

Configurer l'authentification externe SWA avec ISE en tant que serveur RADIUS

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Topologie du réseau](#)

[Configurer](#)

[Configuration ISE](#)

[Configuration SWA](#)

[Vérifier](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes pour configurer l'authentification externe sur Secure Web Access (SWA) avec Cisco ISE comme serveur RADIUS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de l'appliance Web sécurisé Cisco.
- Connaissance de la configuration des stratégies d'authentification et d'autorisation sur ISE.
- Connaissances de base de RADIUS.

Cisco vous recommande également de disposer des éléments suivants :

- Accès à l'administration SWA et ISE.
- Versions compatibles WSA et ISE.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Lorsque vous activez l'authentification externe pour les utilisateurs administratifs de votre SWA, le périphérique vérifie les informations d'identification de l'utilisateur avec un serveur LDAP (Lightweight Directory Access Protocol) ou RADIUS comme spécifié dans la configuration de l'authentification externe.

Topologie du réseau



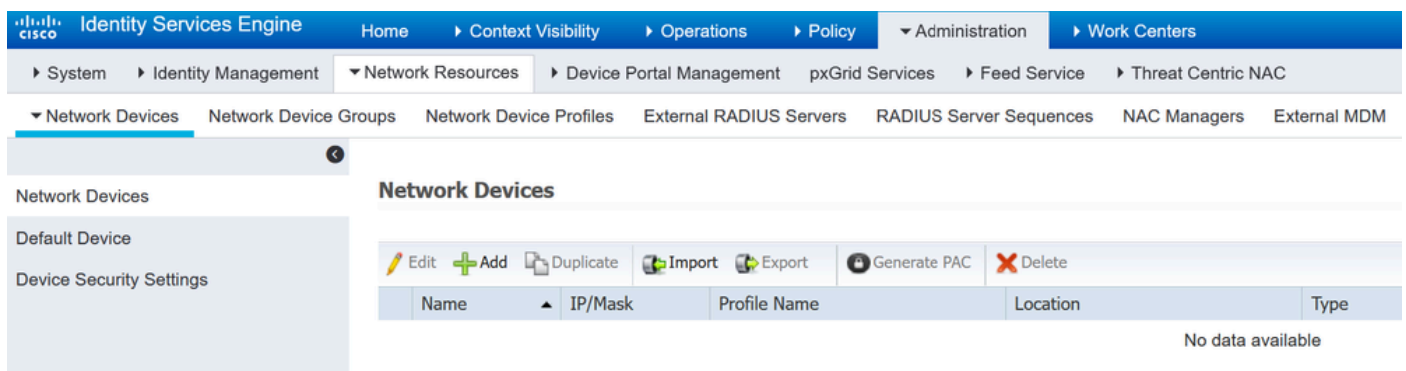
Schéma de topologie du réseau

Les utilisateurs administratifs accèdent à SWA sur le port 443 avec leurs informations d'identification. SWA vérifie les informations d'identification avec le serveur RADIUS.

Configurer

Configuration ISE

Étape 1. Ajoutez un nouveau périphérique réseau. Accédez à Administration > Network Resources > Network Devices > +Add.



Ajouter SWA en tant que périphérique réseau dans ISE

Étape 2. Attribuez un nom à l'objet périphérique réseau et insérez l'adresse IP SWA.

Cochez la case RADIUS et définissez un secret partagé.



Remarque : la même clé doit être utilisée ultérieurement pour configurer le serveur RADIUS dans SWA.

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

Configurer la clé partagée du périphérique réseau SWA

Étape 2.1. Cliquez sur Submit.

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

Envoyer la configuration des périphériques réseau

Étape 3. Créez les groupes d'identités utilisateur requis. Accédez à Administration > Identity Management > Groups > User Identity Groups > + Add.



Remarque : vous devez configurer différents groupes d'utilisateurs pour qu'ils correspondent à différents types d'utilisateurs.

Identity Groups

- Endpoint Identity Groups
- User Identity Groups

User Identity Groups

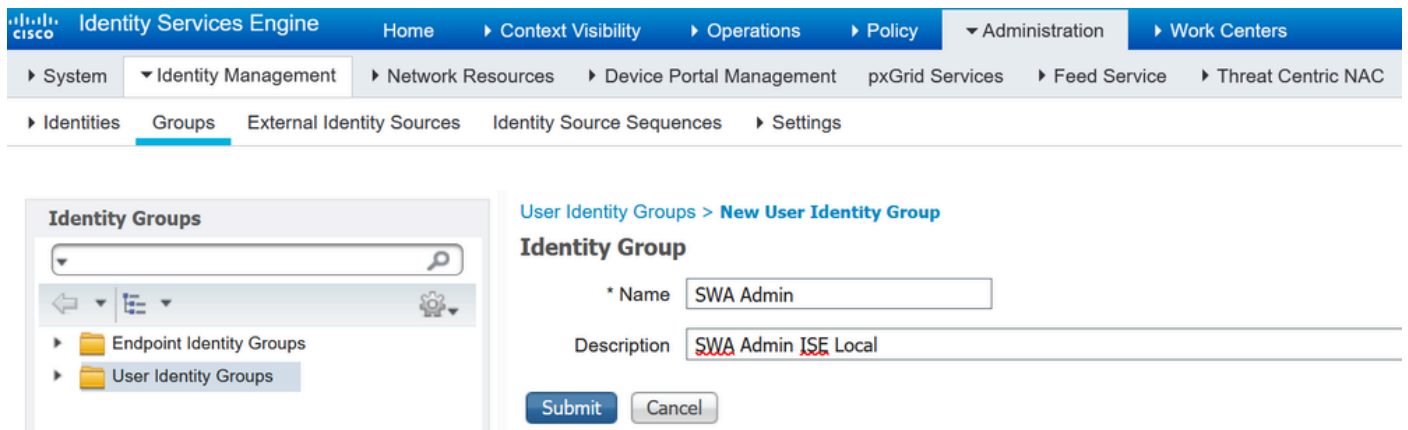
Edit + Add X Delete Import Export

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

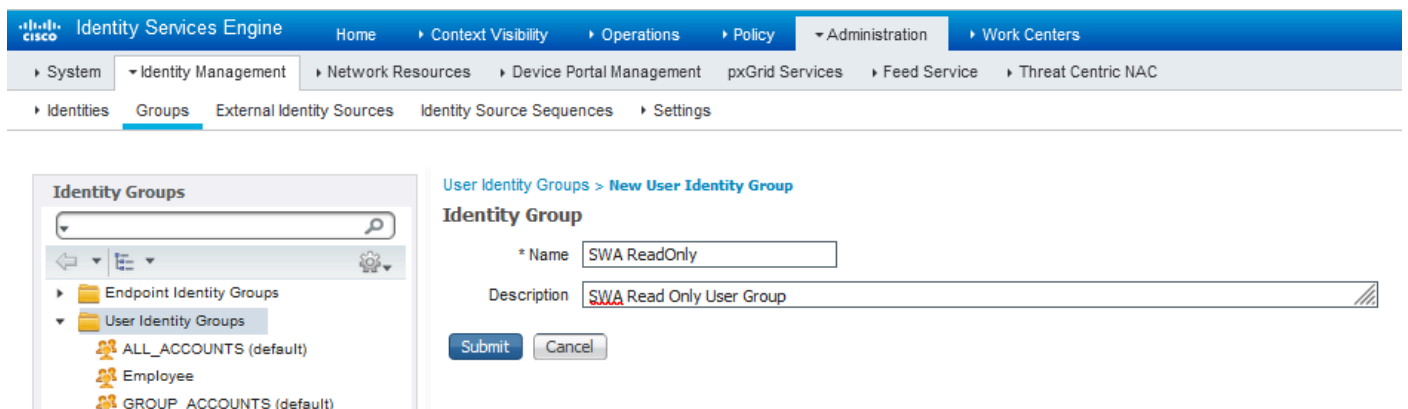
Ajouter un groupe d'identités utilisateur

Étape 4. Saisissez le nom du groupe, sa description (facultatif) et Submit. Répétez ces étapes

pour chaque groupe. Dans cet exemple, vous créez un groupe pour les utilisateurs administrateurs et un autre pour les utilisateurs en lecture seule.



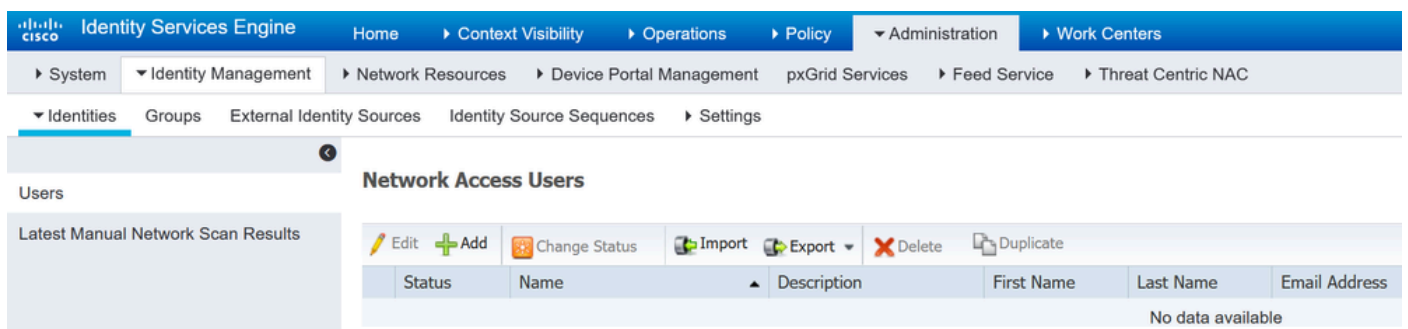
Ajouter un groupe d'



identités utilisateurAjouter un groupe d'identités utilisateur pour les utilisateurs SWA en lecture seule

Étape 5. Vous devez créer des utilisateurs d'accès réseau correspondant au nom d'utilisateur configuré dans SWA.

Créez les utilisateurs d'accès réseau et ajoutez-les à leur groupe correspondant. Accédez à Administration > Identity Management > Identities > + Add.



Ajouter des utilisateurs locaux dans ISE

Étape 5.1. Vous devez créer des utilisateurs d'accès réseau avec des droits d'administrateur. Attribuez un nom et un mot de passe.

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: adminuser

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: Re-Enter Password:

* Login Password:

Ajouter un utilisateur Admin

Étape 5.2. Choisissez SWA Admin dans la section User Groups.

Account Disable Policy

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

User Groups

Assign Admin Group to the Admin User

Étape 5.3. Vous devez créer un utilisateur avec des droits en lecture seule. Attribuez un nom et un mot de passe.

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"/> ⓘ

Ajouter un utilisateur en lecture seule

Étape 5.4. Sélectionnez SWA ReadOnly dans la section User Groups.

Account Disable Policy

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

User Groups

ⓘ

Attribuer un groupe d'utilisateurs en lecture seule à l'utilisateur en lecture seule

Étape 6. Créez le profil d'autorisation pour l'utilisateur Admin.

Accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.

Définissez un nom pour le profil d'autorisation et assurez-vous que le type d'accès est défini sur ACCESS_ACCEPT.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionaryes 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

Ajouter un profil d'autorisation pour les administrateurs

Étape 6.1. Dans les paramètres d'attributs avancés, accédez à Radius > Class—[25] et entrez la valeur Administrator et cliquez sur Submit.

Advanced Attributes Settings

Radius:Class = Administrator

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit Cancel

Add Authorization Profile for Admin Users

Étape 7. Répétez l'étape 6 pour créer le profil d'autorisation pour l'utilisateur en lecture seule.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys 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:

Ajouter un profil d'autorisation pour les utilisateurs en lecture seule

ÉTAPE 7.1. Cette fois, créez Radius : Class avec la valeur ReadUser à la place de Administrator.

Advanced Attributes Settings

Radius:Class = ReadUser

Attributes Details

Access Type = ACCESS_ACCEPT
Class = ReadUser

Submit Cancel

Ajouter un profil d'autorisation pour les utilisateurs en lecture seule

Étape 8. Créez des ensembles de stratégies qui correspondent à l'adresse IP SWA. Cela empêche l'accès à d'autres périphériques avec ces informations d'identification utilisateur.

Accédez à Policy > PolicySets et cliquez sur l'icône + placée dans l'angle supérieur gauche.

Policy Sets

+ Status	Policy Set Name	Description	Conditions
<input type="text" value="Search"/>			

Ajouter un jeu de stratégies dans ISE

Étape 8.1. Une nouvelle ligne est placée en haut de vos ensembles de stratégies.

Attribuez un nom à la nouvelle stratégie et ajoutez une condition pour l'attribut RADIUS NAS-IP-Address afin qu'il corresponde à l'adresse IP SWA.

Cliquez sur Utiliser pour conserver les modifications et quitter l'éditeur.

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

Ajouter une stratégie pour mapper un périphérique réseau SWA

Étape 8.2. Cliquez sur Save.

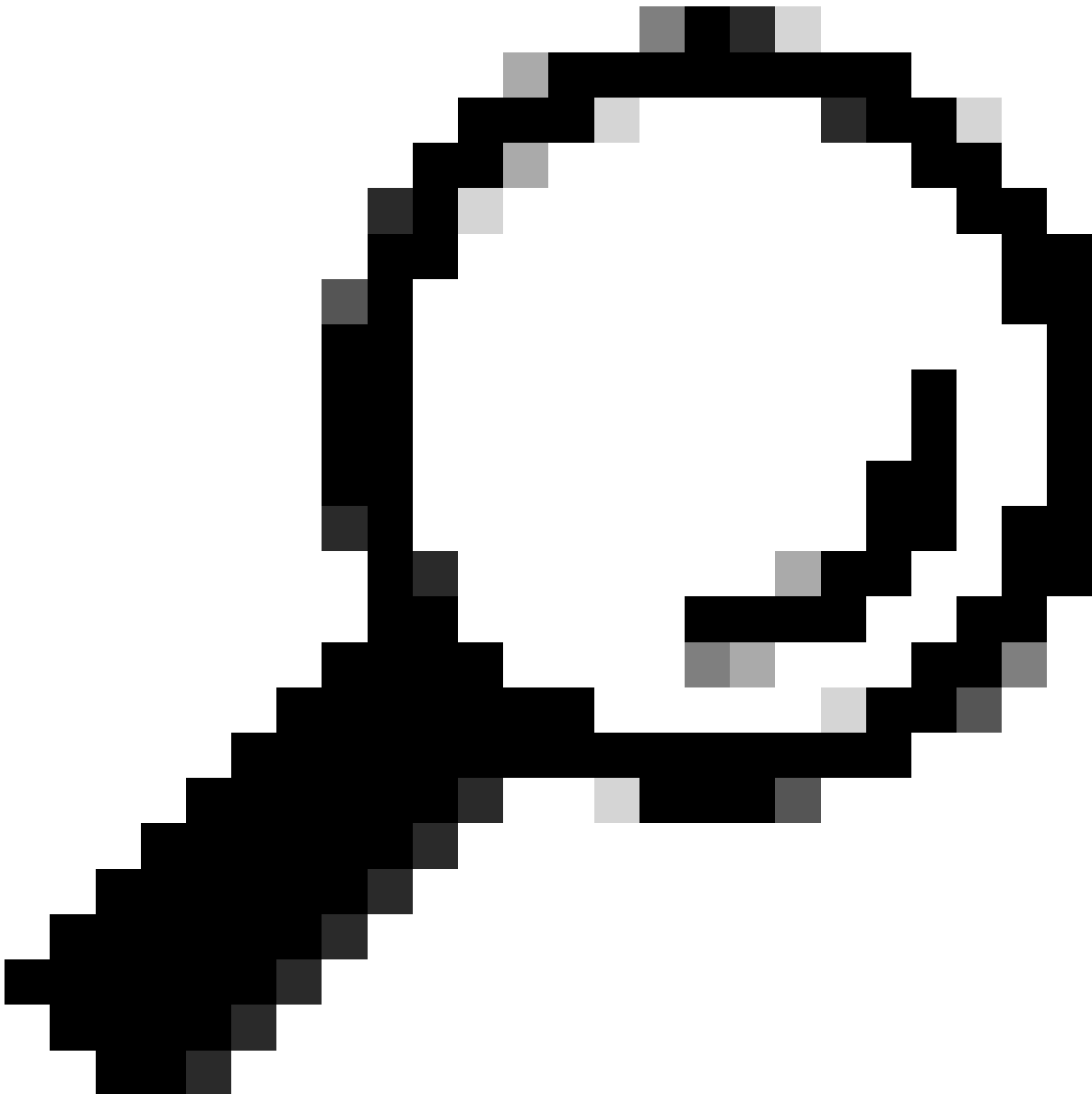
Policy Sets

[Reset Policyset Hitcounts](#)[Reset](#)[Save](#)

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search								
		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](#)

Enregistrer la stratégie



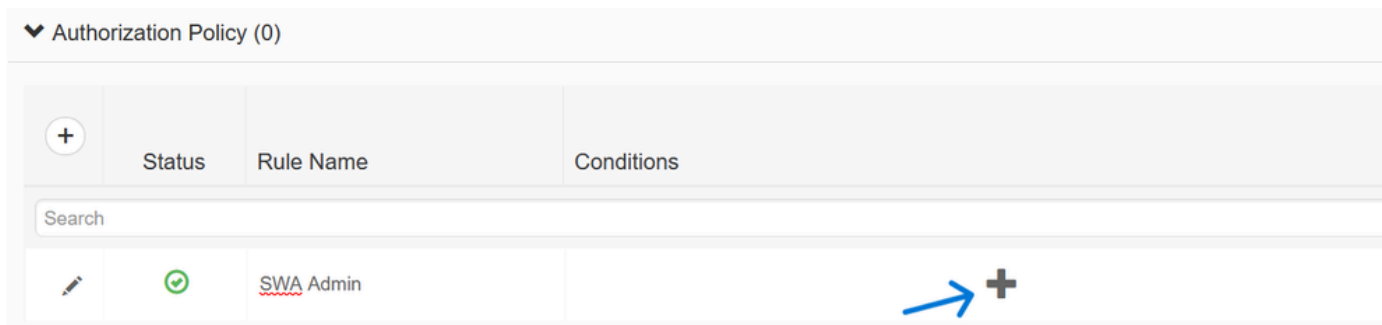
Conseil : dans cet article, la liste des protocoles d'accès réseau par défaut est autorisée. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.

Étape 9. Pour afficher les nouveaux ensembles de stratégies, cliquez sur l'icône > dans la colonne View. Développez le menu Politique d'autorisation et cliquez sur l'icône + pour ajouter une

nouvelle règle permettant l'accès à l'utilisateur disposant de droits d'administrateur.

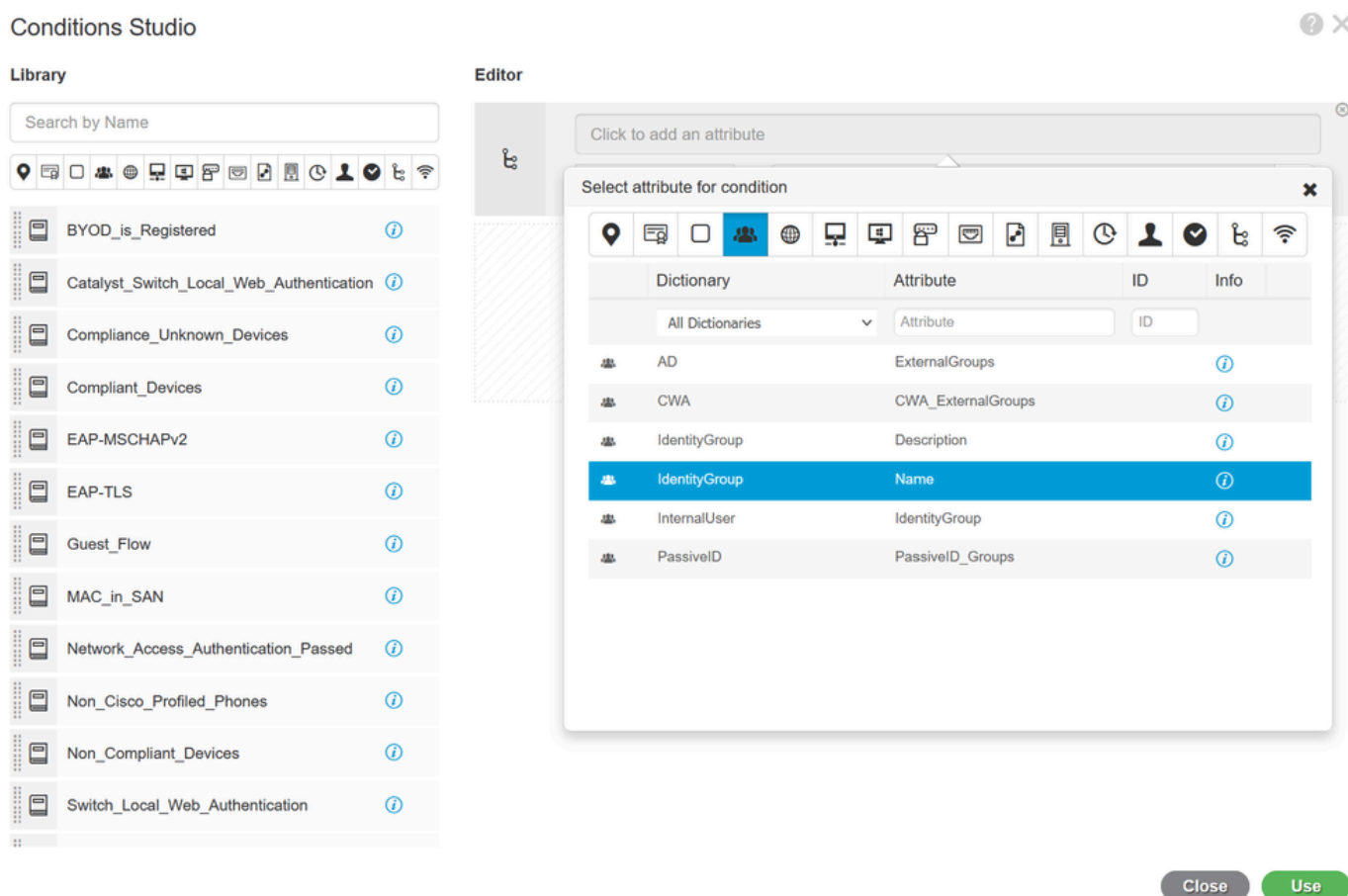
Définissez un nom.

Étape 9.1. Pour créer une condition correspondant au groupe d'utilisateurs Admin, cliquez sur l'icône +.



Ajouter une condition de stratégie d'autorisation

Étape 9.2. Définissez les conditions pour faire correspondre le groupe d'identités de dictionnaire avec le groupe d'identités Attribute Name Equals User Identity Groups : SWA admin.



Sélectionnez Identity Group comme condition

Étape 9.3. Faites défiler vers le bas et sélectionnez User Identity Groups : SWA admin.

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

Faites défiler vers le bas et sélectionnez Identity Group Name

Étape 9.4. Cliquez sur Utiliser.

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

Sélectionner la stratégie d'autorisation pour le groupe d'utilisateurs Admin SWA

Étape 10. Cliquez sur l'icône + pour ajouter une deuxième règle pour autoriser l'accès à l'utilisateur avec des droits en lecture seule.

Définissez un nom.

Définissez les conditions pour faire correspondre le groupe d'identités de dictionnaire avec le groupe d'identités Attribute Name Equals User Identity Groups : SWA ReadOnly et cliquez sur Use.

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

Sélectionner la stratégie d'autorisation pour le groupe d'utilisateurs en lecture seule

Étape 11. Définissez le profil d'autorisation pour chaque règle, puis cliquez sur Enregistrer.

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		Hits	Actions
				Profiles	Security Groups		
	✓	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

Sélectionner le profil d'autorisation

Configuration SWA

Étape 1. Dans l'interface utilisateur graphique de SWA, accédez à Administration système et cliquez sur Users.

Étape 2. Cliquez sur Enable dans External Authentication.

The screenshot shows the Cisco Secure Web Appliance (S100V) administration interface. The navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The 'Users' section contains a table with the following data:

<input type="checkbox"/>	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 highlighted with a red arrow.

Activer l'authentification externe dans SWA

Étape 3. Entrez l'adresse IP ou le nom de domaine complet de l'ISE dans le champ RADIUS Server Hostname et entrez le même secret partagé que celui qui est configuré à l'étape 2, Configuration ISE.

Étape 4. Sélectionnez Mapper les utilisateurs authentifiés en externe à plusieurs rôles locaux dans Mappage de groupe.

Étape 4.1. Saisissez Administrator dans le champ RADIUS CLASS Attribute et sélectionnez Role Administrator.

Étape 4.2. Saisissez ReadUser dans le champ RADIUS CLASS Attribute et sélectionnez Role Read-Only Operator.



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

Configuration de l'authentification externe pour le serveur RADIUS

Étape 5 : pour configurer les utilisateurs dans SWA, cliquez sur Add User. Entrez User Name et sélectionnez User Type requis pour le rôle souhaité. Entrez Passphrase et Retype Passphrase, qui est requis pour l'accès à l'interface utilisateur graphique si l'appliance ne peut pas se connecter à un serveur RADIUS externe.

Remarque : si l'apppliance ne parvient pas à se connecter à un serveur externe, elle tente d'authentifier l'utilisateur en tant qu'utilisateur local défini sur l'apppliance Web sécurisée.

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	

Configuration utilisateur dans SWA

Étape 6 : cliquez sur Submit and Commit Changes.

Vérifier

Accédez à l'interface utilisateur graphique SWA avec les informations d'identification utilisateur

configurées et vérifiez les journaux actifs dans ISE. Pour vérifier les journaux en direct dans ISE, accédez à Operations > Live Logs :

The screenshot displays the Cisco Identity Services Engine (ISE) interface. At the top, the Cisco logo and 'Identity Services Engine' are visible. The main content is divided into two sections: 'Overview' and 'Authentication Details'. The 'Overview' section shows a table with the following data:

Field	Value
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

The 'Authentication Details' section shows a table with the following data:

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

To the right of these sections is a 'Steps' list showing a sequence of events:

- 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

Vérification de la connexion utilisateur ISE

Informations connexes

- [Guide de l'utilisateur d'AsyncOS 14.0 pour Cisco Secure Web Appliance](#)
- [Guide d'administration ISE 3.0](#)
- [Matrice de compatibilité ISE pour l'appliance Web sécurisée](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.