ISE를 RADIUS 서버로 사용하는 SWA 외부 인증 구성

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>배군 정보</u> <u>네트 워크 토폴로지</u> <u>구성</u> <u>ISE 구성</u> <u>SWA 컨피그레이션</u> <u>다음을 확인합니다.</u>

<u>관련 정보</u>

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 초기화 된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SWA의 관리자 사용자에 대해 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 확인 합니다.

구성

ISE 구성

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

Home Context	Visibility • O	perations Polic	Administration	Work Centers	
Network Resources	Device Portal	Management pxGr	id Services Feed S	Service	AC
oups Network Devi	ce Profiles Exte	rnal RADIUS Servers	RADIUS Server Sec	quences NAC Managers	External MDM
Network Devic	es				
🥖 Edit 🕂 Add 🛙	🚡 Duplicate 🛛 👔	mport 🚯 Export	🕒 Generate PAC 🛛 🗶 D	elete	
Name	▲ IP/Mask	Profile Name	Lo	cation	Туре
				No data a	vailable
	Home Context Network Resources Dups Network Devi Network Devic Cell Add Name	Home → Context Visibility → O Network Resources → Device Portal Dups Network Device Profiles Exter Network Devices ✓ Edit ♣Add ⊉Duplicate ⊉In Name ▲ IP/Mask	Home Context Visibility Operations Polic Network Resources Device Portal Management pxGr Dups Network Device Profiles External RADIUS Servers Network Devices Vertice Polic / Edit Add Duplicate Profile Name Name IP/Mask Profile Name	Home ◆ Context Visibility ◆ Operations ◆ Policy ◆ Administration Network Resources ◆ Device Portal Management pxGrid Services ◆ Feed S Dups Network Device Profiles External RADIUS Servers RADIUS Server Sec Network Devices Vetwork Devices Pedit ♣ Add Duplicate @ Import @ Generate PAC X D Name ▲ IP/Mask Profile Name Lo	Home Context Visibility Operations Policy Administration Work Centers Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric N Dups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers NAC Managers Pedit Add Duplicate Import Export Generate PAC Delete Name IP/Mask Profile Name Location No data a No data No data

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 D	evices List > SV	SWA
Network Devices	Networ	k Devices	
Default Device			
Device Security Settings			* Name SWA
		D	Description
		IP Address	s • IP: 10.106.38.176 / 32
		* Devi	Device Profile ditte Cisco 💌 🕀
		Мо	Model Name
		Coffwor	
		Soltwar	
		* Network De	C Device Group
		Location	on All Locations 📀 Set To Default
		IPSEC	EC No.
		Device Type	Pe All Device Types 📀 Set To Default
	\checkmark	▼ RADIUS Aut	Authentication Settings
		- HADIOO Add	
		BADUUS	NUC UDB Sottings
		RADIUS	ios obe settings
			Protocol RADIUS
			* Shared Secret Show
SWA 네트워크 디바이스 공유 키 구	1성		

2.1단계. Submit(제출)을 클릭합니다.

▼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/dtis (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 ASCI HEXADECIMAL
► TACACS Authentication Settings
► SNMP Settings
► Advanced TrustSec Settings
Cancel

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.

dentity Services Engine Home	Context Visibility Operations Policy	
► System Identity Management Network Re	esources	ervices
Identities Groups External Identity Sources	Identity Source Sequences	
Identity Groups	User Identity Groups	
⟨= • = •	/ Edit 🕂 Add 🗙 Delete 👻 🎲 Import 😱	Export 👻
Endpoint Identity Groups	Name	Description
 User Identity Groups 	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
	Employee	Default Employee User Group
	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
	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.

Context Visibility	 Operations 	▶ Policy	- Administration	Work Centers
ork Resources	ortal Managemen	t pxGrid S	ervices Feed Se	ervice Threat Centric NAC
ces Identity Source Seque	nces I Setting	s		
User Identity Group Identity Group * Name Description Submit Can	os > New User Id SWA Admin SWA Admin ISE	entity Group		
Context Visibility	+ Policy -/	Administration	♦ Work Centers	
urces + Device Portal Managem	ent pxGrid Service	es 🔸 Feed Sei	rvice + Threat Centric	NAC
lentity Source Sequences 🔹 🕨 Sett	ings			
User Identity Groups > New User Identity Group * Name SWA ReadOr Description SWA Read O Submit Cancel	Identity Group]		
	Context Visibility For Resources Device Proces Identity Source Seque User Identity Group Identity Group * Name Description Submit Cana Context Visibility Operations urces Device Portal Managementation tentity Source Sequences Sett User Identity Groups > New User Identity Group * Name SWA ReadOr Description SWA ReadOr Submit Cance	Context Visibility Operations Pork Resources Device Portal Management Press Identity Source Sequences Setting User Identity Groups > New User Id Identity Group * Name SWA Admin SWA Admin ISE Submit Cancel Context Visibility Operations Policy Policy Context Visibility Operations Policy Policy	e > Context Visibility > Operations > Policy orok Resources > Device Portal Management pxGrid Sinces Identity Source Sequences > Settings User Identity Groups > New User Identity Group Identity Group * Name SWA Admin SWA ReadOnly Submit Cancel Submit Cancel The page Sequence Submit Cancel	Context Visibility Operations Policy Administration ork Resources Device Portal Management pxGrid Services Feed Secces Identity Source Sequences Settings User Identity Groups New User Identity Group Identity Group * Name SWA Admin Description SWA Admin ISE Local Submit Cancel Context Visibility Operations Policy Administration • Work Centers User Identity Groups > New User Identity of Policy * Administration • Work Centers User Identity Groups > New User Identity Group Context Visibility • Operations • Policy • Administration • Work Centers User Identity Groups > New User Identity Group Identity Groups > New User Identity Group * Name SWA ReadOnly Description SWA ReadOnly User Identity Group * Name SWA ReadOnly Description SWA ReadOnly Description Submit Cancel

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.

cisco Ident	ity Services Engine	Home ► Cont	ext Visibility 🔹 🕨	Operations F	Policy	- Administration	♦ Work Cer	nters	
 System 	◄ Identity Management	Network Resource	es Device Port	al Management p	oxGrid Ser	rvices + Feed Ser	vice I Thr	eat Centric NAC	
◄ Identities	Groups External Iden	tity Sources Identi	y Source Sequence	es > Settings					
	G								
Users		Network Acc	ess Users						
Latest Manua	I Network Scan Results	/ Edit 🕂 Add	🔀 Change Status	Import 🕞	Export 👻	🗙 Delete 🛛 🕞 Duj	olicate		
		Status	Name	▲ De	escription	Firs	t Name	Last Name	Email Address
								No data availab	ble

ISE에서 로컬 사용자 추가

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

dent dent	tity Services Engine	Home + Contex	tt Visibility → Operations	Policy - Adm	ninistration 🔹 Wo	ork Centers
 System 	+ Identity Management	Network Resources	Device Portal Management	pxGrid Services	Feed Service	Threat Centric NAC
✓ Identities	Groups External Ide	ntity Sources Identity S	Source Sequences			
Users Latest Manua	l Network Scan Results	Network Access U Network Access U Network Acc * Name ad Status Email	isers List > New Network Access ccess User dminuser Enabled v	s User		
		✓ Passwords Password * Login Pas	Type: Internal Users Password ssword	Re-E	nter Password	Generate P

```
관리자 사용자 추가
```

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

 Account Disable Policy 							
Disable account if date exceeds	2024-03-28	(yyyy-mm-dd)					
▼ User Groups							
SWA Admin 📀 —							
Submit Cancel							

Admin User(관리자 사용자)에 관리자 그룹 할당

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

dentity Services Engine	Home
+ System - Identity Management	Network Resources Device Portal Management pxGrid Service Feed Service Threat Centric NAC
- Identities Groups External Identi	ity Sources Identity Source Sequences + Settings
Users Latest Manual Network Scan Results	Network Access Users List > New Network Access User Name rouser Status C Enabled Email
	▼ Passwords
	Password Type: Internal Users +
	Password Re-Enter Password
	* Login Password Generate Password (
	Enable Password Generate Password (

```
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						

6단계. 관리자 사용자에 대한 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 설정되 었는지 확인합니다.

읽기 전용 사용자에게 읽기 전용 사용자 그룹 할당

dentity Services Engine	Home	 Operations 	Policy	Administration	▶ Work Centers
Policy Sets Profiling Posture C	lient Provisioning Policy Eleme	nts			
Dictionaries Conditions Result	ts				
Authentication	Authorization Profiles > New Au Authorization Profile	thorization Profile			
- Authorization	* Name	SWA Admin			
Authorization Profiles	Description				
Downloadable ACLs	* Access Type	ACCESS_ACCEPT	Ţ		
▶ Profiling	Network Device Profile	diste Cisco 👻 🕀			
▶ Posture	Service Template				
Client Provisioning	Track Movement				
	Passive Identity Tracking				

관리자 사용자에 대한 권한 부여 프로파일 추가

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



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

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

dentity Services Engine	Home	 Operations 	▼ Policy	 Administration 	 Work Centers
Policy Sets Profiling Posture C	Client Provisioning Policy Eleme	nts			
Dictionaries Conditions Resul	Its				
Authentication	Authorization Profiles > New Au Authorization Profile	thorization Profile	e		
- Authorization	* Name	SWA ReadOnly			
Authorization Profiles	Description				
Downloadable ACLs	* Access Type	ACCESS_ACCEPT		*	
▶ Profiling	Network Device Profile	delle Cisco 👻 🕀			
▶ Posture	Service Template				
Client Provisioning	Track Movement	i			
	Passive Identity Tracking	i			

읽기 전용 사용자에 대한 권한 부여 프로파일 추가

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

 Advanced Attributes Set 	tings
Radius:Class	
 Attributes Details 	
Access Type = ACCESS_ACCEPT Class = ReadUser	
Submit Cancel	

읽기 전용 사용자에 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.

uhuhu cisco	Identit	Services	Engine	Home	▸ Conte	xt Visibility	 Operations 	▼ Policy	Administration	Work Centers
Polic	y Sets	Profiling	Posture	Client Provisio	oning 🕨	Policy Elemer	nts			
Polic	y Set	6								
+	S	tatus	Policy Set	t Name		Description		Condi	tions	
Sear	ch									

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.

Conditions Studio

Library													
Sear	Search 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											

	Radius·NAS-I	P-Addres	55		
Q	Equals	~	10.106.38.176		
	Set to 'ls not'			Duplicate	Save
	Set to 'Is not'			Duplicate	Sa
		977A	New AND OR		
		(/// .	(1))///////////////////////////////////		

Close Use

SWA 네트워크 디바이스를 매핑하기 위한 정책 추가

8.2단계. 저장을 클릭합니다.

Policy	Sets							Reset Poli	cyset Hitcoun	ts Reset	Save
•	Status	Policy Set Name	Description	Con	ditions	Allowe	ed Protocols / Ser	ver Sequence	Hits	Actions	View
Search											
1	Ø	SWA Access		0	Radius NAS-IP-Address EQUALS 10.106.38.176	Defau	ult Network Access	× * +		¢	>
	\odot	Default	Default policy set			Defa	ult Network Access	× • +	0	¢	>
										Reset	Save

정책 저장

ØX



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 사용자에 대한 액세스를 허용 하는 새 규칙을 추가합니다.

이름을 설정합니다.

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

✓ Author	rization Polic	y (0)			
+	Status	Rule Name	Conditions		
Search					
1	\odot	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 관리 자)

Con	ditions Studio																	
Libra	у		Editor															
Sea	rch by Name			Click	to add	an attribute												
Q E	0 * • • • • • • • • • • • • • •) t; 후	Ę	Select	attribu	ite for condit	ion				<u>\</u>						,	•
	BYOD_is_Registered	<i>()</i>		0	- 2	0 🛎	۲	P	Ģ	9 89		•	ଡ଼	1	Ø	٤	((:-	2
	Catalyst_Switch_Local_Web_Authentication	<i>(</i>)			Dic	ctionary				Attribu	te			ID		Info		
	Compliance_Unknown_Devices				A	II Dictionaries			~	Attribu	te			ID				
	Compliant_Devices	()		盡	AD	VA				Externa	Groups	Groups				() ()		
	EAP-MSCHAPv2	<i>(i</i>)		4	Ide	ntityGroup				Descrip	tion					© ()		
	EAP-TLS	1		48	lde	ntityGroup				Name						<i>(</i>)		
	Guest_Flow	()		盡	Inte	ernalUser				Identity	Group	une				0		
	MAC_in_SAN	<i>(i</i>)		1000	1 0.	3314612				1 033140		apa				U		
	Network_Access_Authentication_Passed																	
	Non_Cisco_Profiled_Phones	1																
	Non_Compliant_Devices	1											 					2
	Switch_Local_Web_Authentication																	

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

s	Sear	ch b	y N	am	Э										
9	ŋ		28	۲	Ŗ	4	8	•		₽	ଡ଼	1	Ø	Ŀ	((-
		BY	OD_	is_	Reg	ister	ed							<i>i</i>)	
		Ca	talys	st_S	witc	h_L	oca	_w	eb_/	Auth	nent	icati	on	<i>i</i>)	
		Co	Compliance_Unknown_Devices											<i>i</i>)	
		Co	Compliant_Devices												
		EAP-MSCHAPv2											<i>i</i>)		
		EA	P-TI	LS										<i>i</i>)	
		Gu	est_	Flo	v									<i>i</i>)	
		MA	.C_i	n_S	AN									<i>i</i>)	
		Ne	twor	k_A	cce	ss_/	Auth	enti	cati	on_l	Pas	sed		<i>i</i>)	
		No	n_C	isco	_Pr	ofile	d_P	hon	es					<i>i</i>)	
		No	n_C	omp	lian	t_D	evic	es						<i>i</i>)	
		Sw	itch_	Lo	al_	Web	A	uthe	ntica	atior	n			<i>i</i>)	

-	- 1	٠		-	-
-	а		т	n	r
_	~	٠	۰.	v	

2

Equals	~	Choose from list or type	
		User Identity Groups:GuestType_Contractor (default)	
Set to 'Is not'		User Identity Groups:GuestType_Daily (default)	
		User Identity Groups:GuestType_SocialLogin (default)	
		User Identity Groups:GuestType_Weekly (default)	
		Liser Identity Groups: OWN_ACCOUNTS (default)	

Close Use

Close Use

0×

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

9.4단계. Use(사용)를 클릭합니다.

Conditions Studio

Libra	y .		Editor				
Sea	rch by Name			IdentityGroup	Name		
Q E	0 4 6 🖵 🛡 🕾 🖻 🗷 🗓 🕑 上 🤇) t: 후	*	Equals	~	×User Identity Groups:SWA Admin	
	BYOD_is_Registered	0		Set to 'Is not'		You can only select 1 item	Save
	Catalyst_Switch_Local_Web_Authentication	0					
	Compliance_Unknown_Devices	0				New AND OR	
	Compliant_Devices	0					
	EAP-MSCHAPv2	0					
	EAP-TLS	0					
	Guest_Flow	()					
	MAC_in_SAN	1					
	Network_Access_Authentication_Passed	<i>(i</i>)					
	Non_Cisco_Profiled_Phones	0					

10단계. 읽기 전용 권한을 가진 사용자에게 액세스를 허용하는 두 번째 규칙을 추가하려면 + 아이콘 을 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.

Con	ditions Studio							0×
Librar	у		Editor					
Sea	rch by Name			IdentityGroup	p∙Name			8
Q) ະ 후	-28-	Equals	~	×User Identity Groups:SWA ReadOnly		
	BYOD_is_Registered	<i>(i)</i>		Set to 'Is not'			Duplicate	Save
	Catalyst_Switch_Local_Web_Authentication	<i>(i)</i>						
	Compliance_Unknown_Devices	<i>(i</i>)				+ New AND OR		
	Compliant_Devices	()						
	EAP-MSCHAPv2	()						
	EAP-TLS	()						
	Guest_Flow	()						
	MAC_in_SAN	()						
	Network_Access_Authentication_Passed	()						
	Non_Cisco_Profiled_Phones	()						
							Close	Use

읽기 전용 사용자 그룹에 대한 권한 부여 정책 선택

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

Policy	Sets → SW	/A Access								ſ	Reset Policyset	Hitcounts	Rese	Save
	Status	Policy Set Name	Description	Co	onditions						Allowed Protoco	ols / Server	Sequence	Hits
Search														
	0	SWA Access		(Radius-NA	S-IP-Address EQUALS 1	10.106.38.176				Default Network	Access	×* +	0
> Auth	entication Po	licy (1)												
> Auth	orization Poli	cy - Local Exceptions												
> Auth	orization Poli	cy - Global Exceptions												
✓ Auth	orization Poli	cy (1)												
								Results						
•	Status	Rule Name	Conditions					Profiles		Security Groups	;		Hits	Actions
Searc	h													
1	\odot	SWA Read Only	盘. Identity	Group-Name EQUALS	3 User Identity G	Froups:SWA ReadOnly		× SWA ReadOnly	+	Select from list	,	+		٥
1	\odot	SWA Admin	at identity	Group-Name EQUALS	3 User Identity G	Groups:SWA Admin		SWA Admin	+	Select from list		+		٥
	ø	Default						(×DenyAccess)	+	Select from list		+	0	٥

SWA 컨피그레이션

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

2단계. 외부 인증에서 활성화를 클릭합니다.

	co Secure	Web Appliance	e			Secure
Repor	rting W	/eb Security Manager	Security Services	Network	System Administration	
				1	•	
Jsers						
Jsers						
Add User.						
All Accounts	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
	admin	Administrator	Administrator	Active	n/a	
Enforce Pa	assphrase Chang	ges				
local lise	r Account & Pa	assobrase Settings				
		Account Lock:	Not configured.			
		Passphrase Reset:	Not configured.			
		Passphrase Rules:	Require at least 8 characte Additional rules configured.	rs.		
						Edit Settings
External /	Authentication	disabled				
External A	autientication is	uisableu.				Enable
Second Fa	actor Authentic	cation Settings				
Two Facto	or Authentication	is disabled.				
						Enable

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 선택 합니다.

S100V						<u>8</u>			
Reporting	Web Security Manager	Security Services	Ne	twork	System Adm	inistration	1		
dit Externa	I Authentication								
cternal Authenti	cation Settings								
🗹 Enable Exte	rnal Authentication								
	Authentication Mode:	Password based Authentica	tion	v					
	Authentication Type:	RADIUS V							
	Protocol	UDP V							
F	RADIUS Server Information:	RADIUS Server Hostname	Port	Shared Secret		Timeout Value (in seconds)	Authentication protocol	Certificate	Add Rov
		10.106.38.150	1812	••••		5	PAP v	Select any	
External Authe	ntication Cache Timeout: 🕐	0 seconds							
	Group Mapping:	 Map externally authentic 	ated user	s to multiple loca	al roles. (reco	mmende	d)		
		RADIUS CLASS Attrib	ute		Role ?			A	dd Row
		administrator			Administra	ator	•		ŵ
		ReadUser			Read-Only	y Operato	r 🕶		Ŵ
		RADIUS CLASS attribut	es are ca:	se-sensitive.					
		O Map all externally authen	ticated us	ers to the Admini	istrator role.				

RADIUS 서버에 대한 외부 인증 컨피그레이션

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



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

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.								
All									
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			

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

dentity Services Engine

Event	5200 Authentication succeeded	
Jsername	adminuser	
indpoint Id		
indpoint Profile		
Authentication Policy	SWA Access >> Default	
uthorization Policy	SWA Access >> SWA Admin	
Authorization Result	SWA Admin	
thentication Details		
Source 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-Accent

사용자 로그인 ISE 확인

관련 정보

- AsyncOS 14.0 for Cisco Secure Web Appliance 사용 설명서
- <u>ISE 3.0 관리 설명서</u>
- <u>Secure Web Appliance용 ISE 호환성 매트릭스</u>
- <u>Cisco 기술 지원 및 다운로드</u>

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 번 역 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.