

RADIUSサーバとしてISEを使用したSWA外部認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Network Topology](#)

[設定](#)

[ISE 設定](#)

[SWAの設定](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco ISEをRADIUSサーバとして使用して、Secure Web Access(SWA)で外部認証を設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Web Applianceの基礎知識。
- ISEでの認証および認可ポリシー設定に関する知識。
- RADIUS の基礎知識。

次の情報も含めることをお勧めします。

- SWAおよびISE管理アクセス。
- 互換性のあるWSAおよびISEバージョン。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- SWA 14.0.2-012
- ISE 3.0.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

SWAの管理ユーザの外部認証を有効にすると、デバイスは外部認証設定で指定されているLightweight Directory Access Protocol(LDAP)またはRADIUSサーバを使用してユーザクレデンシャルを確認します。

Network Topology



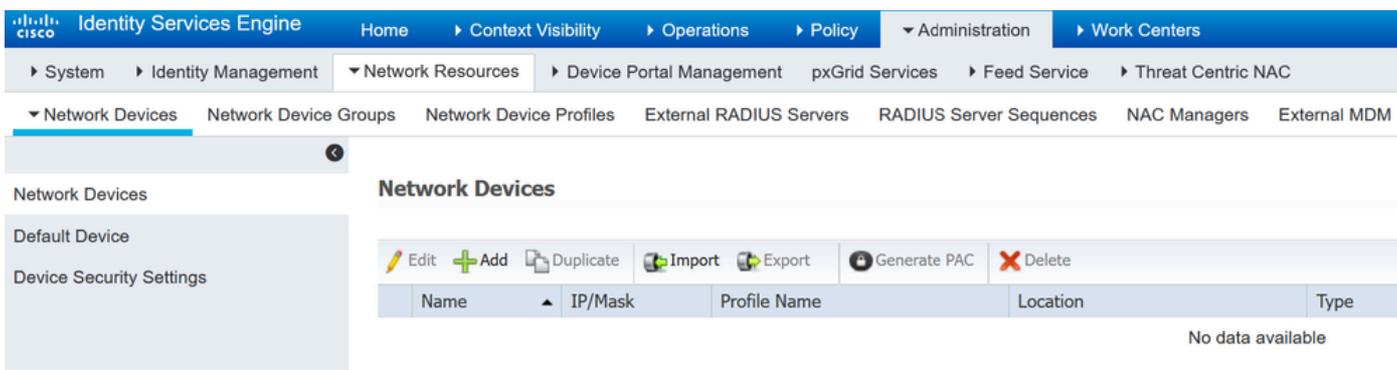
ネットワークトポロジ図

管理ユーザは、クレデンシャルを使用してポート443でSWAにアクセスします。SWAがRADIUSサーバでクレデンシャルを確認します。

設定

ISE 設定

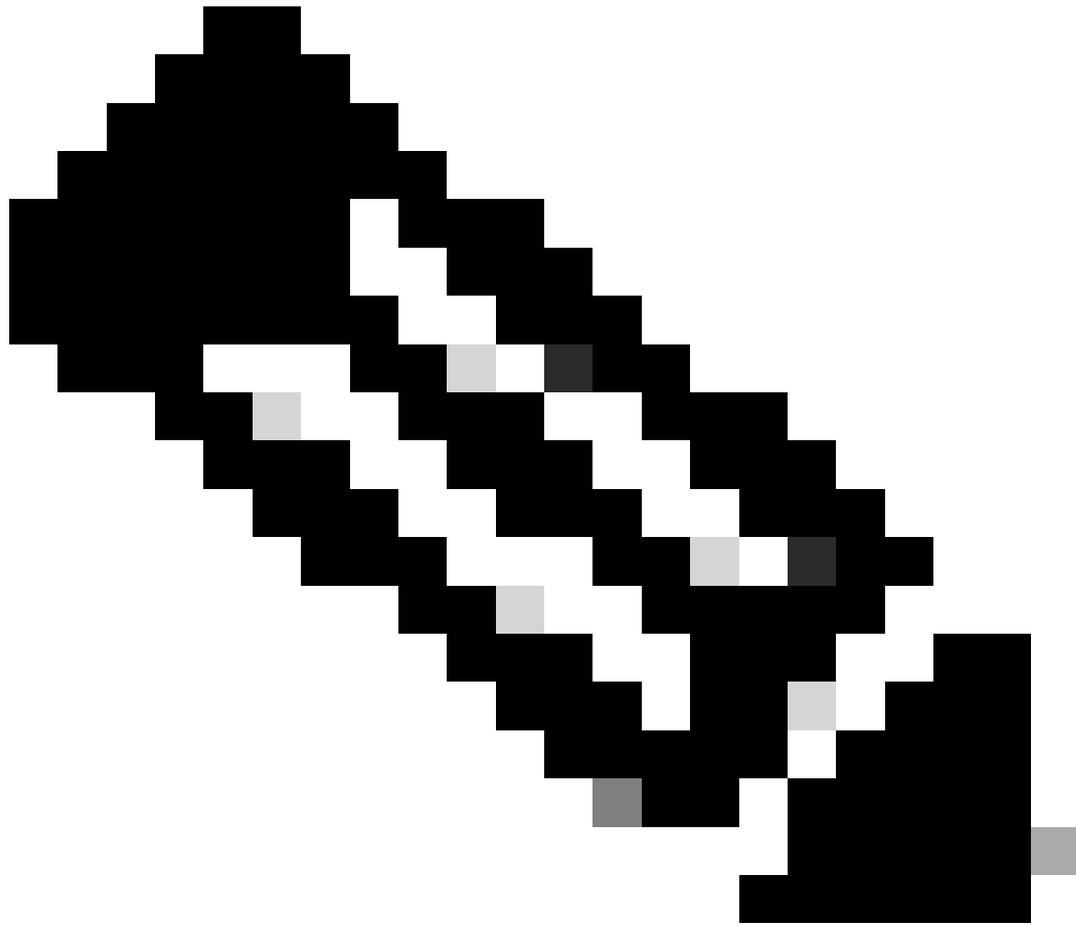
ステップ 1：新しいネットワークデバイスを追加します。Administration > Network Resources > Network Devices > +Addの順に移動します。



ISEのネットワークデバイスとしてのSWAの追加

ステップ 2：ネットワークデバイスオブジェクトに名前を割り当て、SWAのIPアドレスを挿入します。

RADIUSのチェックボックスをオンにして、共有秘密を定義します。



注：後でSWAにRADIUSサーバを設定するときにも、同じキーを使用する必要があります。

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ネットワークデバイスの共有キーの設定

ステップ 2.1 : [Submit] をクリックします。

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

ネットワークデバイス設定の送信

ステップ 3 : 必要なユーザIDグループを作成します。Administration > Identity Management > Groups > User Identity Groups > + Addの順に移動します。

注：異なるユーザタイプに一致させるには、異なるユーザグループを設定する必要があります。

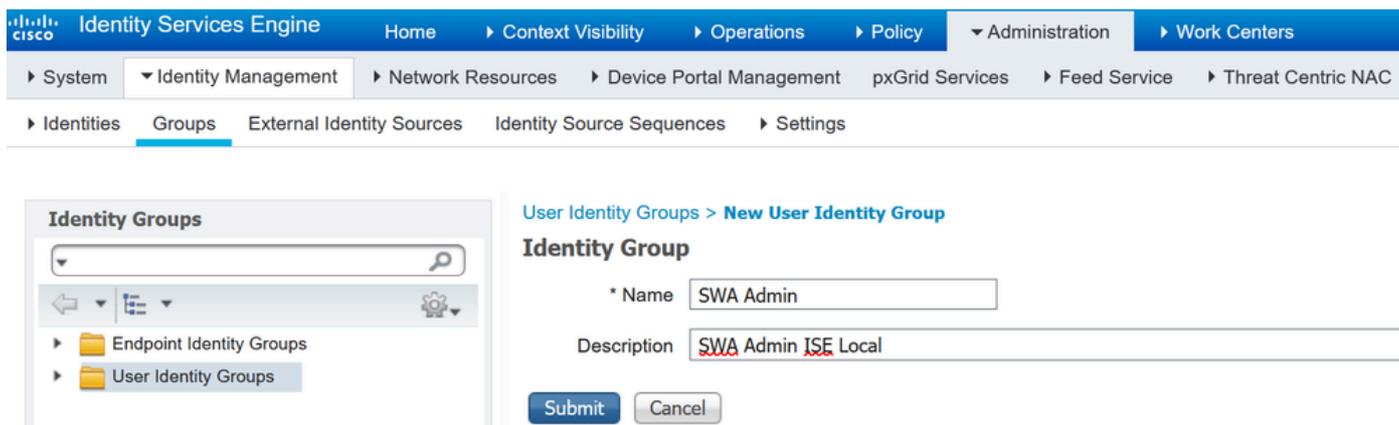
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Administration > Work Centers > Identity Management > Groups. The 'User Identity Groups' section is active, displaying a table of existing groups. The table has columns for 'Name' and 'Description'. The groups listed are:

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

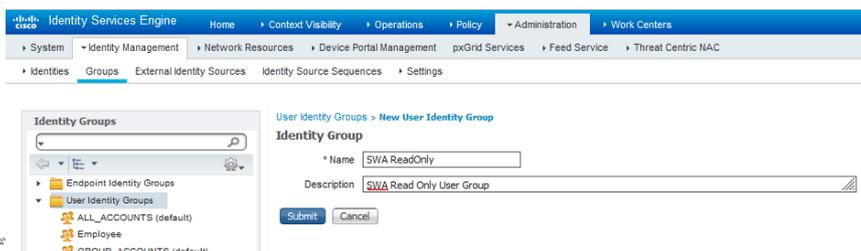
ユーザIDグループの追加

ステップ 4：グループ名、説明（オプション）、および送信を入力します。グループごとにこれ

らの手順を繰り返します。この例では、管理者ユーザ用のグループと、読み取り専用ユーザ用のグループを作成します。



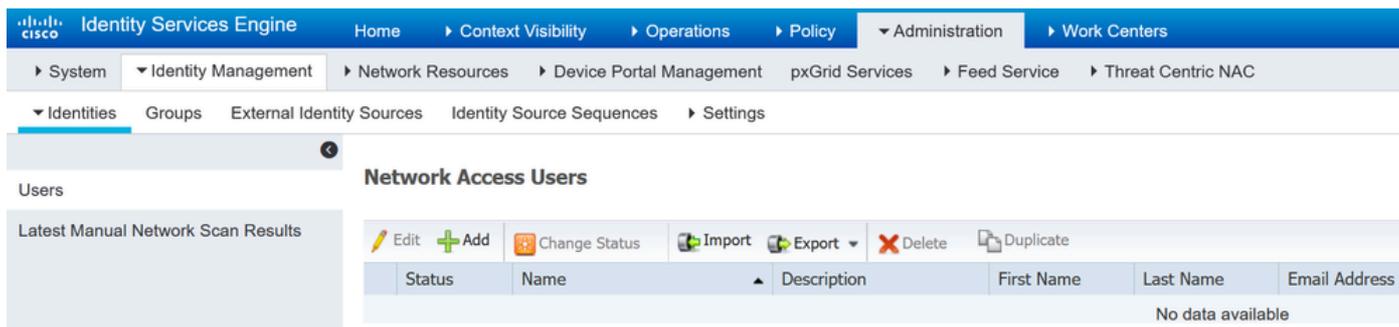
ユーザID



グループの追加
SWA読み取り専用ユーザのユーザIDグループの追加

ステップ 5 : SWAで設定されたユーザ名と一致するネットワークアクセスユーザを作成する必要があります。

ネットワークアクセスユーザを作成し、対応するグループに追加します。Administration > Identity Management > Identities > + Addの順に移動します。



ISEでのローカルユーザの追加

ステップ 5.1 : 管理者権限を持つネットワークアクセスユーザを作成する必要があります。名前とパスワードを割り当てます。

Identity Services Engine Administration > Work Centers > Identity Management > Identities > Network Access Users List > New Network Access User

Network Access User

* Name:

Status: Enabled

Email:

Passwords

Password Type:

Password:

Re-Enter Password:

* Login Password:

管理者ユーザの追加

ステップ 5.2 : User GroupsセクションでSWA Adminを選択し、Admin UserにAdmin Groupを割り当てます。

ステップ 5.3 : 読み取り専用権限を持つユーザを作成する必要があります。名前とパスワードを割り当てます。

Identity Services Engine Administration > Work Centers > Identity Management > Identities > Network Access Users List > New Network Access User

Network Access User

* Name:

Status: Enabled

Email:

Passwords

Password Type:

Password:

Re-Enter Password:

* Login Password:

Enable Password:

読み取り専用ユーザの追加

ステップ 5.4 : User GroupsセクションでSWA ReadOnlyを選択します。

▼ Account Disable Policy

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

▼ User Groups

SWA ReadOnly

Submit

Cancel

読み取り専用ユーザグループの読み取り専用ユーザへの割り当て

手順 6： 管理者ユーザの許可プロファイルを作成します。

Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Addの順に移動します。

許可プロファイルの名前を定義し、アクセスタイプがACCESS_ACCEPTに設定されていることを確認します。

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main navigation bar includes: Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. Under Policy Elements, the 'Results' sub-menu is selected. The left sidebar shows a tree view with 'Authentication' and 'Authorization' expanded. Under 'Authorization', 'Authorization Profiles' is selected. The main content area is titled 'Authorization Profiles > New Authorization Profile' and 'Authorization Profile'. The form fields are: '* Name' (SWA Admin), 'Description' (empty), '* Access Type' (ACCESS_ACCEPT), 'Network Device Profile' (Cisco), 'Service Template' (checkbox), 'Track Movement' (checkbox with info icon), and 'Passive Identity Tracking' (checkbox with info icon).

管理者ユーザの許可プロファイルの追加

ステップ 6.1： Advanced Attributes Settingsで、Radius > Class—[25]に移動し、値 Administratorを入力してSubmit.

▼ Advanced Attributes Settings

Radius:Class = Administrator

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit

Cancel

Add Authorization Profile for Admin Usersをクリックします

手順 7 : ステップ6を繰り返して、読み取り専用ユーザの許可プロファイルを作成します。

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

読み取り専用ユーザの許可プロファイルの追加

ステップ 7.1 : 今回はAdministratorではなくReadUserの値でRadius:Classを作成します。

▼ Advanced Attributes Settings

Radius:Class = ReadUser

▼ Attributes Details

Access Type = ACCESS_ACCEPT
Class = ReadUser

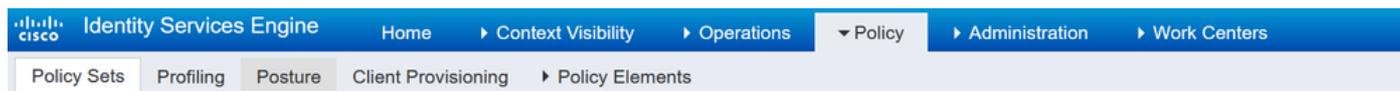
Submit

Cancel

読み取り専用ユーザの許可プロファイルの追加

ステップ 8 : SWAのIPアドレスに一致するポリシーセットを作成します。これは、これらのユーザクレデンシャルを使用して他のデバイスにアクセスするのを防ぐためです。

Policy > PolicySetsに移動し、左上隅にある+アイコンをクリックします。



Policy Sets

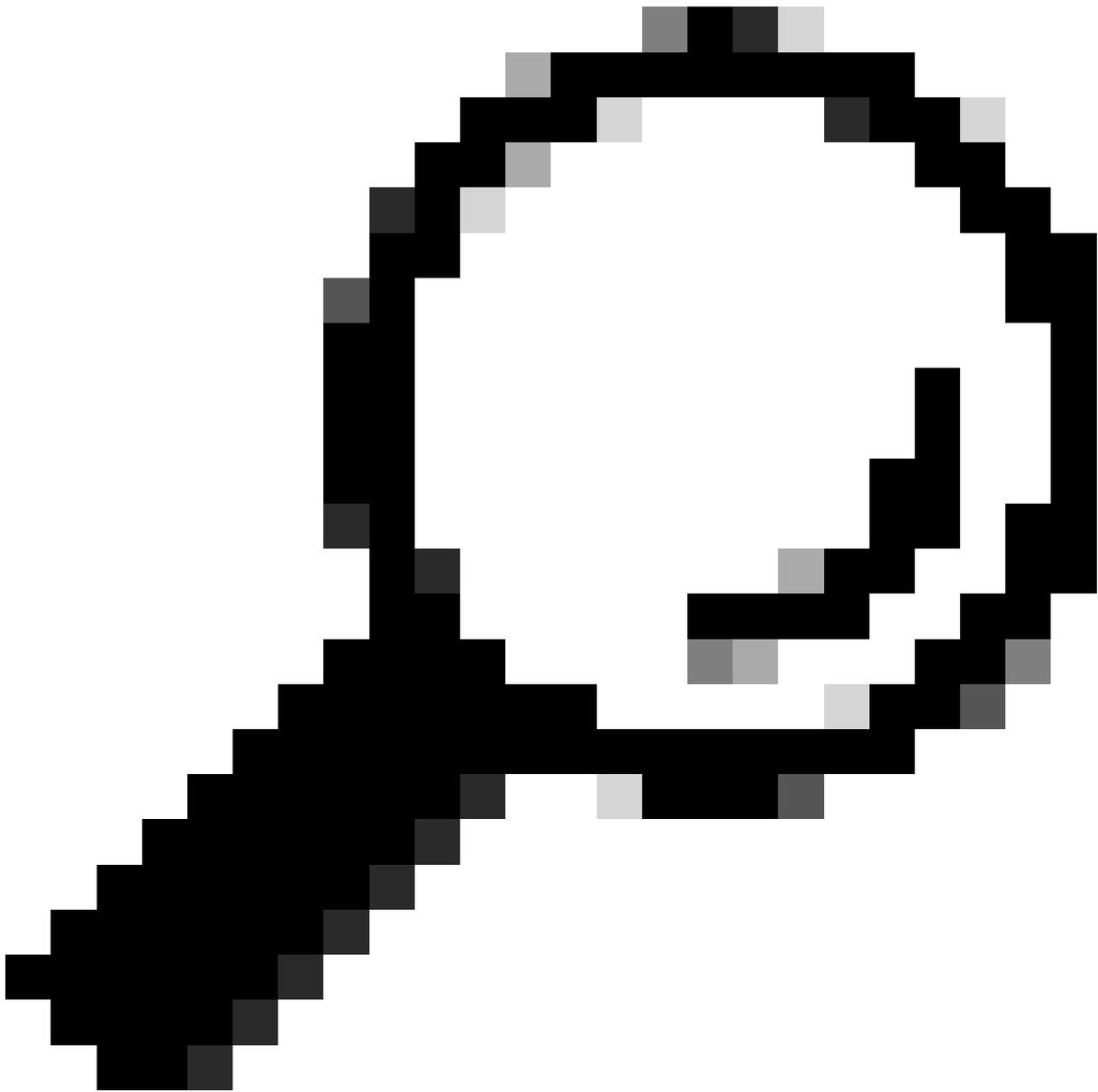
+ Status	Policy Set Name	Description	Conditions
Search			

ISEでのポリシーセットの追加

ステップ 8.1 : 新しい行がポリシーセットの先頭に配置されます。

新しいポリシーに名前を付け、SWAのIPアドレスと一致するようにRADIUS NAS-IP-Address属性の条件を追加します。

Useをクリックして変更を保存し、エディタを終了します。



ヒント：この記事では、デフォルトのネットワークアクセスプロトコルリストが許可されています。新しいリストを作成し、必要に応じて絞り込むことができます。

ステップ 9：新しいポリシーセットを表示するには、表示列の>アイコンをクリックします。Authorization Policyメニューを展開し、+アイコンをクリックして、管理者権限を持つユーザへのアクセスを許可する新しいルールを追加します。

名前を設定します。

ステップ 9.1：管理者ユーザグループに一致する条件を作成するには、+アイコンをクリックします。

許可ポリシー条件の追

▼ Authorization Policy (0)

	Status	Rule Name	Conditions
		<u>SWA Admin</u>	

加

ステップ 9.2 : 条件を、Dictionary Identity Group with Attribute Name Equals User Identity Groups: SWA admin.

Select Identity Group as Condition

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		?

に設定し
ます。

Close Use

ステップ 9.3 : 下にスクロールしてUser Identity Groups: SWA adminを選択します。

下にスクロールして

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

Identity Group Nameを選択します。

ステップ 9.4 : Useをクリックします。

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

SWA管理ユーザグループの許可ポリシーの選択

ステップ 10: +アイコンをクリックして、読み取り専用権限を持つユーザにアクセスを許可する2番目のルールを追加します。

名前を設定します。

条件を、Dictionary Identity Group with Attribute Name Equals User Identity Groups: SWA ReadOnlyに一致するように設定し、Useをクリックします。

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_Profiling_Phones (i)

Editor

IdentityGroup-Name

Equals

× User Identity Groups:SWA ReadOnly

Set to 'Is not'

Duplicate Save

+ New AND OR

Close Use

読み取り専用ユーザグループの許可ポリシーの選択

ステップ 11 ルールごとに許可プロファイルを設定し、Saveをクリックします。

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

SWAの設定

ステップ 1 : SWAのGUIで、System Administrationに移動し、Usersをクリックします。

ステップ 2 : External AuthenticationでEnableをクリックします。

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. The 'Second Factor Authentication Settings' section shows 'Two Factor Authentication is disabled.' and an 'Enable...' button.

SWAでの外部認証の有効化

ステップ 3 : RADIUSサーバホスト名フィールドにISEのIPアドレスまたはFQDNを入力し、ステップ2のISE設定で設定したのと同じ共有秘密を入力します。

ステップ 4 : Map externally authenticated users to multiple local roles in Group Mappingを選択します。

ステップ 4.1 : RADIUS CLASS AttributeフィールドにAdministratorと入力し、Role Administratorを選択します。

ステップ 4.2 : RADIUS CLASS AttributeフィールドにReadUserと入力し、Role Read-Only Operatorを選択します。

Edit External Authentication

External Authentication Settings

Enable External Authentication

Authentication Mode: Password based Authentication

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:

RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Certificate	Add Row
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サーバの外部認証設定

ステップ5:SWAでユーザを設定するには、ユーザの追加をクリックします。ユーザ名を入力し、目的のロールに必要なユーザタイプを選択します。パスワードと再入力：パスワードを入力します。これは、アプライアンスが外部RADIUSサーバに接続できない場合にGUIアクセスに必要です。

注：アプライアンスが外部サーバに接続できない場合、アプライアンスはユーザをセキュアWebアプライアンスで定義されているローカルユーザとして認証しようとします。

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"/> 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	

SWAでのユーザ設定

ステップ6:Submitをクリックして、変更を確定します。

確認

設定されたユーザクレデンシャルでSWA GUIにアクセスし、ISEのライブログを確認します。

ISEのライブログを確認するには、Operations > Live Logsの順に移動します。

Identity Services Engine

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

ユーザログインISEの確認

関連情報

- [AsyncOS 14.0 for Cisco Secure Web Applianceユーザガイド](#)
- [ISE 3.0管理ガイド](#)
- [セキュアWebアプライアンスのISE互換性マトリックス](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。