

將SWA第二因素身份驗證配置為ISE作為RADIUS伺服器

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路拓撲](#)

[設定步驟](#)

[ISE 組態](#)

[SWA配置](#)

[驗證](#)

[參考資料](#)

簡介

本文檔介紹如何在將Cisco身份服務引擎作為RADIUS伺服器的安全Web裝置上配置第二因素身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- SWA的基本知識。
- 瞭解ISE上的身份驗證和授權策略配置。
- 基本RADIUS知識。

思科建議您：

- 安全網路裝置(SWA)和思科身份服務引擎(ISE)管理訪問。
- 您的ISE已整合到Active Directory或LDAP。
- Active Directory或LDAP配置為使用者名稱「admin」以驗證SWA預設「admin」帳戶。
- 相容的WSA和ISE版本。

採用元件

本檔案中的資訊是根據以下軟體版本：

- SWA 14.0.2-012
- ISE 3.0.0。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

為SWA上的管理使用者啟用第二因素身份驗證時，裝置在驗證SWA中配置的憑據之後第二次使用RADIUS伺服器驗證使用者憑據。

網路拓撲



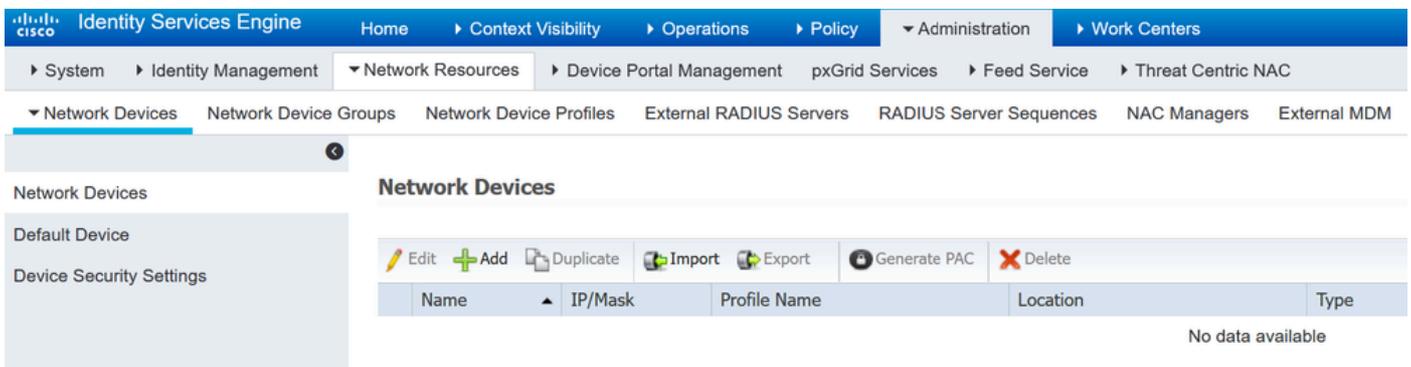
圖-網路拓撲圖

管理使用者使用其憑據訪問埠443上的SWA。SWA使用RADIUS伺服器驗證憑據以進行第二次因子身份驗證。

設定步驟

ISE 組態

步驟 1. 新增網路裝置。導航到管理>網路資源>網路裝置> +增加。



在ISE中增加SWA作為網路裝置

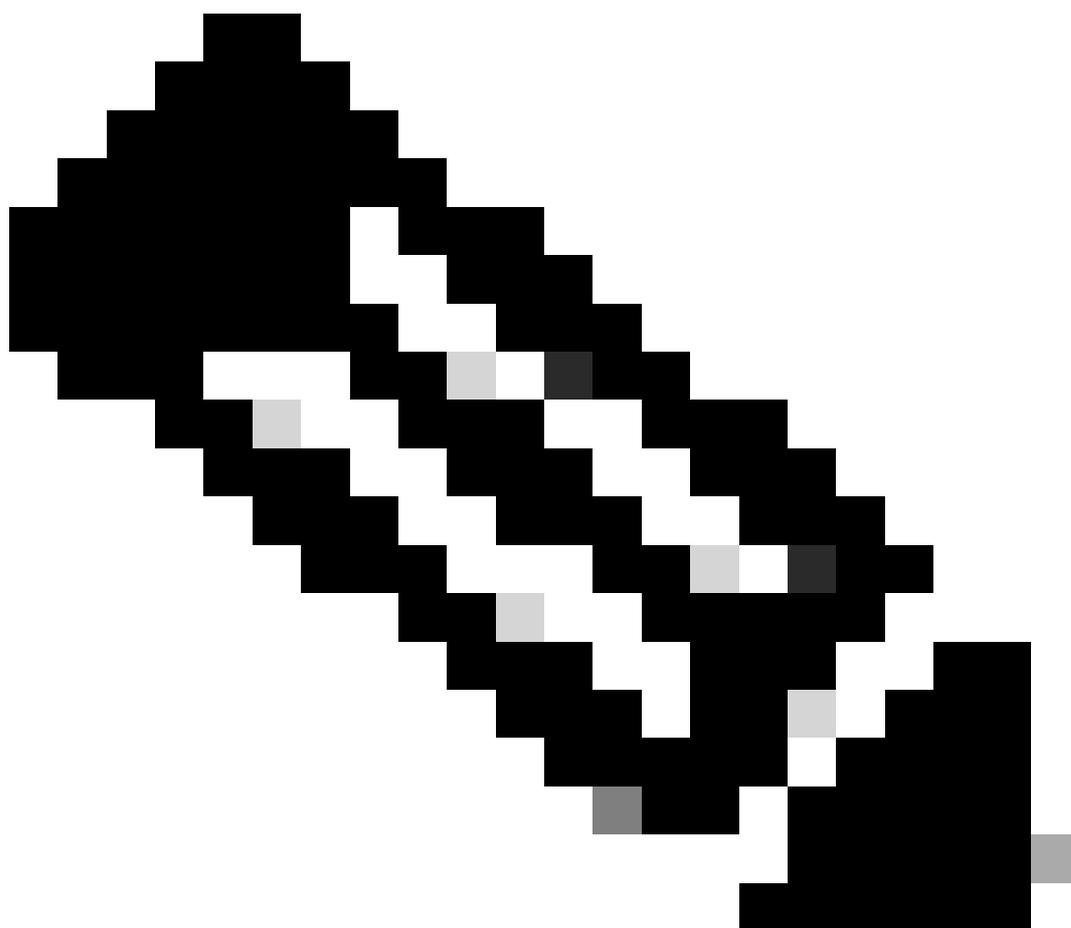
步驟 2. 在ISE中配置網路裝置。

步驟 2.1.為網路裝置對象分配Name。

步驟 2.2.插入SWA IP地址。

步驟 2.3.選中RADIUS覈取方塊。

步驟 2.4.定義共用金鑰。



注意：稍後必須使用相同的金鑰來配置SWA。

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網路裝置共用金鑰

步驟 2.5.按一下Submit。

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

* Shared Secret: [masked] Show

Use Second Shared Secret: Show

CoA Port: 1700 Set To Default

RADIUS DTLS Settings

DTLS Required:

Shared Secret: radius/dtls

CoA Port: 2083 Set To Default

Issuer CA of ISE Certificates for CoA: Select if required (optional)

DNS Name: [empty]

General Settings

Enable KeyWrap:

* Key Encryption Key: [masked] Show

* Message Authenticator Code Key: [masked] Show

Key Input Format: ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

Submit Cancel

提交網路裝置配置

步驟 3. 您需要建立與SWA中配置的使用者名稱匹配的網路訪問使用者。導航到管理>身份管理>身份 > + Add。

Identity Services Engine 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

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address
No data available					

在ISE中增加本地使用者

步驟 3.1. 分配名稱。

步驟 3.2. (選擇性) 輸入使用者的電子郵件地址。

步驟 3.3. 設定密碼。

步驟 3.4. 點選儲存。

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:
 ⓘ

Enable Password:
 ⓘ

在ISE中增加本地使用者

步驟 4. 建立與SWA IP地址匹配的策略集。這是為了防止使用這些使用者憑證訪問其他裝置。
 導航到策略>策略集，點選位於左上角的+圖示。

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中增加策略集

步驟 4.1. 新行將放置在策略集的頂部。輸入新策略的名稱。

步驟 4.2. 為RADIUS NAS-IP-Address屬性增加一個條件以匹配SWA IP地址。

步驟 4.3. 按一下Use以保留更改並退出編輯器。



注意：此示例允許預設網路訪問協定清單。您可以建立一個新清單，並根據需要縮小其範圍。

步驟 5. 要檢視新的策略集，請在檢視列中按一下「>」圖示。

步驟 5.1. 展開 Authorization Policy 選單，然後按一下 + 圖示以增加允許所有已驗證使用者訪問的新規則。

步驟 5.2. 設定名稱。

步驟 5.3. 設定條件以將網路訪問詞典與屬性 AuthenticationStatus Equals AuthenticationPassed 相匹配，然後按一下 Use。

SWA配置

步驟 1. 從SWA GUI導航至系統管理，然後按一下使用者。

步驟 2. 在Second Factor Authentication Settings中，按一下Enable。

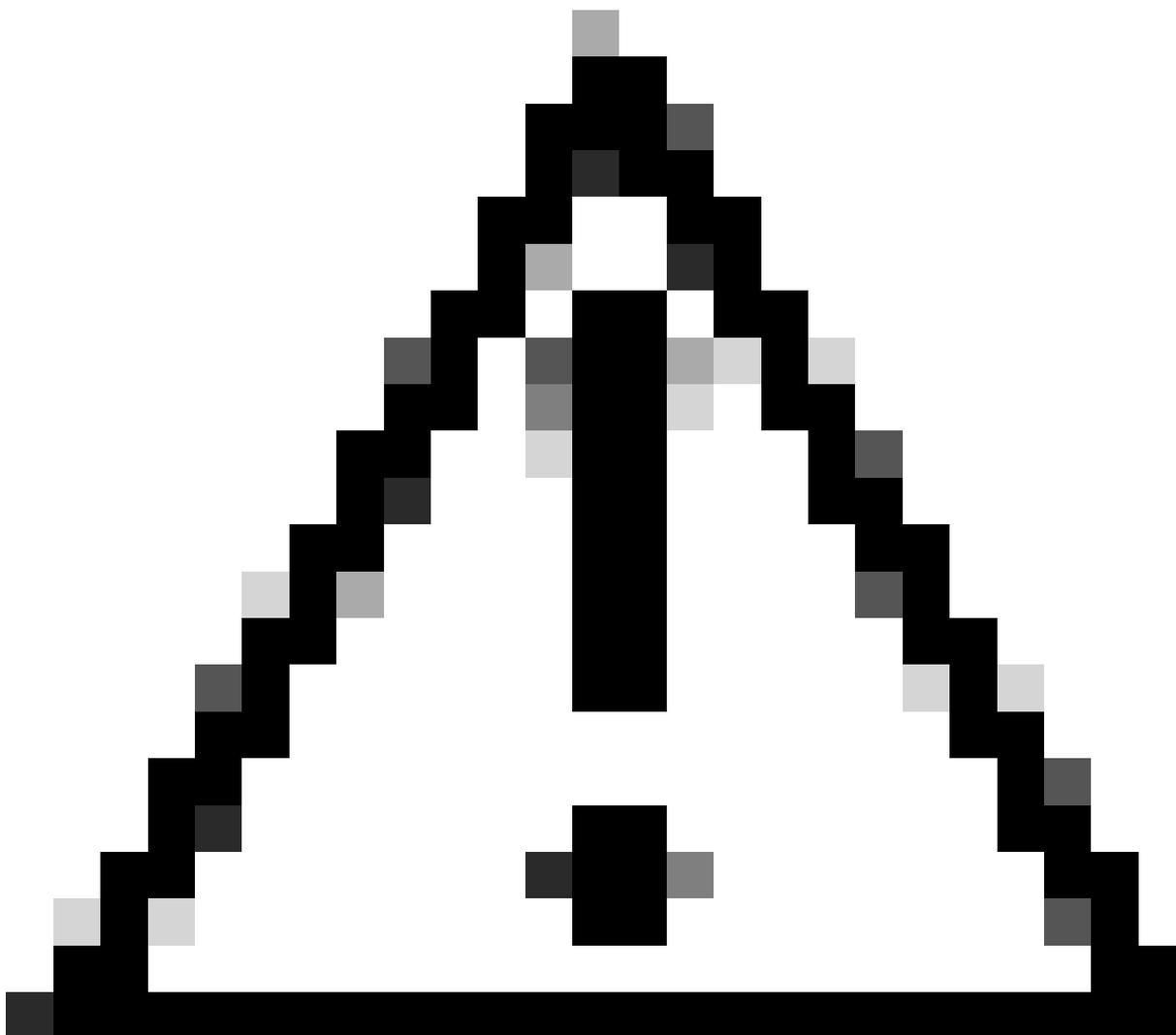
The screenshot displays the Cisco Secure Web Appliance (S100V) GUI. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The main content area is titled 'Users' and contains several sections:

- Users:** A table with columns for 'All Accounts', 'User Name', 'Full Name', 'User Type', 'Account Status', 'Passphrase Expires', and 'Delete'. A single user 'admin' is listed with the role 'Administrator' and status 'Active'. Below the table is an 'Enforce Passphrase Changes' button.
- Local User Account & Passphrase Settings:** A table with settings for 'Account Lock' (Not configured), 'Passphrase Reset' (Not configured), and 'Passphrase Rules' (Require at least 8 characters. Additional rules configured...). An 'Edit Settings...' button is at the bottom right.
- External Authentication:** A section stating 'External Authentication is disabled.' with an 'Enable...' button.
- Second Factor Authentication Settings:** A section stating 'Two Factor Authentication is disabled.' with an 'Enable...' button. A blue arrow points to this button.

在SWA中啟用第二因素身份驗證

步驟 3. 在RADIUS伺服器主機名欄位中輸入ISE的IP地址，並輸入在ISE配置的第2步中配置的共用金鑰。

步驟 4. 選取需要啟用「第二因子」強制的必要預先定義角色。



注意：如果在SWA中啟用第二因素身份驗證，則預設的「admin」帳戶也將在第二因素實施中啟用。您必須將ISE與LDAP或Active Directory (AD)整合以驗證「admin」憑證，因為ISE不允許將「admin」配置為網路訪問使用者。



Users

Users

Add User...

All
 Accounts

User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
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...

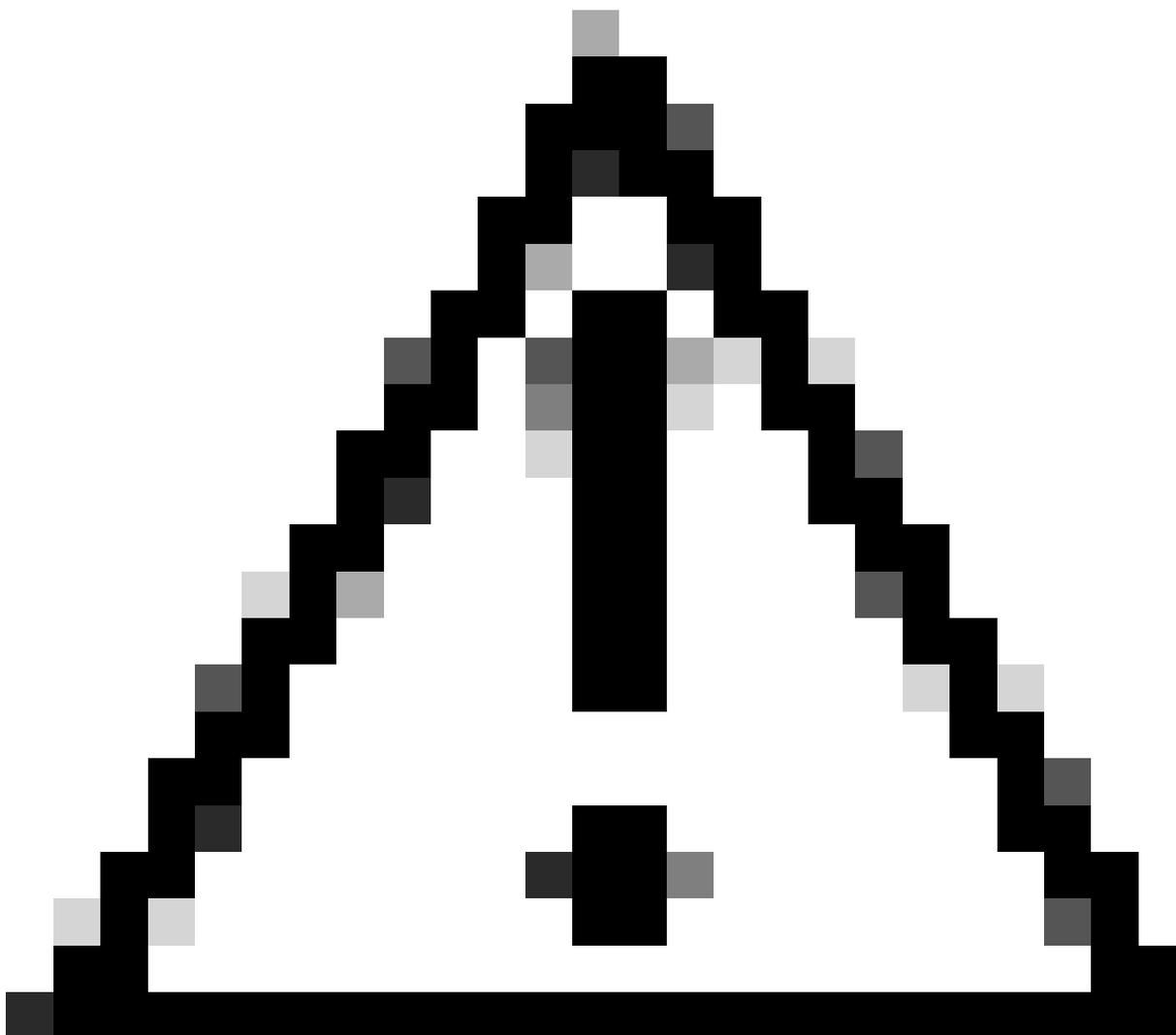
Second Factor Authentication Settings

Two Factor Authentication is disabled.

Enable...



在SWA中啟用第二因素身份驗證



注意：如果在SWA中啟用第二因素身份驗證，則預設的「admin」帳戶也將在第二因素實施中啟用。您必須將ISE與LDAP或Active Directory (AD)整合以驗證「admin」憑證，因為ISE不允許將「admin」配置為網路訪問使用者。

Second Factor Authentication

Second Factor Authentication Settings

Enable Second Factor Authentication

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:	RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	
	10.106.38.150	1812	*****	5	PAP	<input type="button" value="Add Row"/> <input type="button" value="Delete"/>

User Role Privileges

Configure user roles for Second Factor Authentication

Second Factor Authentication is enforced to:

Predefined Roles

- Administrator
- Operator
- Read-Only Operator
- Guest

Two Factor Login Page

Appearance:

Current Logo:

Use Current Logo

Upload Custom Logo from Local Computer: Browse... No file selected.

Company Name:
(Max 150 characters only)

Custom text Information:
(Max 500 characters only)

Login help Information:
(Examples: For login trouble Please contact, Contact Name ,123-1234-123,admin@example.com or help URL. Note:Max 500 characters only)

[View Existing Two Factor Login Page](#)

配置第二因素身份驗證

第5步：要在SWA中配置使用者，請點選增加使用者。輸入使用者名稱並選擇所需角色所需的使用者型別。輸入密碼短語和重新鍵入密碼短語。

Users

	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	adminuser	Admin User	Administrator	Active	n/a	<input type="button" value="Delete"/>
<input type="checkbox"/>	rouser	RO User	Read-Only Operator	Active	n/a	<input type="button" value="Delete"/>

SWA中的使用者配置

第6步：點選提交和提交更改。

驗證

使用配置的使用者憑證訪問SWA GUI。身份驗證成功後，您將被重定向到輔助身份驗證頁面。在這裡，您需要輸入在ISE中配置的輔助身份驗證憑證。



Passcode:

Login

Copyright © 2003-2022 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

驗證第二個因子登入

參考資料

- [Cisco Secure Web Appliance AsyncOS 14.0使用手冊](#)
- [ISE 3.0管理指南](#)
- [安全Web裝置的ISE相容性清單](#)
- [整合AD用於ISE GUI和CLI登入](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。