

在ISE上配置外部TACACS伺服器並對其進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[配置ISE](#)

[配置ACS](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹使用身分識別服務引擎(ISE)作為代理的部署中使用外部TACACS+伺服器的功能。

必要條件

需求

- 基本瞭解ISE上的裝置管理。
- 本文檔基於Identity Service Engine 2.0版，適用於任何高於2.0版本的Identity Service Engine。

採用元件

附註：本文檔中對ACS的任何引用都可以解釋為對任何外部TACACS+伺服器的引用。但是，ACS上的配置和任何其他TACACS伺服器上的配置可能不同。

本文中的資訊係根據以下軟體和硬體版本：

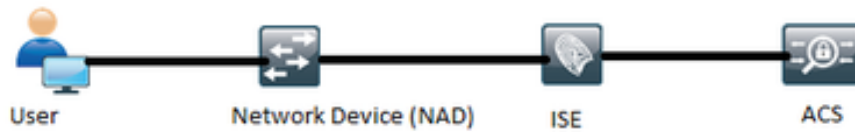
- 身分識別服務引擎2.0
- 存取控制系統(ACS)5.7

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。如果您的網路正在作用，請確保您已瞭解任何組態變更的潛在影響。

設定

本節幫助配置ISE以代理TACACS+請求至ACS。

網路圖表



配置ISE

1. 可在ISE上配置多個外部TACACS伺服器，並可用於驗證使用者。要在ISE上配置外部TACACS+伺服器，請導航至工作中心>裝置管理>網路資源> TACACS外部伺服器。按一下Add並填寫外部伺服器詳細資訊的詳細資訊。

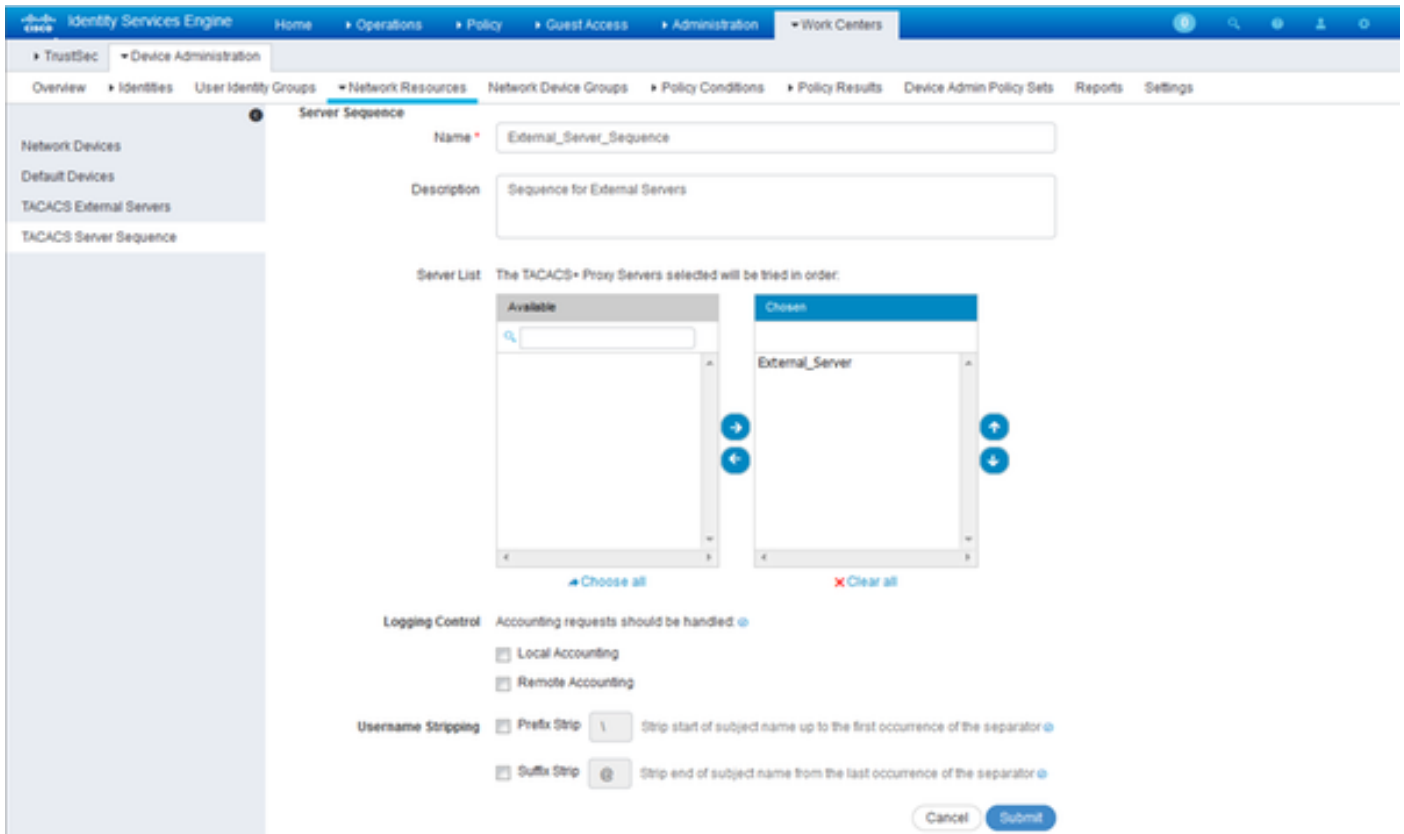
The screenshot shows the ISE configuration interface for TACACS External Servers. The breadcrumb navigation is: Home > Operations > Policy > Guest Access > Administration > Work Centers > TrustSec > Device Administration > Network Resources > TACACS External Servers > External_Server. The form fields are as follows:

Field	Value
Name	External_Server
Description	External TACACS Server
Host IP	10.127.196.237
Connection Port	49 (1-65,535)
Timeout	20 Seconds (1-999)
Shared Secret	***** (with Show Secret button)
Use Single Connect	<input type="checkbox"/>

Buttons: Cancel, Save

本節提供的共用金鑰必須與ACS中使用的共用金鑰相同。

2. 若要使用已配置的外部TACACS伺服器，必須將其新增到TACACS伺服器序列中，以便在策略集中使用。要配置TACACS伺服器序列，請導航至工作中心>裝置管理>網路資源> TACACS伺服器序列。按一下Add，填寫詳細資訊，然後按照該順序選擇需要使用的伺服器。

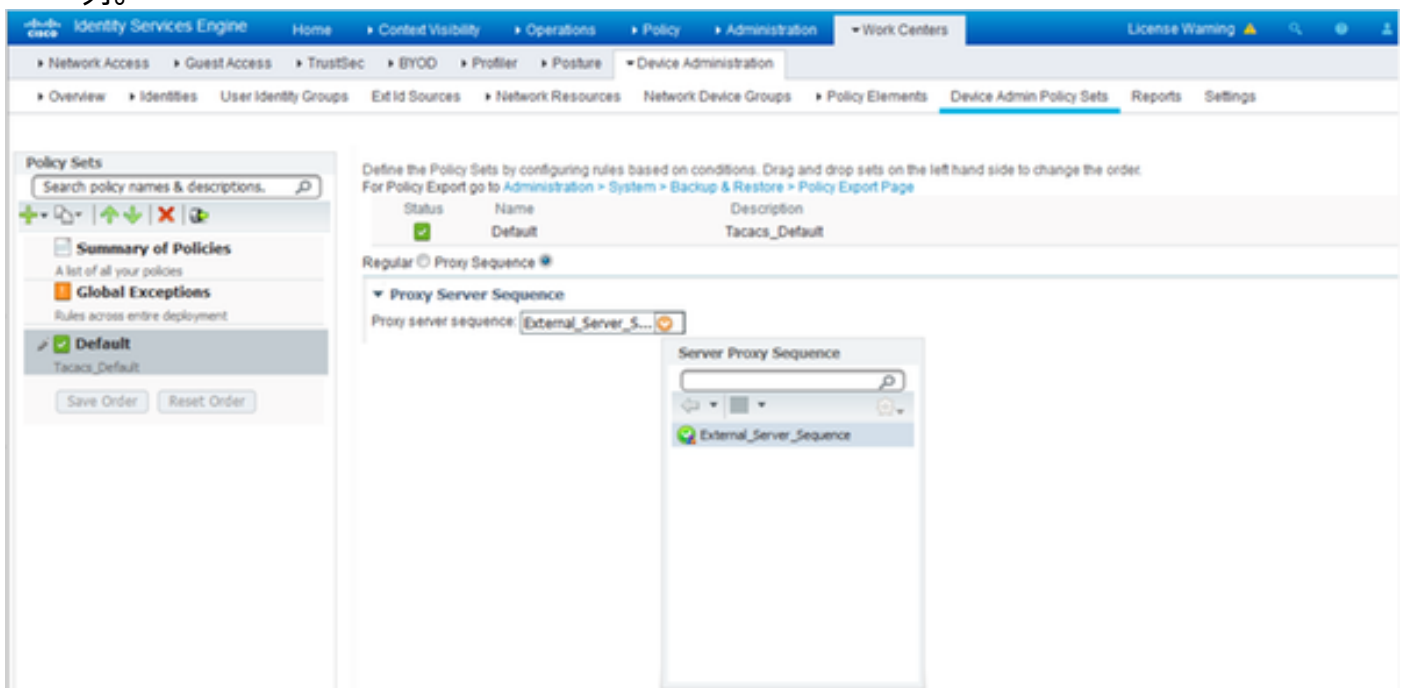


除了伺服器序列外，還提供了另外兩個選項。日誌控制和使用者名稱剝離。

Logging Control提供選項以在本地記錄ISE上的記帳請求或將記帳請求記錄到處理身份驗證的外部伺服器。

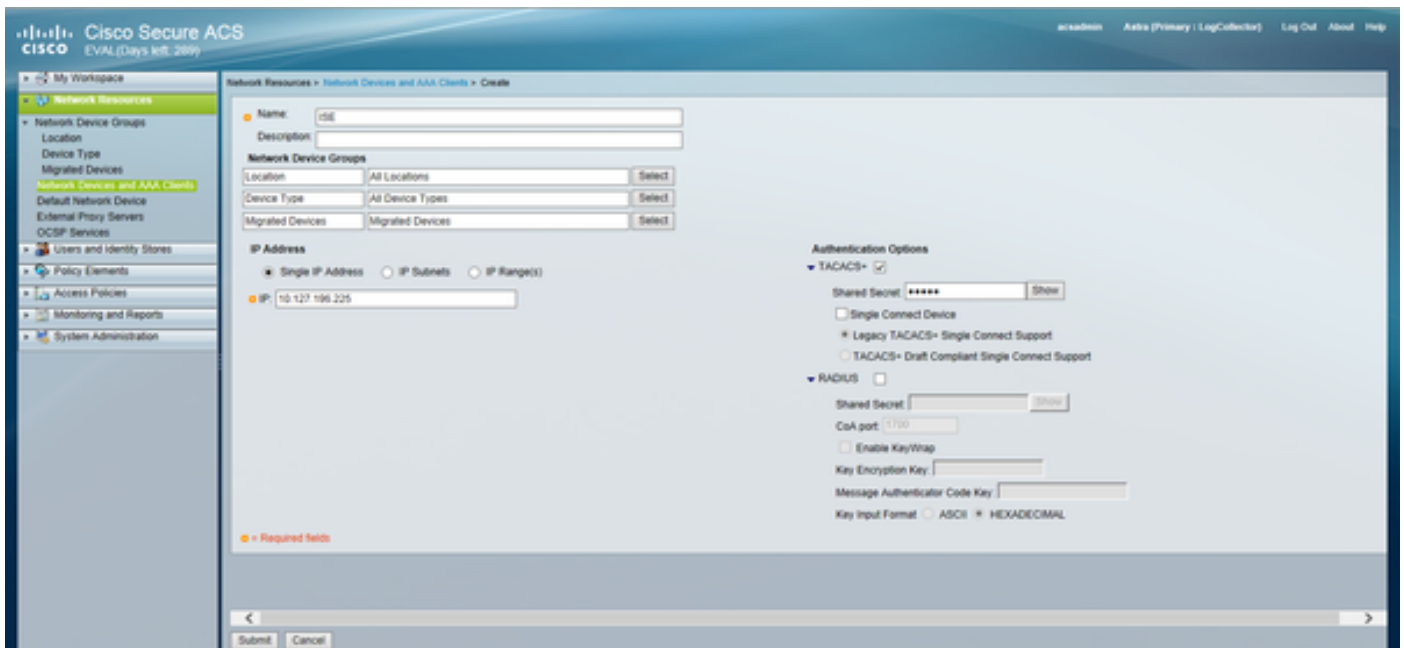
使用者名稱剝離用於在將請求轉發到外部TACACS伺服器之前通過指定分隔符來剝離字首或字尾。

3. 要使用已配置的外部TACACS伺服器序列，必須將策略集配置為使用建立的序列。若要將策略集配置為使用外部伺服器序列，請導航到**Work Centers > Device Administration > Device Admin Policy Sets > [選擇策略集]**。切換單選按鈕，顯示代理序列。選擇建立的外部伺服器序列。



配置ACS

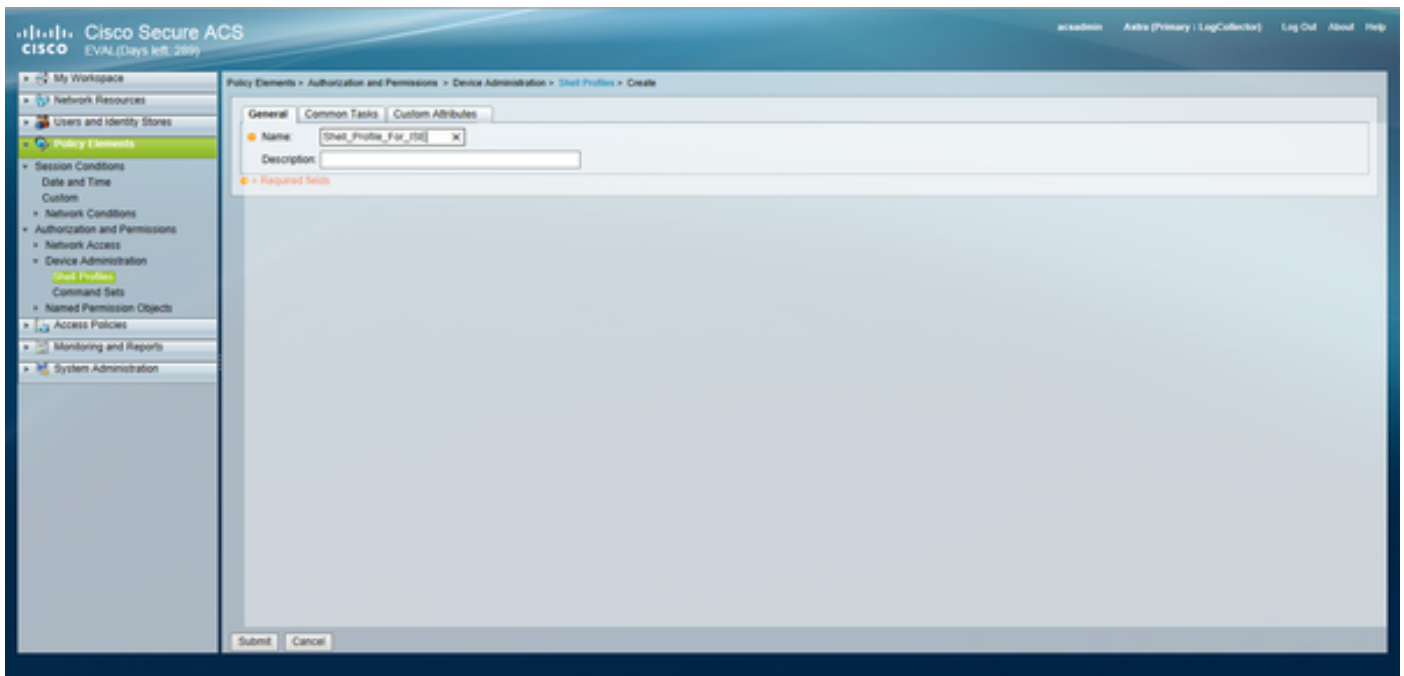
對於ACS，ISE只是要傳送TACACS請求的另一個網路裝置。若要將ISE配置為ACS中的網路裝置，請導航至**Network Resources > Network Devices and AAA Clients**。按一下**Create**並使用ISE上配置的共用金鑰填寫ISE伺服器的詳細資訊。



The screenshot shows the Cisco Secure ACS web interface for configuring a new Network Device Group. The breadcrumb path is "Network Resources > Network Devices and AAA Clients > Create". The form includes the following fields and options:

- Name:** iSE
- Description:** (empty)
- Network Device Groups:**
 - Location:** All Locations (Selected)
 - Device Type:** All Device Types (Selected)
 - Migrated Devices:** Migrated Devices (Selected)
- IP Address:**
 - Single IP Address
 - IP Subnets
 - IP Range(s)
 - IP:** 10.127.196.225
- Authentication Options:**
 - TACACS+
 - Shared Secret:** ***** (Show)
 - Single Connect Device
 - Legacy TACACS+ Single Connect Support
 - TACACS+ Draft Compliant Single Connect Support
 - RADIUS
 - Shared Secret:** (empty) (Show)
 - CoA port:** 1710
 - Enable KeyWrap
 - Key Encryption Key:** (empty)
 - Message Authenticator Code Key:** (empty)
 - Key Input Format:** ASCII HEXADECIMAL


在ACS上配置裝置管理引數，即外殼配置檔案和命令集。要配置Shell配置檔案，請導航到**Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**。根據需要按一下**建立**並配置名稱、常見任務和自定義屬性。




The screenshot shows the Cisco Secure ACS web interface for creating a new Shell Profile. The breadcrumb path is "Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create". The form includes the following fields and options:

- General** | Common Tasks | Custom Attributes
- Name:** Shell_Profile_For_ISE
- Description:** (empty)
- Required fields:** (indicated by a red icon)

若要配置命令集，請導航到**Policy Elements > Authorization and Permissions > Device Administration > Command Sets**。按一下**Create**並根據要求填寫詳細資訊。

General
Name: Status: 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
 Protocol:

Results
Service:

根據要求配置「服務選擇」規則中選擇的「訪問服務」。要配置「訪問服務規則」，請導航到 **Access Policies > Access Services > Default Device Admin > Identity**，可以在其中選擇需要使用身份儲存進行身份驗證。可通過導航到 **Access Policies > Access Services > Default Device Admin > Authorization** 來配置授權規則。

附註： 特定裝置的授權策略和外殼配置可能有所不同，這超出了本文檔的範圍。

驗證

使用本節內容，確認組態是否正常運作。

可以在ISE和ACS上執行驗證。ISE或ACS的配置錯誤將導致身份驗證失敗。ACS是處理身份驗證和授權請求的主伺服器，ISE負責與ACS伺服器之間的通訊，並充當請求的代理。由於資料包在兩個伺服器上都經過，因此可以在兩個伺服器上驗證身份驗證或授權請求。

網路裝置配置為ISE作為TACACS伺服器，而不是ACS。因此，請求首先到達ISE，並根據配置的規則，ISE決定是否需要將該請求轉發到外部伺服器。可以在ISE上的TACACS Live日誌中驗證這一點

。

若要檢視ISE上的即時日誌，請導航至**操作> TACACS >即時日誌**。在此頁面上可檢視即時報告，並可通過按一下與感興趣的特定請求有關的放大鏡圖示來檢查特定請求的詳細資訊。

Steps

- 13020 Get TACACS+ default network device setting
- 13013 Received TACACS+ Authentication START Request
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Network Access.Protocol
- 15006 Matched Default Rule
- 13064 TACACS proxy received incoming request for forwarding.
- 13065 TACACS proxy received valid incoming authentication request.
- 13063 Start forwarding request to remote TACACS server.
- 13074 Finished to process TACACS Proxy request.
- 13020 Get TACACS+ default network device setting
- 13014 Received TACACS+ Authentication CONTINUE Request
- 13064 TACACS proxy received incoming request for forwarding.
- 13065 TACACS proxy received valid incoming authentication request.
- 13071 Continue flow (seq_no > 1).
- 13063 Start forwarding request to remote TACACS server.
- 13074 Finished to process TACACS Proxy request.

若要檢視ACS上的身份驗證報告，請導航到**監視和報告>啟動監視和報告檢視器>監視和報告>報告>AAA協定> TACACS身份驗證**。同樣，通過按一下與感興趣的特定請求有關的放大鏡圖示可以檢查特定請求的詳細資訊

Steps
Message
Received TACACS+ Authentication START Request
Evaluating Service Selection Policy
Matched rule
Selected Access Service - Default Device Admin
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
TACACS+ will use the password prompt from global TACACS+ configuration.
Returned TACACS+ Authentication Reply
Received TACACS+ Authentication CONTINUE Request
Using previously selected Access Service
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
Authentication Passed
Evaluating Group Mapping Policy
Evaluating Exception Authorization Policy
No rule was matched
Evaluating Authorization Policy
Matched Default Rule
Returned TACACS+ Authentication Reply

疑難排解

本節提供的資訊可用於對組態進行疑難排解

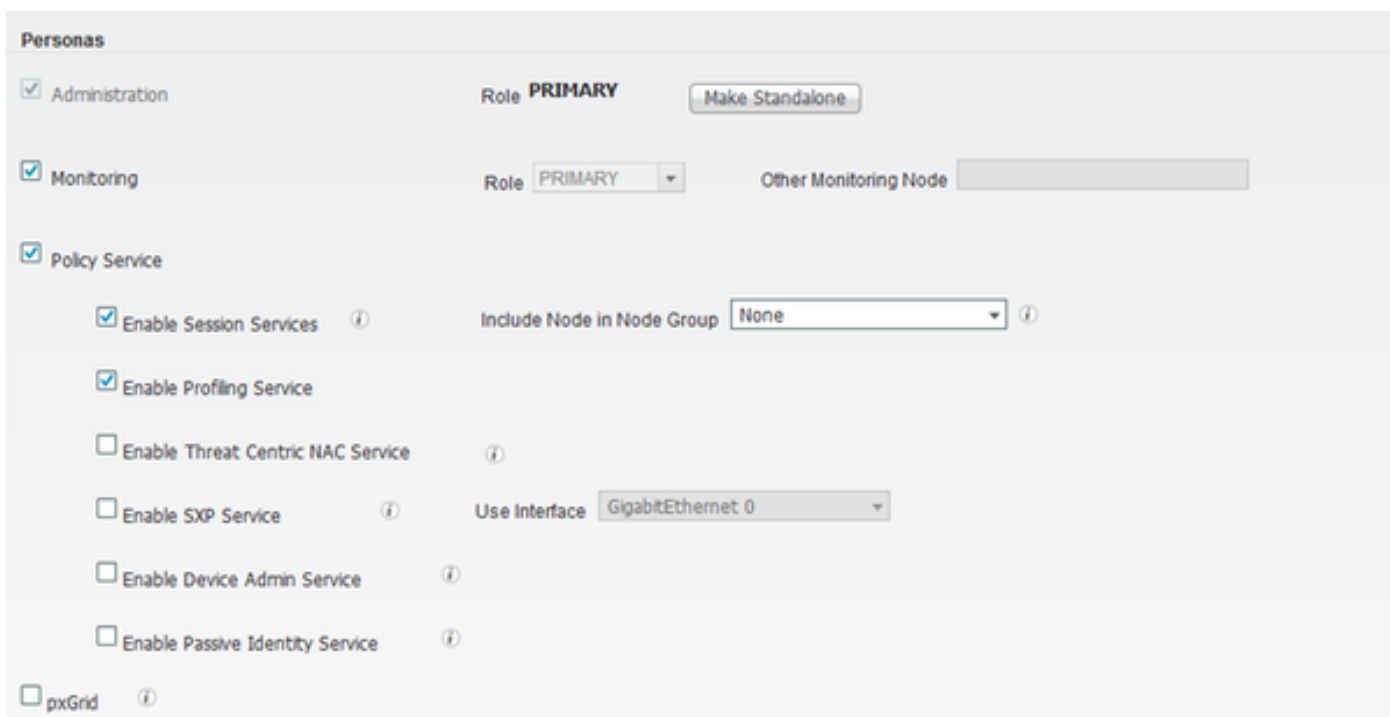
1. 如果ISE上報告的詳細資訊顯示圖中所示的錯誤消息，則表明在ISE或網路裝置(NAD)上配置的共用金鑰無效。

Message Text

TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. 如果在ISE上沒有請求身份驗證報告，但終端使用者拒絕訪問網路裝置，這通常表明存在多種情況。

- 請求本身未到達ISE伺服器。
- 如果在ISE上禁用了裝置管理角色，則對ISE的任何TACACS+請求將以靜默方式丟棄。報告或即時日誌中不會顯示指示相同內容的日誌。要驗證這一點，請導航到**管理>系統>部署> [選擇節點]**。按一下**Edit**，並注意**General Settings**頁籤下的「**Enable Device Admin Service**」覈取方塊，如圖所示。需要選中該覈取方塊才能在ISE上使用裝置管理。



- 如果裝置管理許可證沒有過期，則所有TACACS+請求都會以靜默方式刪除。GUI中未顯示相同內容的日誌。導航到Administration > System > Licensing以檢查裝置管理許可證。

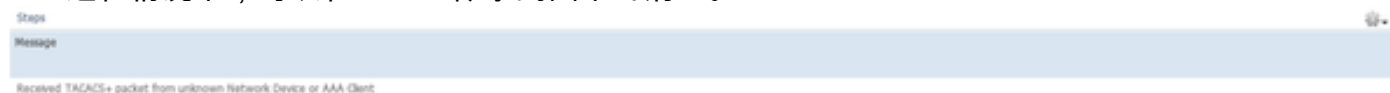
Licenses How do I register, modify or lookup my licenses?

License File	Quantity	Term	Expiration Date
EVALUATION.lic			
Base	100	90 days	22-Jan-2017 (43 days remaining)
Plus	100	90 days	22-Jan-2017 (43 days remaining)
Apex	100	90 days	22-Jan-2017 (43 days remaining)
Wired	100	90 days	22-Jan-2017 (43 days remaining)
Device Admin	Uncounted	90 days	22-Jan-2017 (43 days remaining)

- 如果未配置網路裝置或者在ISE上配置了錯誤的網路裝置IP，則ISE將靜默丟棄資料包。系統不會將任何響應傳送回客戶端，並且在GUI中不會顯示任何日誌。這是與ACS相比，TACACS+的ISE中的行為變化，ACS通知請求來自未知網路裝置或AAA客戶端。
- 請求到達ACS，但響應未返回到ISE。如圖所示，可以從ACS上的報告檢查此情況。這通常是因為為ISE配置的ACS或為ACS配置的ISE上的共用金鑰無效。




- 即使ISE未配置或ISE管理介面的IP地址未配置在網路裝置配置中的ACS，也不會傳送響應。在這種情況下，可以在ACS上觀察到圖中的消息。



- 如果在ACS上看到成功的身份驗證報告，但在ISE上看不到報告，並且使用者被拒絕，則很可能是網路中的問題。這可以通過使用必要過濾器的ISE上的資料包捕獲來驗證。要在ISE上收集資料包捕獲，請導航到操作>故障排除>診斷工具>常規工具> TCP轉儲。

TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status  Stopped

Host Name

Network Interface

Promiscuous Mode On Off

Filter

Example: 'ip host helios and not iceberg'

Format

Dump File Last created on Fri Dec 09 20:51:18 IST 2016
File size: 9,606 bytes
Format: Raw Packet Data
Host Name: tornado
Network Interface: GigabitEthernet 0
Promiscuous Mode: On

- 3.如果可在ISE上檢視報告，但無法在ACS上檢視，則可能表示由於ISE上的策略集配置錯誤（可以根據ISE上的詳細報告進行故障排除），或者由於網路問題（可以通過ACS上的資料包捕獲進行識別）導致請求無法到達ACS。
- 4.如果在ISE和ACS上均看到報告，但使用者仍被拒絕訪問，則在ACS上的訪問策略配置中通常是一個問題，可以根據ACS的詳細報告進行故障排除。此外，必須允許從ISE返回網路裝置的流量。