

将ISE配置为RADIUS服务器的SWA外部身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络拓扑](#)

[配置](#)

[ISE配置](#)

[SWA配置](#)

[验证](#)

[相关信息](#)

简介

本文档介绍在Cisco ISE作为RADIUS服务器的安全Web访问(SWA)上配置外部身份验证的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全网络设备的基础知识。
- 了解ISE上的身份验证和授权策略配置。
- RADIUS基础知识。

Cisco建议您还应具备：

- SWA和ISE管理访问权限。
- 兼容的WSA和ISE版本。

使用的组件

本文档中的信息基于以下软件版本：

- SWA 14.0.2-012
- ISE 3.0.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

当您为SWA的管理用户启用外部身份验证时，设备会使用在外部身份验证配置中指定的轻型目录访问协议 (LDAP)或RADIUS服务器验证用户凭证。

网络拓扑



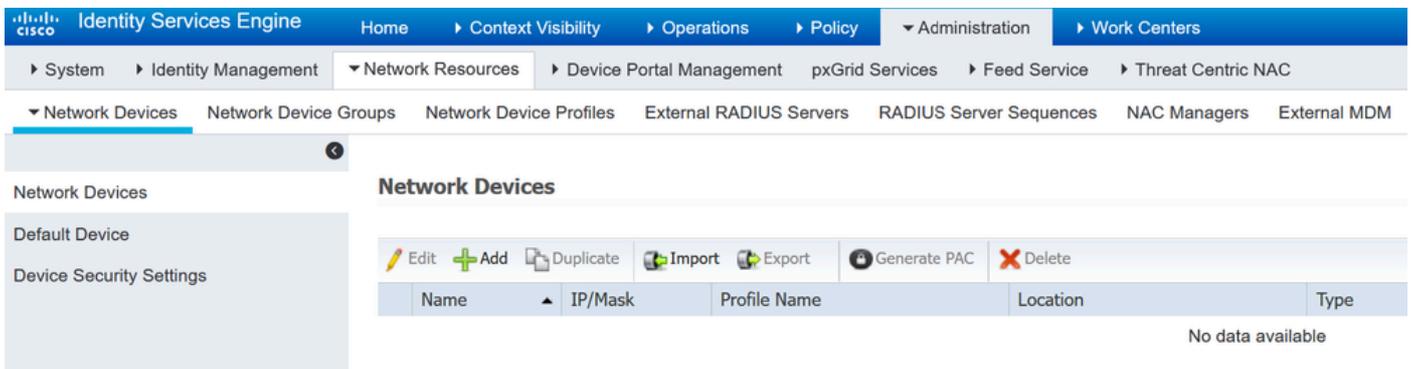
网络拓扑图

管理用户使用其凭证访问端口443上的SWA。SWA使用RADIUS服务器验证凭证。

配置

ISE 配置

步骤1: 添加新的网络设备。导航到管理>网络资源>网络设备> +Add。



在ISE中添加SWA作为网络设备

第二步：为网络设备对象分配名称并插入SWA IP地址。

选中RADIUS 复选框并定义共享密钥。



注意：稍后必须在SWA中配置相同的RADIUS服务器密钥。

Network Devices

Default Device

Device Security Settings

Network Devices List > SWA

Network Devices

* Name

Description

IP Address /

* Device Profile  Cisco

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

配置SWA网络设备共享密钥

步骤 2.1 单击“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

提交网络设备配置

第三步：创建所需的用户身份组。导航到管理>身份管理> Groups >用户身份组> + Add。



注意：您需要配置不同的用户组以匹配不同类型的用户。

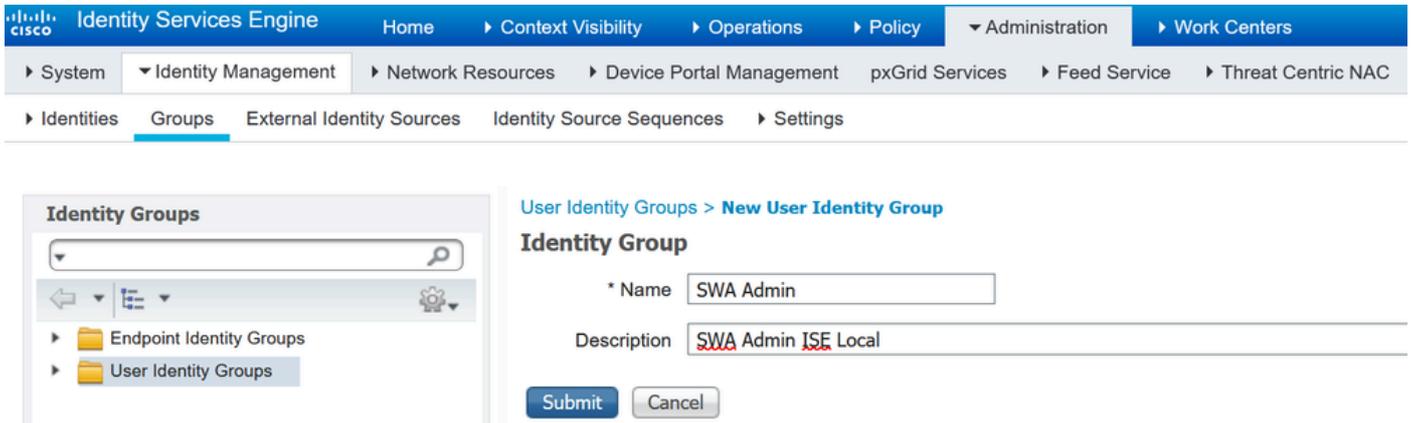
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main navigation bar includes: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Identities, Groups, External Identity Sources, Identity Source Sequences, and Settings. The 'Groups' tab is selected.

The 'Identity Groups' sidebar shows a tree view with 'Endpoint Identity Groups' and 'User Identity Groups' (selected). The main content area is titled 'User Identity Groups' and contains a table of existing groups.

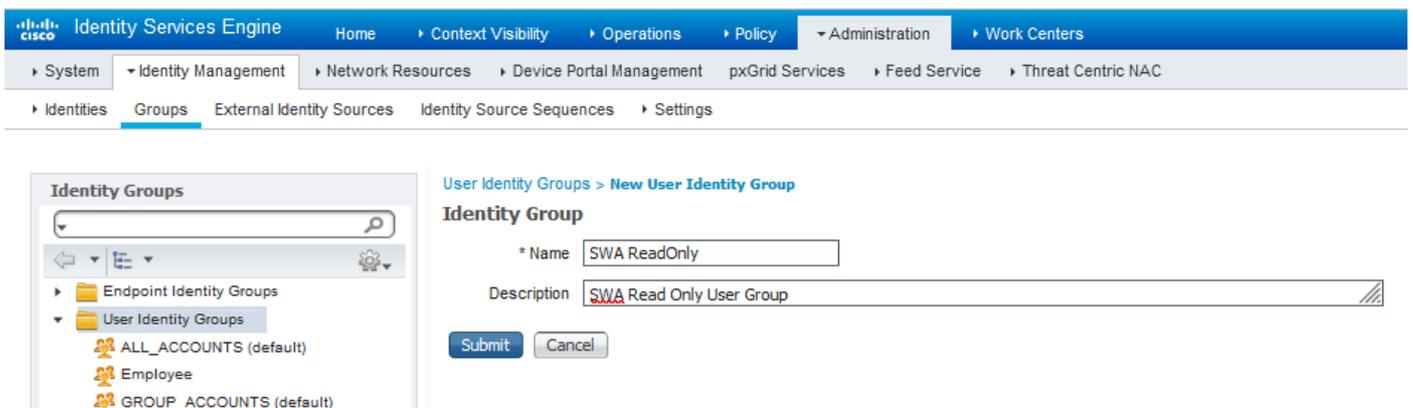
Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor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

添加用户身份组

第四步：输入组名称、说明（可选）和提交。对每个组重复这些步骤。在本示例中，您为管理员用户创建一个组，为只读用户创建另一个组。



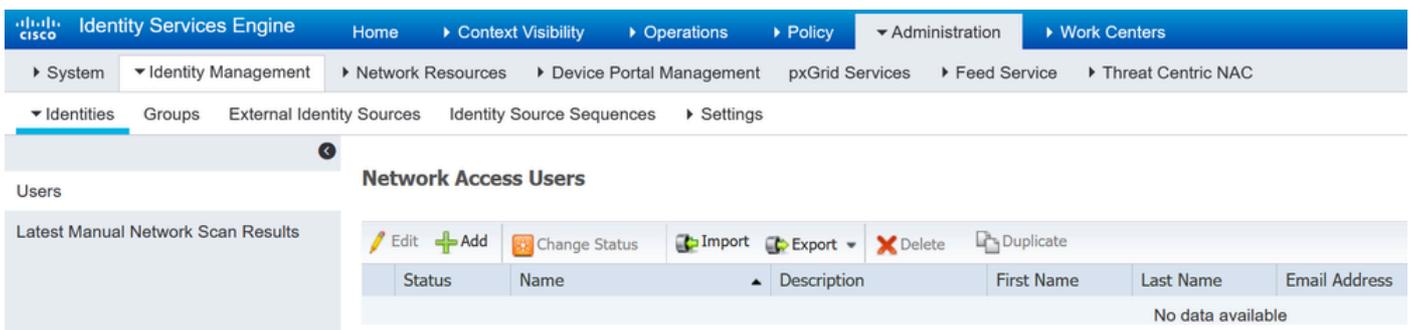
添加用户身份



组为SWA只读用户添加用户身份组

第五步：您需要创建与SWA中配置的用户名匹配的网络访问用户。

创建网络访问用户并将其添加到其对应组。导航到管理>身份管理>身份> + Add。



在ISE中添加本地用户

步骤 5.1 您需要创建具有管理员权限的网络访问用户。指定名称和密码。

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

添加管理员用户

步骤 5.2在User Groups部分中选择SWA Admin。

Account Disable Policy

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

User Groups

SWA Admin

将
Admin Group分配给Admin User

步骤 5.3您需要创建具有只读权限的用户。指定名称和密码。

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)

添加只读用户

步骤 5.4在User Groups部分中选择SWA ReadOnly。

Account Disable Policy

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

User Groups

SWA ReadOnly

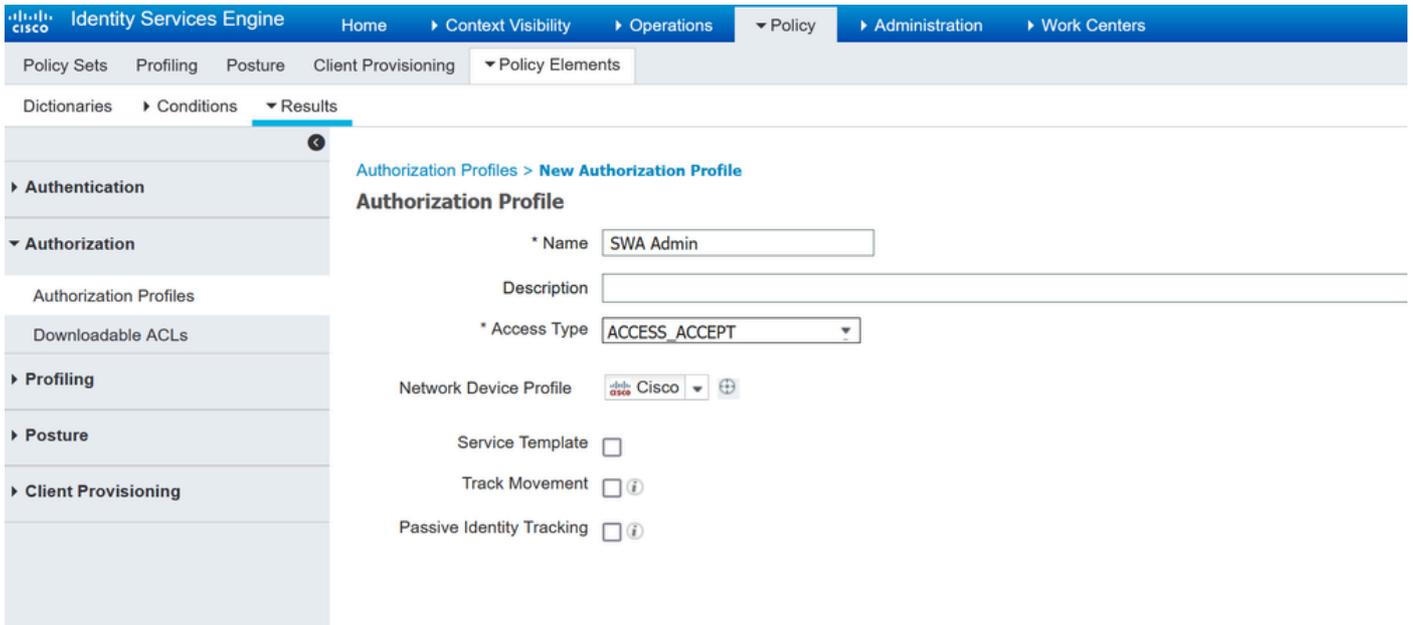
Submit Cancel

将只读用户组分配给只读用户

第六步：为管理员用户创建授权配置文件。

导航到策略>Policy元素>结果>授权>授权配置文件> +Add。

定义授权配置文件的名称，并确保将访问类型设置为ACCESS_ACCEPT。



添加管理员用户的授权配置文件

步骤 6.1 在“高级属性设置”中，导航到 Radius > Class—[25]，输入值 Administrator，然后点击提交

Advanced Attributes Settings

Radius:Class = Administrator

Attributes Details

Access Type = ACCESS_ACCEPT
Class = Administrator

Submit Cancel

添加管理员用户的授权配置文件

步骤 7. 重复第6步为只读用户创建授权配置文件。

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

为只读用户添加授权配置文件

第 7.1 步：使用值ReadUser创建Radius : Class，这次使用Administrator。

Advanced Attributes Settings

Radius:Class = ReadUser

Attributes Details

Access Type = ACCESS_ACCEPT
Class = ReadUser

Submit Cancel

为只读用户添加授权配置文件

步骤 8 创建与SWA IP地址匹配的策略集。这是为了防止使用这些用户凭证访问其他设备。

导航到策略>策略集，点击位于左上角的+图标。

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

在ISE中添加策略集

步骤 8.1 新行位于策略集的顶部。

为新策略命名并为RADIUS NAS-IP-Address属性添加一个条件以匹配SWA IP地址。

单击Use以保留更改并退出编辑器。

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

添加策略以映射SWA网络设备

步骤 8.2 Click Save.

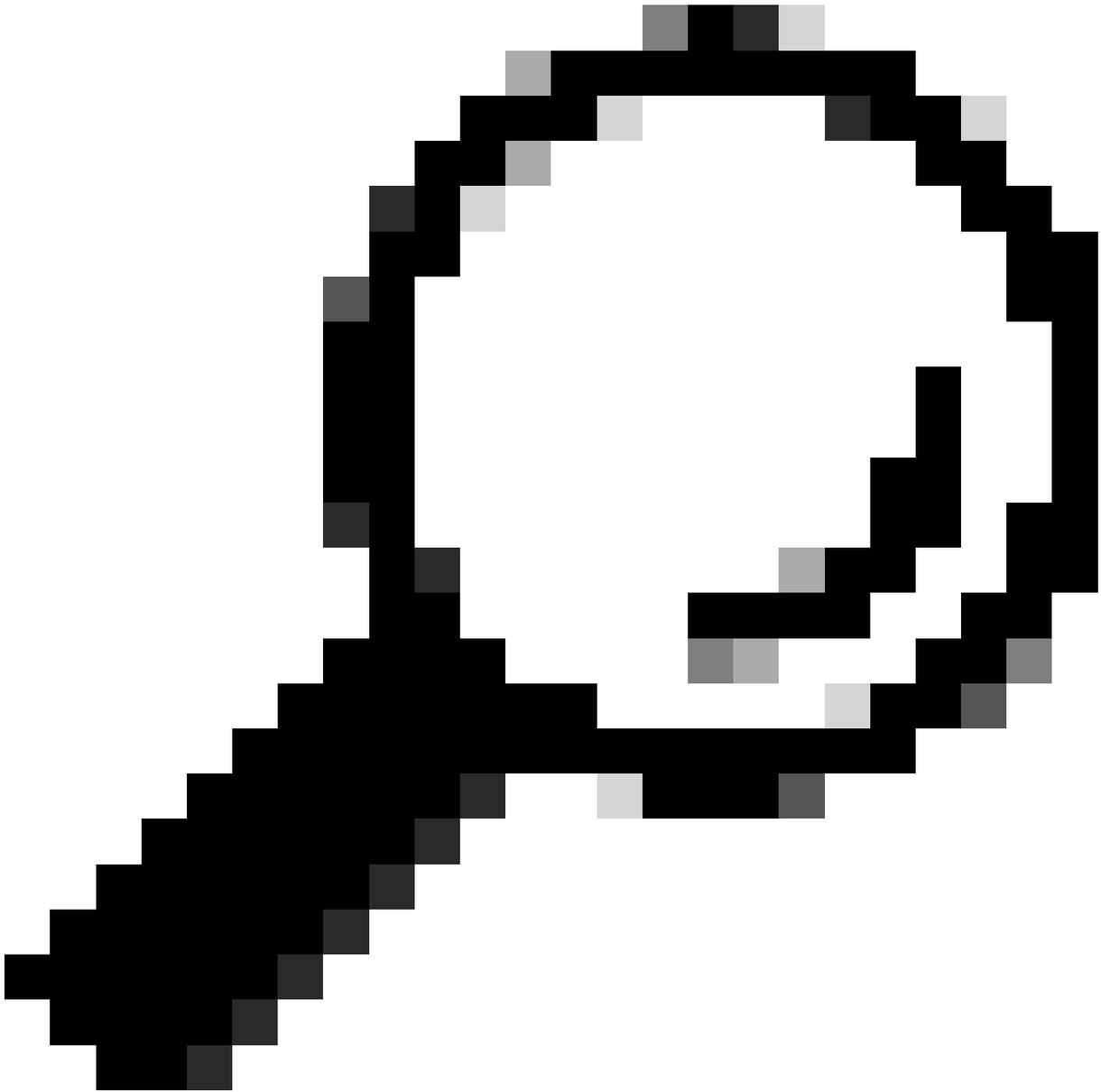
Policy Sets

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

策略保存



提示：在本文中，默认网络访问协议列表是允许的。您可以创建新列表并根据需要缩小范围。

步骤 9 要查看新的策略集，请点击查看列中的 > 图标。展开 Authorization Policy 菜单并单击 + 图标以添加新规则，从而允许对具有管理员权限的用户进行访问。

设置名称。

步骤 9.1 要创建匹配管理员用户组的条件，请点击 + 图标。

添

▼ Authorization Policy (0)

	Status	Rule Name	Conditions
Search			
		SWA Admin	

加授权策略条件

步骤 9.2 设置条件以匹配 Attribute Name Equals User Identity Groups : SWA admin.
Select Identity Group as Condition 的字典身份组

步骤 9.3 向下滚动并选择 User Identity Groups : 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

Scroll Down and Select Identity Group Name

步骤 9.4 单击 Use。



Users

Users

[Add User...](#)

<input type="checkbox"/> 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...](#)

在SWA中启用外部身份验证

第三步：在RADIUS Server Hostname字段中输入ISE的IP地址或FQDN，并输入在步骤2 ISE配置中配置的共同共享密钥。

第四步：在Group Mapping中选择Map external authenticated users to multiple local roles。

步骤 4.1在RADIUS CLASS Attribute字段中输入Administrator并选择Role Administrator。

步骤 4.2在RADIUS CLASS Attribute字段中输入ReadUser并选择角色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:

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服务器的外部身份验证配置

第5步：要在SWA中配置用户，请点击添加用户。输入User Name并选择所需角色所需的User Type。输入Passphrase和Retype Passphrase，如果设备无法连接到任何外部RADIUS服务器，则需要此口令才能进行GUI访问。

注意：如果设备无法连接到任何外部服务器，它会尝试将用户验证为安全Web设备上定义的本地用户。

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中的用户配置

第6步：点击提交并提交更改。

验证

使用配置的用户凭证访问SWA GUI，并检查ISE中的实时日志。要检查ISE中的实时日志，请导航到

操作>实时日志：

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

验证用户登录ISE

相关信息

- [思科安全Web设备AsyncOS 14.0用户指南](#)
- [ISE 3.0管理员指南](#)
- [安全Web设备的ISE兼容性列表](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。