

Konfigurieren der externen SWA-Authentifizierung mit der ISE als RADIUS-Server

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerktopologie](#)

[Konfigurieren](#)

[ISE-Konfiguration](#)

[SWA-Konfiguration](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren der externen Authentifizierung für Secure Web Access (SWA) mit der Cisco ISE als RADIUS-Server beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Cisco Secure Web Appliance
- Kenntnis der Konfiguration von Authentifizierungs- und Autorisierungsrichtlinien auf der ISE
- Grundlegendes RADIUS-Wissen

Cisco empfiehlt außerdem Folgendes:

- Administrationszugriff für SWA und ISE.
- Kompatible WSA- und ISE-Versionen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- SWA 14.0.2-012
- ISE 3.0.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Wenn Sie die externe Authentifizierung für administrative Benutzer Ihres SWAs aktivieren, überprüft das Gerät die Benutzeranmeldeinformationen mit einem LDAP- (Lightweight Directory Access Protocol) oder RADIUS-Server, wie in der Konfiguration für die externe Authentifizierung angegeben.

Netzwerktopologie



Diagramm der Netzwerktopologie

Administrative Benutzer greifen mit ihren Anmeldeinformationen auf Port 443 auf SWA zu. SWA verifiziert die Anmeldeinformationen mit dem RADIUS-Server.

Konfigurieren

ISE-Konfiguration

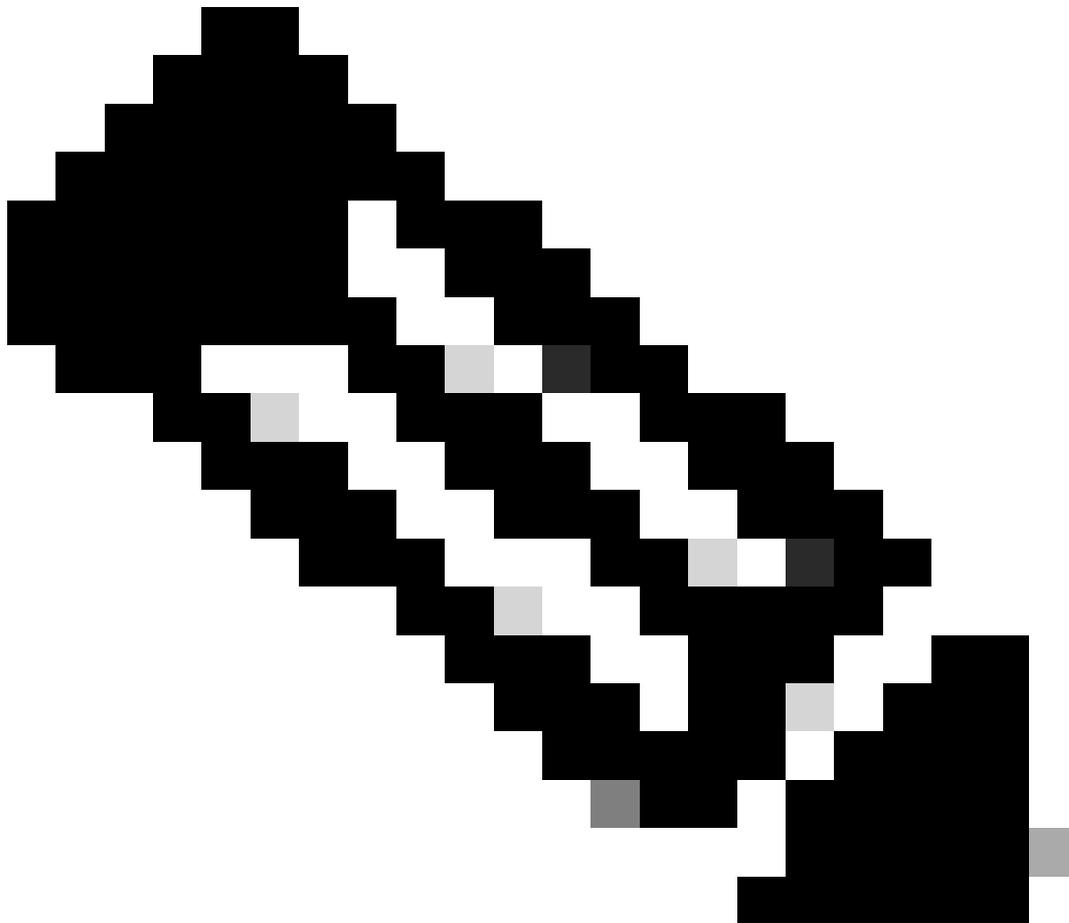
Schritt 1: Hinzufügen eines neuen Netzwerkgeräts Navigieren Sie zu Administration > Network Resources > Network Devices > +Add.



SWA als Netzwerkgerät in der ISE hinzufügen

Schritt 2: Weisen Sie dem Netzwerkgeräteobjekt einen Namen zu, und fügen Sie die SWA-IP-Adresse ein.

Aktivieren Sie das Kontrollkästchen RADIUS, und definieren Sie einen gemeinsamen geheimen Schlüssel.



Hinweis: Derselbe Schlüssel muss später zum Konfigurieren des RADIUS-Servers in SWA verwendet werden.

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

Gemeinsamer SWA-Schlüssel für Netzwerkgerät konfigurieren

Schritt 2.1: Klicken Sie auf Senden.

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

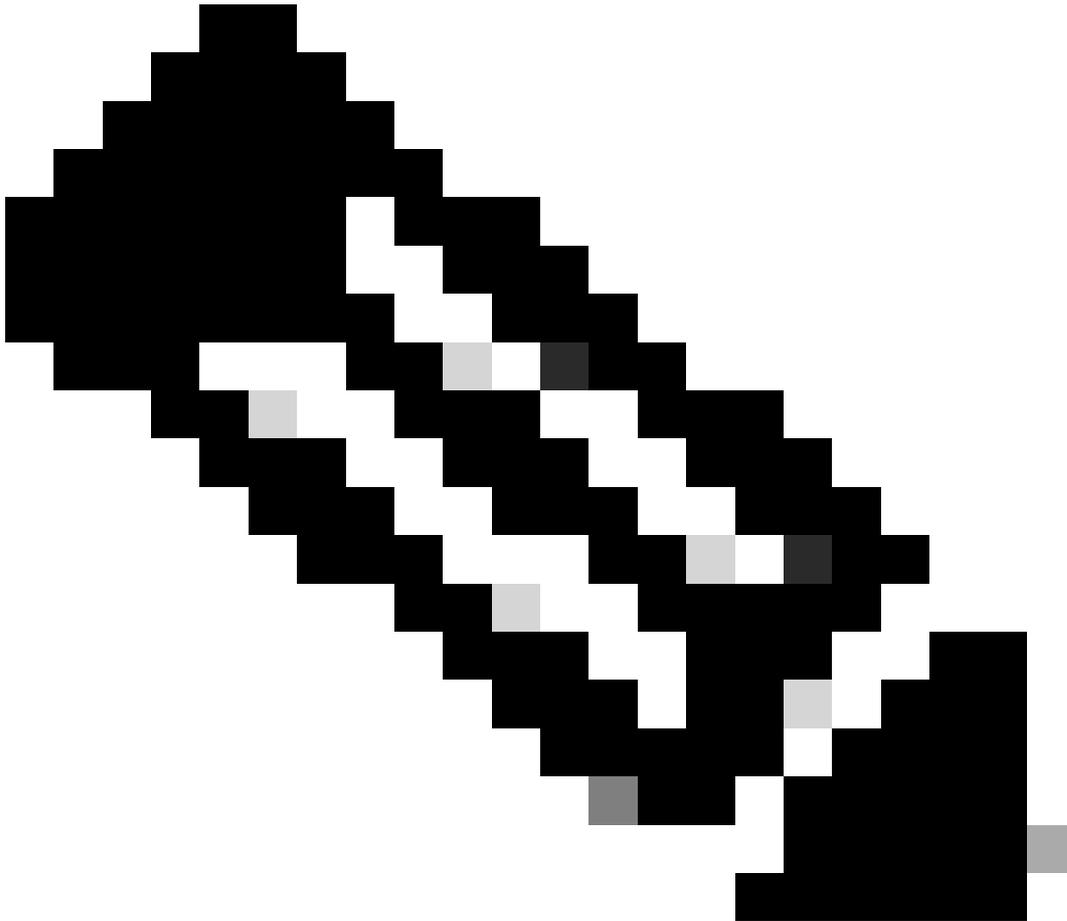
▶ TACACS Authentication Settings

▶ SNMP Settings

▶ Advanced TrustSec Settings

Konfiguration des Netzwerkgeräts senden

Schritt 3: Erstellen Sie die erforderlichen Benutzeridentitätsgruppen. Navigieren Sie zu Administration > Identity Management > Groups > User Identity Groups > + Add.



Hinweis: Sie müssen verschiedene Benutzergruppen konfigurieren, um unterschiedlichen Benutzertypen gerecht zu werden.

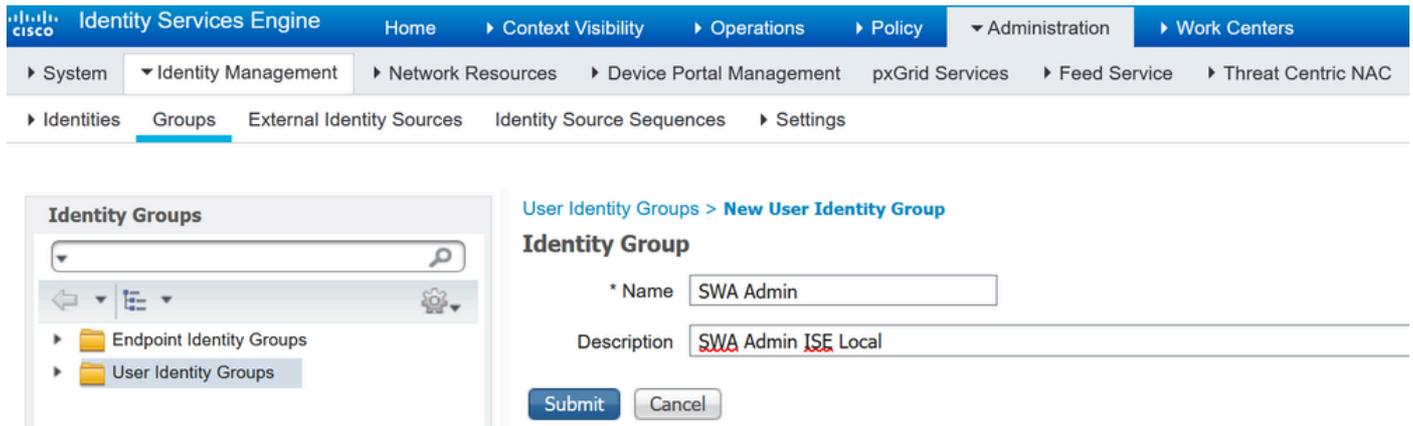
The screenshot shows the Cisco ISE Administration interface. The breadcrumb navigation is: Administration > User Identity Groups. The main content area is titled 'User Identity Groups' and includes a toolbar with 'Edit', '+ Add', 'Delete', 'Import', and 'Export'. Below the toolbar is a table with the following data:

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

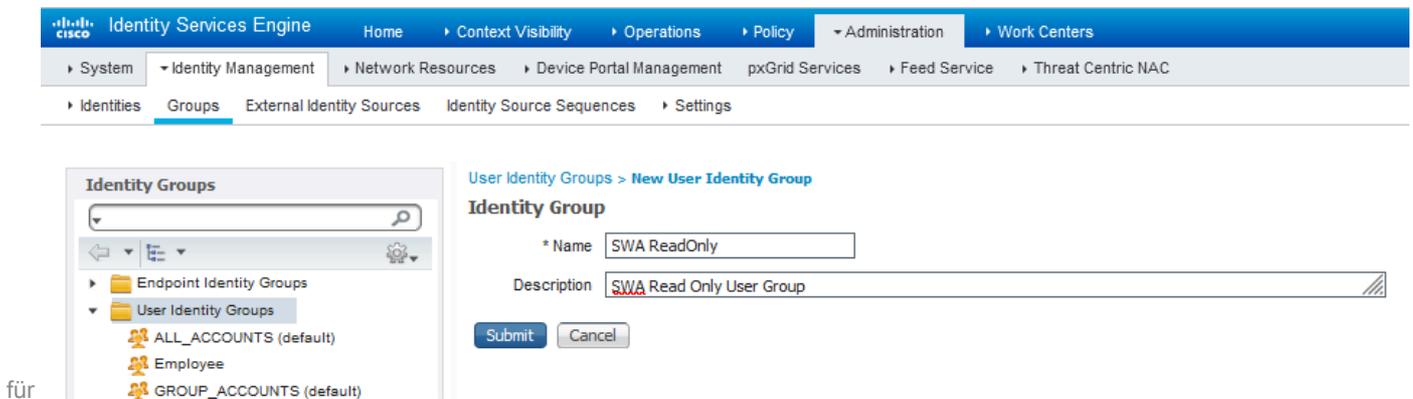
Benutzeridentitätsgruppe hinzufügen

Schritt 4: Geben Sie den Gruppennamen, die Beschreibung (optional) und die Übermittlungsoption

ein. Wiederholen Sie diese Schritte für jede Gruppe. In diesem Beispiel erstellen Sie eine Gruppe für Administrator-Benutzer und eine weitere Gruppe für schreibgeschützte Benutzer.



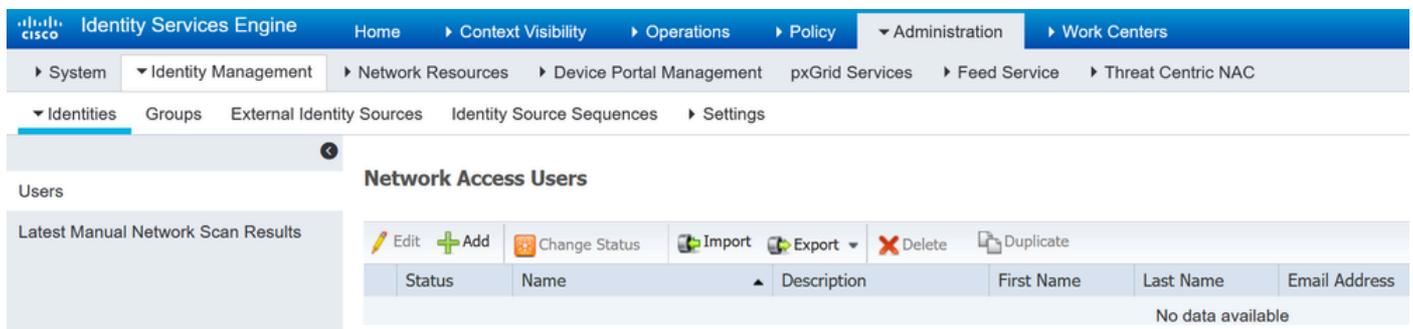
Benutzeridentitätsgruppe hinzufügen Benutzeridentitätsgruppe



für schreibgeschützte SWA-Benutzer hinzufügen

Schritt 5: Sie müssen Netzwerkzugriffsbenutzer erstellen, die mit dem in SWA konfigurierten Benutzernamen übereinstimmen.

Erstellen Sie die Netzwerkzugriffsbenutzer, und fügen Sie sie der entsprechenden Gruppe hinzu. Navigieren Sie zu Administration > Identity Management > Identities > + Add.



Hinzufügen lokaler Benutzer zur ISE

Schritt 5.1: Sie müssen einen Netzwerkzugriffsbenutzer mit Administratorrechten erstellen. Weisen Sie einen Namen und ein Kennwort zu.

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:

Administrator-Benutzer hinzufügen

Schritt 5.2: Wählen Sie im Abschnitt "User Groups" (Benutzergruppen) die Option SWA Admin

Account Disable Policy

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

User Groups

(Admin-Gruppe)
aus. Weisen Sie dem Admin-Benutzer eine Admin-Gruppe zu.

Schritt 5.3: Sie müssen einen Benutzer mit Lesezugriff erstellen. Weisen Sie einen Namen und ein Kennwort zu.

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	<input type="password" value="••••••"/>	<input type="password" value="••••••"/>	<input type="button" value="Generate Password"/> ⓘ
Enable Password	<input type="password"/>	<input type="password"/>	<input type="button" value="Generate Password"/> ⓘ

Schreibgeschützten Benutzer hinzufügen

Schritt 5.4: Wählen Sie im Abschnitt User Groups (Benutzergruppen) die Option SWA ReadOnly aus.

Account Disable Policy

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

User Groups

⌵

Weisen Sie dem schreibgeschützten Benutzer eine schreibgeschützte Benutzergruppe zu.

Schritt 6: Erstellen Sie das Autorisierungsprofil für den Admin-Benutzer.

Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile > +Hinzufügen.

Definieren Sie einen Namen für das Autorisierungsprofil, und stellen Sie sicher, dass der Zugriffstyp auf ACCESS_ACCEPT festgelegt ist.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name SWA Admin

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Autorisierungsprofil für Administratorbenutzer hinzufügen

Schritt 6.1: Navigieren Sie in den erweiterten Attributeinstellungen zu Radius > Class—[25], geben

Advanced Attributes Settings

Radius:Class Administrator

Attributes Details

Access Type = ACCESS_ACCEPT

Class = Administrator

Submit Cancel

Sie den Wert Administrator ein, und klicken Sie auf Submit (Senden).

Add Authorization Profile for Admin Users (Autorisierungsprofil für Administratorbenutzer hinzufügen).

Schritt 7. Wiederholen Sie Schritt 6, um das Autorisierungsprofil für den schreibgeschützten Benutzer zu erstellen.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name SWA ReadOnly

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

Autorisierungsprofil für schreibgeschützte Benutzer hinzufügen

SCHRITT 7.1: Erstellen Sie diesmal Radius:Class mit dem Wert ReadUser anstelle von

Administrator.

Advanced Attributes Settings

Radius:Class = ReadUser

Attributes Details

Access Type = ACCESS_ACCEPT
Class = ReadUser

Submit Cancel

Autorisierungsprofil für schreibgeschützte Benutzer hinzufügen

Schritt 8: Erstellen Sie Richtlinienätze, die mit der SWA-IP-Adresse übereinstimmen. Dadurch wird der Zugriff auf andere Geräte mit diesen Benutzeranmeldeinformationen verhindert.

Navigieren Sie zu Policy > PolicySets, und klicken Sie in der linken oberen Ecke auf das Symbol +.

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				

Richtliniensatz in ISE hinzufügen

Schritt 8.1: Eine neue Zeile wird oben in Ihren Richtlinienätzen platziert.

Geben Sie der neuen Richtlinie einen Namen, und fügen Sie eine Bedingung für das RADIUS NAS-IP-Address-Attribut hinzu, damit es mit der SWA-IP-Adresse übereinstimmt.

Klicken Sie auf Verwenden, um die Änderungen beizubehalten und den Editor zu beenden.

Conditions Studio



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

Hinzufügen einer Richtlinie zum Zuordnen eines SWA-Netzwerkgeräts

Schritt 8.2: Klicken Sie auf Speichern.

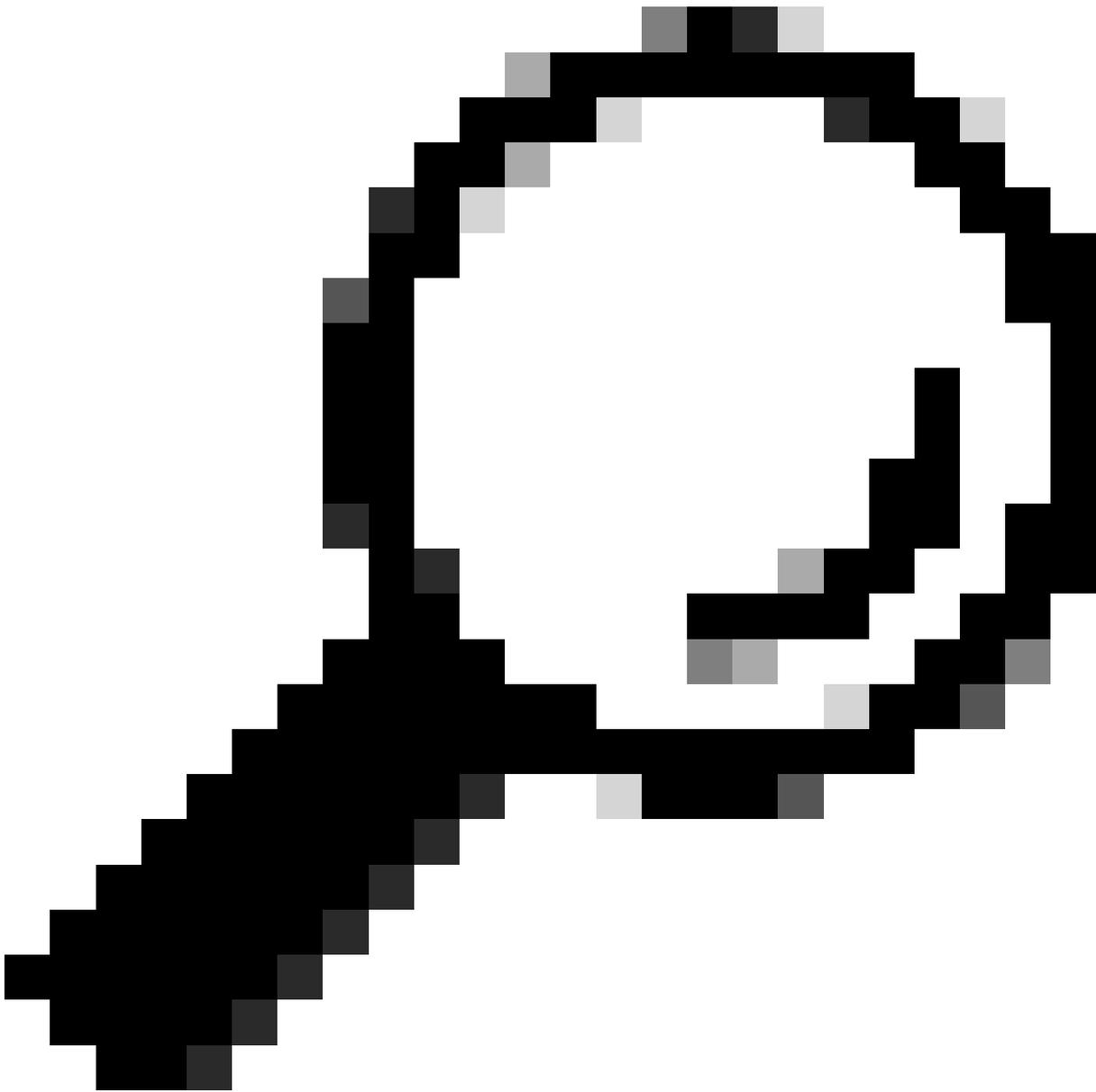
Policy Sets

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 x +			
		Default	Default policy set		Default Network Access x +	0		

Reset Save

Richtlinie speichern



Tipp: In diesem Artikel ist die Liste der Standardprotokolle für den Netzwerkzugriff zulässig. Sie können eine neue Liste erstellen und diese nach Bedarf eingrenzen.

Schritt 9. Um die neuen Richtlinienätze anzuzeigen, klicken Sie in der Spalte Ansicht auf das Symbol >. Erweitern Sie das Menü Autorisierungsrichtlinie, und klicken Sie auf das Symbol +, um eine neue Regel hinzuzufügen, die den Zugriff für Benutzer mit Administratorrechten ermöglicht.

Legen Sie einen Namen fest.

Schritt 9.1: Um eine Bedingung zu erstellen, die mit der Admin-Benutzergruppe übereinstimmt, klicken Sie auf + Symbol

▼ Authorization Policy (0)

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

Autorisierungsrichtlinienbedingung hinzufügen

Schritt 9.2: Legen Sie die Bedingungen fest, die der Dictionary-Identitätsgruppe mit dem Attributnamen gleich den Benutzeridentitätsgruppen entsprechen: SWA admin.

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_Profiled_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		
CWA	CWA_ExternalGroups		
IdentityGroup	Description		
IdentityGroup	Name		
InternalUser	IdentityGroup		
PassiveID	PassiveID_Groups		

Identitätsgruppe als Bedingung auswählen

Close Use

Schritt 9.3: Blättern Sie nach unten, und wählen Sie Benutzeridentitätsgruppen: SWA admin.

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_Profiled_Phones ⓘ

Non_Compliant_Devices ⓘ

Switch_Local_Web_Authentication ⓘ

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

Blättern Sie nach unten und wählen Sie Identitätsgruppenname aus.

Schritt 9.4: Klicken Sie auf Verwenden.

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_Profiled_Phones ⓘ

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

Autorisierungsrichtlinie für SWA-Admin-Benutzergruppe auswählen

Schritt 10. Klicken Sie auf das Symbol +, um eine zweite Regel hinzuzufügen, um Benutzern mit schreibgeschützten Rechten den Zugriff zu gestatten.

Legen Sie einen Namen fest.

Legen Sie die Bedingungen fest, die der Dictionary-Identitätsgruppe mit dem Attributnamen gleich den Benutzeridentitätsgruppen: SWA ReadOnly (Nur SWA lesen) entsprechen, und klicken Sie auf Verwenden.

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

Editor

IdentityGroup-Name

Equals

× User Identity Groups:SWA ReadOnly

Set to 'Is not'

Duplicate

Save

+ New AND OR

Close Use

Autorisierungsrichtlinie für schreibgeschützte Benutzergruppe auswählen

Schritt 11. Legen Sie das Autorisierungsprofil für jede Regel fest, und klicken Sie auf Speichern.

Policy Sets → SWA Access

Reset Policyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	SWA Access		Radius-NAS-IP-Address EQUALS 10.106.38.176	Default Network Access × +	0

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

	Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
+	✓	SWA Read Only	IdentityGroup-Name EQUALS User Identity Groups:SWA ReadOnly	SWA ReadOnly +	Select from list +			
✎	✓	SWA Admin	IdentityGroup-Name EQUALS User Identity Groups:SWA Admin	SWA Admin +	Select from list +			
	✓	Default		DenyAccess +	Select from list +		0	

Reset Save

Autorisierungsprofil auswählen

SWA-Konfiguration

Schritt 1: Navigieren Sie in der SWA-GUI zu Systemverwaltung, und klicken Sie auf Benutzer.

Schritt 2: Klicken Sie in Externe Authentifizierung auf Aktivieren.

Users

Add User...

All Accounts	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. Additional rules configured...

Edit Settings...

External Authentication

External Authentication is disabled.

Enable...

Second Factor Authentication Settings

Two Factor Authentication is disabled.

Enable...

Externe Authentifizierung in SWA aktivieren

Schritt 3: Geben Sie die IP-Adresse oder den FQDN der ISE in das Feld RADIUS Server Hostname ein, und geben Sie den gleichen Shared Secret ein, der in Schritt 2, ISE-Konfiguration, konfiguriert wurde.

Schritt 4: Wählen Sie Extern authentifizierte Benutzer mehreren lokalen Rollen in der Gruppenzuordnung zuordnen.

Schritt 4.1: Geben Sie Administrator in das Feld RADIUS CLASS Attribute ein, und wählen Sie Role Administrator aus.

Schritt 4.2: Geben Sie ReadUser in das Feld RADIUS CLASS Attribute ein, und wählen Sie den Role Read-Only Operator aus.



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

Konfiguration für die externe Authentifizierung für RADIUS-Server

Schritt 5: Um Benutzer in SWA zu konfigurieren, klicken Sie auf Benutzer hinzufügen. Geben Sie den Benutzernamen ein, und wählen Sie den für die gewünschte Rolle erforderlichen Benutzertyp aus. Geben Sie die Passphrase ein, und geben Sie sie erneut ein. Dies ist für den GUI-Zugriff erforderlich, wenn die Appliance keine Verbindung zu einem externen RADIUS-Server herstellen kann.



Hinweis: Wenn die Appliance keine Verbindung zu einem externen Server herstellen kann, versucht sie, den Benutzer als lokalen Benutzer zu authentifizieren, der auf der sicheren Webappliance definiert ist.

Users

Users						
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	

Benutzerkonfiguration in SWA

Schritt 6: Klicken Sie auf Senden und Änderungen bestätigen.

Überprüfung

Zugriff auf die SWA-GUI mit den konfigurierten Benutzeranmeldeinformationen und Überprüfung der Live-Protokolle in der ISE Um die Live-Protokolle in der ISE zu überprüfen, navigieren Sie zu Operations > Live Logs:

The screenshot displays the Cisco Identity Services Engine (ISE) interface. At the top, there is a blue header with the Cisco logo and the text "Identity Services Engine". Below the header, the main content is divided into two panels. The left panel, titled "Overview", shows a table of authentication details. The right panel, titled "Steps", lists a sequence of events with their corresponding IDs and descriptions.

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

Authentication Details	
Source Timestamp	2024-01-28 17:28:31.573
Received 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-Accept

Benutzeranmeldung bei ISE überprüfen

Zugehörige Informationen

- [Bedienungsanleitung für AsyncOS 14.0 für Cisco Secure Web Appliance](#)
- [ISE 3.0 - Administratorhandbuch](#)
- [ISE-Kompatibilitätsmatrix für Secure Web Appliance](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.