.0 관리 설명서](#)
- [Secure Web Appliance용 ISE 호환성 매트릭스](#)
- [Cisco 기술 지원 및 다운로드](#)

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.