使用ISE配置EAP-TLS身份驗證

目錄

簡介

本文檔介紹使用Cisco ISE引入可擴展身份驗證協定 — 傳輸層安全身份驗證的初始配置。

必要條件

需求

思科建議您瞭解以下主題：

- 對EAP和RADIUS通訊流有基礎認識。
- 根據通訊流程，具備基本RADIUS驗證知識和基於憑證的驗證方法。
- 瞭解Dot1x和MAC驗證略過(MAB)之間的差異。

- 對公開金鑰基礎架構(PKI)有基礎認識。
- 瞭解如何從證書頒發機構(CA)獲取簽名證書並管理終端上的證書。
- 在網路設備（有線或無線）上配置與身份驗證、授權和記帳(AAA)(RADIUS)相關的設定。
- 請求方配置（在端點上）以與RADIUS/802.1x一起使用。

採用元件

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(ISE)版本3.x。
- CA — 核發憑證(可以是企業CA、第三方/公共CA，或是使用憑證布建入口)。
- Active Directory（外部身份源） — 來自Windows Server;與ISE相容。
- 網路存取裝置(NAD) — 可以是針對802.1x/AAA設定的交換器（有線）或無線LAN控制器(WLC)（無線）。
- 終端 — 向（使用者）身份和請求方配置頒發的證書，可以通過RADIUS/802.1x進行網路訪問身份驗證：使用者身份驗證。可以獲取電腦證書，但本示例中未使用該證書。

注意：由於本指南使用ISE版本3.1，因此所有文檔參考均基於此版本。但是，在早期版本的Cisco ISE上完全可以完全支援相同/類似的配置。

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

主要重點是ISE配置，該配置可應用於多個場景，例如（但不限於）通過有線或無線連線的IP電話/終端進行身份驗證。

在本指南的範圍內，瞭解ISE(RADIUS)身份驗證流的這些階段非常重要：

- 身份驗證 — 識別並驗證請求網路訪問的終端身份（電腦、使用者等）。
- Authorization — 確定終端身份可以在網路上授予哪些許可權/訪問許可權。
- 記帳 — 實現網路訪問後，報告和跟蹤終端身份的網路活動。

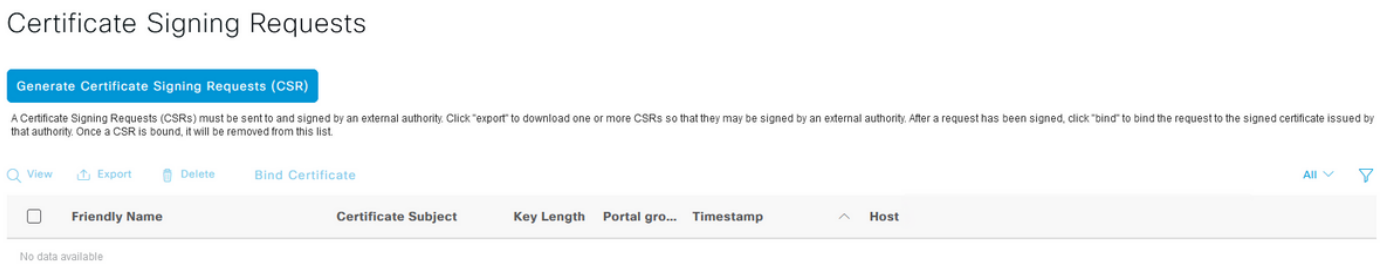
設定

獲取伺服器和客戶端證書

步驟 1.從ISE生成證書簽名請求

第一步是從ISE生成證書簽名請求(CSR)並將其提交到CA（伺服器），以便獲取頒發給ISE的已簽名的證書作為系統證書。在可擴展身份驗證協定 — 傳輸層安全身份驗證(EAP-TLS)身份驗證期間，ISE可以將此證書顯示為伺服器證書。這在ISE UI中執行。導航至 **Administration > System: Certificates > Certificate Management > Certificate Signing Requests.**在 **Certificate Signing Requests**，按一下 **Generate Certificate Signing**

Requests (CSR) 如下圖所示。



證書型別要求使用不同的擴展金鑰。此清單概述了每種證書型別需要使用的擴展金鑰：

ISE身份證書

- 多用途(Admin、EAP、Portal、pxGrid) — 客戶端和伺服器身份驗證
- Admin — 伺服器身份驗證
- EAP身份驗證 — 伺服器身份驗證
- 資料包傳輸層安全(DTLS)身份驗證 — 伺服器身份驗證
- 門戶 — 伺服器身份驗證
- pxGrid — 客戶端和伺服器身份驗證
- 安全斷言標籤語言(SAML)- SAML簽名證書
- ISE消息服務 — 生成簽名證書或生成全新的消息證書

預設情況下，ISE消息服務系統證書用於部署、節點註冊和其他節點間通訊中的每個ISE節點之間的資料複製，並且由ISE內部證書頒發機構(CA)伺服器（ISE內部）提供和頒發。無需對此證書執行任何操作。

管理員系統證書用於標識每個ISE節點，例如何時使用與管理員UI（管理）關聯的API，以及某些節點間通訊。為了首次設定ISE，請設定管理員系統證書。此操作與本配置指南沒有直接關係。

為了通過EAP-TLS（基於證書的身份驗證）執行IEEE 802.1x，請對EAP身份驗證系統證書執行操作，因為該證書在EAP-TLS流期間用作提供給終端/客戶端的伺服器證書；結果在TLS隧道內受到保護。要開始使用，請建立一個CSR以建立EAP身份驗證系統證書，並將其提供給貴組織（或公共CA提供商）中管理CA伺服器的人員，以便進行簽名。最終結果是繫結到CSR並通過這些步驟關聯到ISE的CA簽名證書。

在「憑證簽署請求(CSR)」表單上，選擇以下選項，以完成CSR並取得其內容：

- Certificate Usage，對於此配置示例，選擇 **EAP Authentication**.
- 如果您計畫在證書中使用萬用字元語句， ***.example.com** ，那麼您還必須檢查 **Allow Wildcard Certificate** 覈取方塊。最佳位置是主題備用名稱(SAN)證書欄位，用於任何用途以及環境中可能存在的多個不同型別終端作業系統的相容性。
- 如果您沒有選擇在證書中放置萬用字元語句，請選擇您要將CA簽名證書關聯到的ISE節點（簽名後）。

> 註：將包含萬用字元語句的CA簽名證書繫結到CSR中的多個節點時，證書將分發到ISE部署中的每個ISE節點（或到所選節點），服務可以重新啟動。但是，每次服務重新啟動會自動限製為一個節點。通過 **show application status ise** ISE CLI命令。

接下來，需要完成該表單以定義主題。這包括公用名(CN)、組織單位(OU)、組織(O)、城市(L)、州(ST)和國家(C)證書欄位。$FQDN$variable是表示與每個ISE節點關聯的管理完全限定域名（主機名+域名）的值。

- 其 Subject Alternative Name (SAN) 欄位也必須填寫，以便包括建立信任所需的任何資訊。作為要求，您需要在證書簽名後定義指向與此證書關聯的ISE節點的FQDN的DNS條目。

- 最後，確保定義符合CA伺服器功能和良好安全實踐的適當金鑰型別、金鑰長度和摘要進行簽名。預設值為：RSA、4096位和SHA-384。可用的選擇和相容性會顯示在此頁面的ISE管理員UI中。

以下是未使用萬用字元語句的已完成CSR表單的示例。確保使用特定於環境的實際值：

Usage

Certificate(s) will be used for: EAP Authentication

Allow Wildcard Certificates: ☐

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise	ise#EAP Authentication
☑ ise2	ise2#EAP Authentication
☑ ise3	ise3#EAP Authentication

Subject

Common Name (CN)
$FQDN$

Organizational Unit (OU)

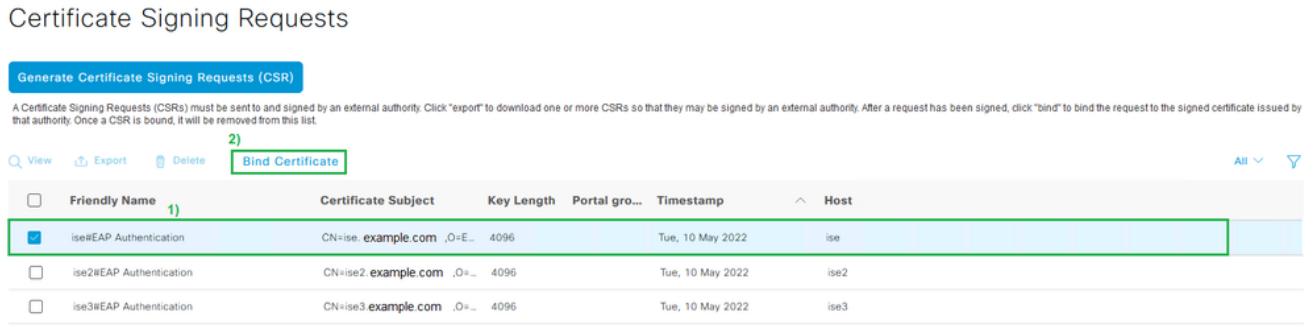
Organization (O)
Example Company

City (L)
San Jose

State (ST)
California

Country (C)
US

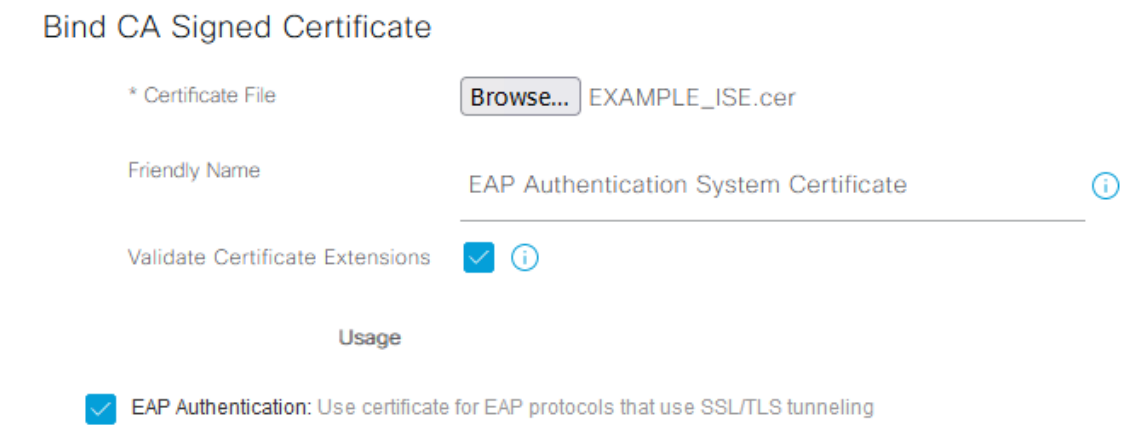
3. 所有證書作為完整CA鏈的一部分匯入到ISE中的受信任證書儲存後，返回到ISE GUI並導航到 **Administration > System: Certificates > Certificate Management: Certificate Signing Requests.**在Friendly Name下找到與已簽名的證書對應的CSR條目，按一下證書的覈取方塊，然後按一下 **Bind Certificate.**



將證書繫結到CSR

註：您需要將單個CA簽名的證書繫結到每個CSR，一次一個。對為部署中的其他ISE節點建立的所有剩餘的CSR重複此操作。

在下一頁上，按一下 **Browse** 並選擇已簽名的證書檔案，定義所需的友好名稱，然後選擇Certificate Usage。提交以儲存更改。



選擇要繫結到CSR的證書

4. 此時，已簽名的證書將移動到ISE GUI。導航至 **Administration > System: Certificates > Certificate Management: System Certificates** 並分配到為其建立CSR的同一節點。對其他節點和/或其他證書使用重複相同的過程。

步驟 3.獲取終結點的客戶端證書

建立與EAP-TLS一起使用的客戶端證書時，需要在終端上瀏覽類似的過程。在本示例中，您需要一個簽名並頒發給使用者帳戶的客戶端證書才能使用ISE執行使用者身份驗證。有關如何從Active Directory環境獲取終端客戶端證書的示例，請參閱：瞭解和配置使用WLC和ISE的EAP-TLS >配置 >EAP-TLS的客戶端。

由於終端和作業系統的型別較多，流程可能稍有不同，因此未提供其他示例。然而，整個過程在概念上是相同的。產生CSR，該CSR具有要包括在憑證中的所有相關資訊，且已由CA簽署，無論是環境中的內部伺服器或是提供此型別服務的公共/第三方公司。

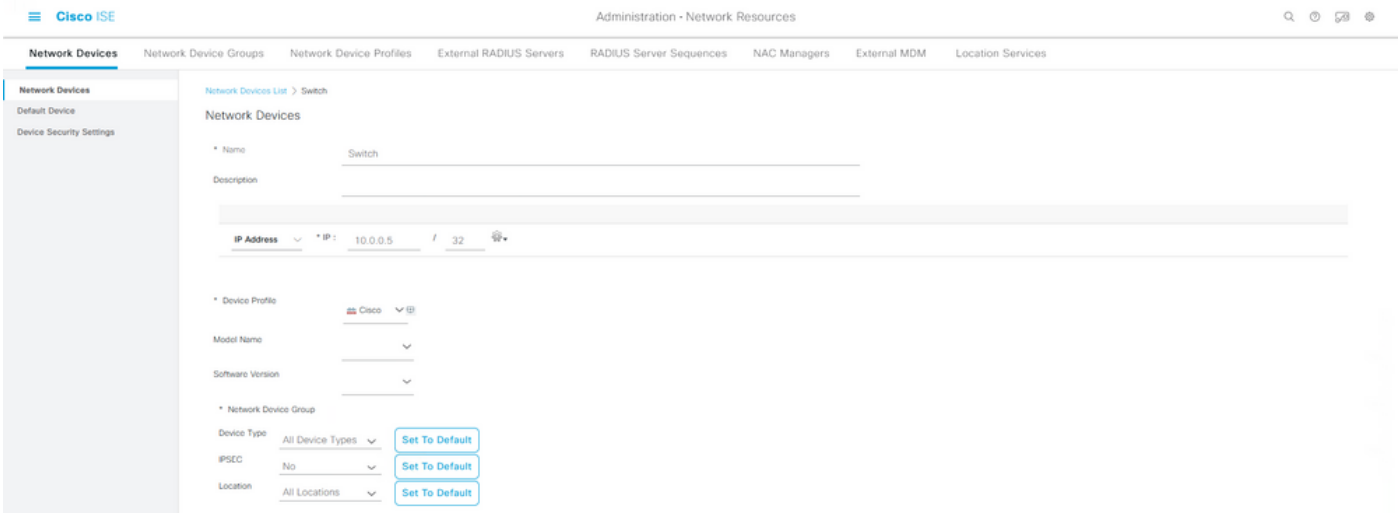
此外，公用名(CN)和主體備用名(SAN)證書欄位包含在身份驗證流程中使用的標識。這也指示請求方在身份方面如何為EAP-TLS配置：電腦和/或使用者身份驗證、電腦身份驗證或使用者身份驗證。本示例在本文檔的其餘部分中僅使用使用者身份驗證。

網路裝置

步驟 4.在ISE中新增網路接入裝置

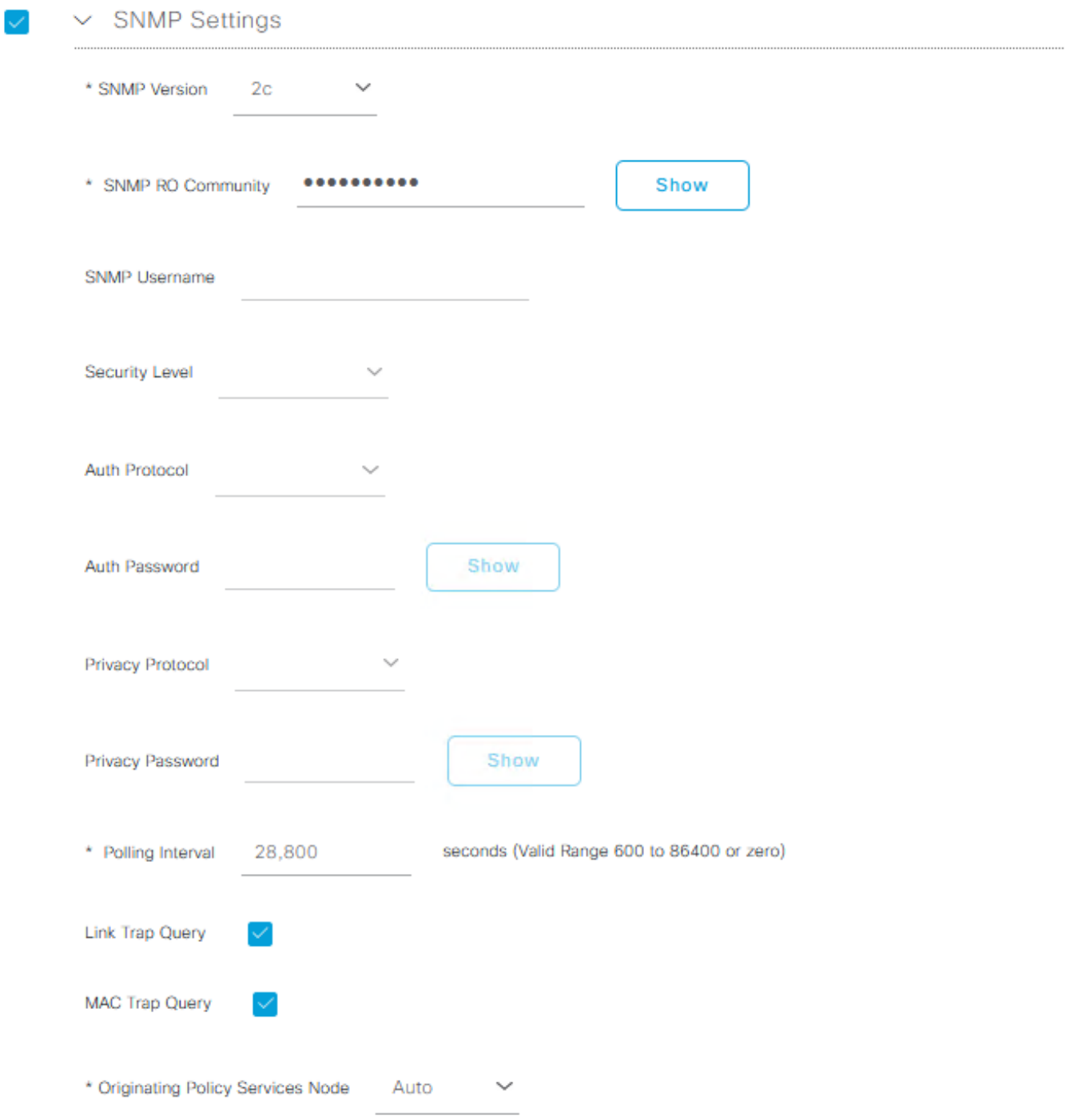
終端連線的網路接入裝置(NAD)也在ISE中配置，以便可以進行RADIUS/TACACS+（裝置管理）通訊。在NAD和ISE之間，共用金鑰/密碼用於信任目的。

要通過ISE GUI新增NAD，請導航至 **Administration > Network Resources: Network Devices > Network Devices** 然後按一下 **Add**中，如下圖所示。



網路裝置示例配置

為了與ISE分析一起使用，您還需要配置SNMPv2c或SNMPv3（更安全），以允許ISE策略服務節點(PSN)通過SNMP查詢與NAD聯絡，該SNMP查詢與向ISE驗證終端相關，以便收集屬性以對使用的終端型別做出準確決策。下一個示例顯示如何從與上一個示例相同的頁面設定SNMP(v2c):



SNMPv2c配置示例

有關詳細資訊，請參閱《思科身份服務引擎管理員指南，版本3.1 > Chapter: Secure Access > Defining Network Devices in Cisco ISE》。

此時，如果您尚未這樣做，您需要在NAD上配置所有與AAA相關的設定，以便通過Cisco ISE進行身份驗證和授權。

策略元素

這些設定是最終繫結到身份驗證策略或授權策略的元素。在本指南中，首先構建每個策略元素，然後將其對映到身份驗證策略或授權策略。在成功完成身份驗證/授權策略的繫結之前，策略不會生效，瞭解這一點很重要。

步驟 5.使用外部身份源

外部身份源只是終端身份（電腦或使用者）帳戶駐留的源，在ISE身份驗證階段使用。Active Directory通常用於支援針對電腦帳戶的電腦身份驗證和/或Active Directory中針對終端使用者帳戶的使用者身份驗證。內部端點（內部）源不儲存電腦帳戶/主機名，因此，它不能用於電腦身份驗證。

此處顯示的是支援ISE的身份源以及可用於每個身份源的協定（身份驗證型別）：

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA
EAP-GTC, PAP (plain text password)	Yes	Yes	Yes	Yes
MS-CHAP password hash: MSCHAPv1/v2 EAP-MSCHAPv2 (as inner method of PEAP, EAP-FAST, or EAP-TTLS) LEAP	Yes	Yes	No	No
EAP-MD5 CHAP	Yes	No	No	No
EAP-TLS PEAP-TLS (certificate retrieval) **Note** For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required but can optionally be added for authorization policy conditions.	No	Yes	Yes	No

身份庫功能

有關策略元素的更多資訊，請參閱Cisco Identity Services Engine管理員指南，版本3.1 >章節：分段>策略集。

將Active Directory安全組新增到ISE

要在ISE策略中使用Active Directory安全組，必須首先將該組新增到Active Directory加入點。在ISE GUI中選擇 **Administration > Identity Management: Active Directory > {select AD instance name / join point} > tab: Groups > Add > Select Groups From Directory.**

有關將ISE 3.x與Active Directory整合的更多資訊和要求，請完整檢視此文檔：Active Directory與Cisco ISE 2.x的整合。

注意：相同的操作適用於將安全組新增到LDAP例項。在ISE GUI中選擇 **Administration > Identity Management: External Identity Sources > LDAP > *LDAP instance name* > tab: Groups > Add > Select Groups From Directory.**

步驟 6.建立證書身份驗證配置檔案

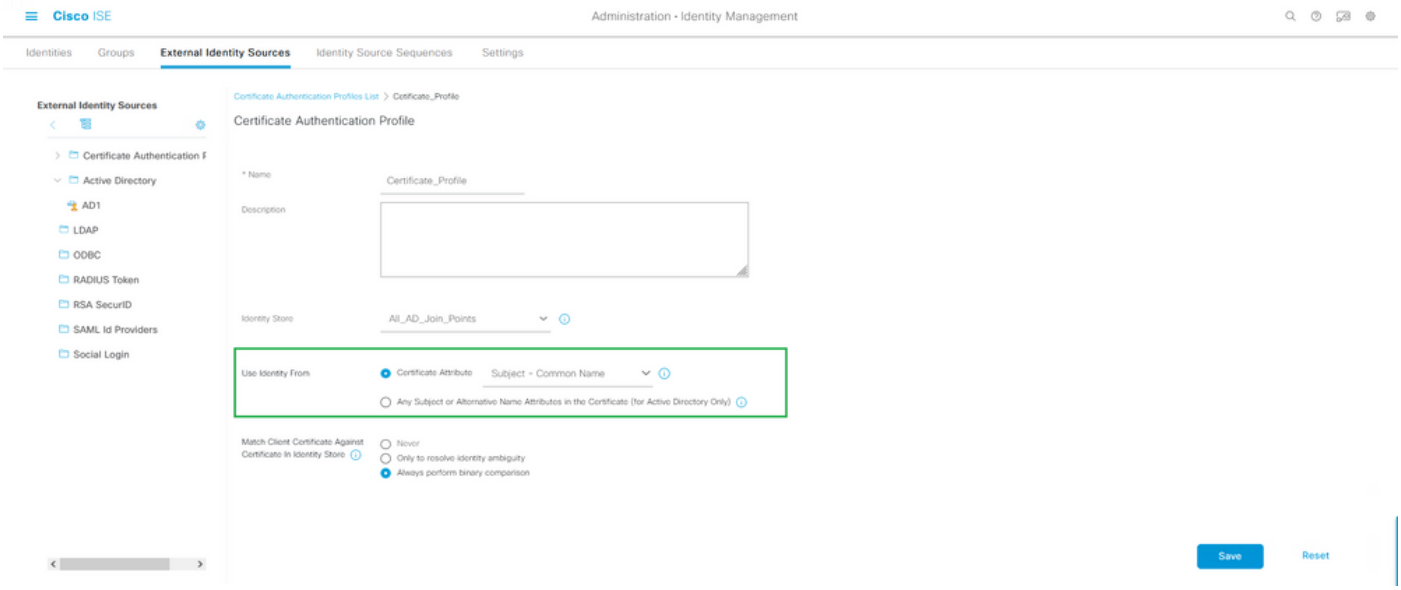
證書身份驗證配置檔案的目的是通知ISE在EAP-TLS期間（也是在其他基於證書的身份驗證方法期間）在向ISE提供的客戶端證書（終端身份證書）上可以找到身份（電腦或使用者）的證書欄位。這些設定繫結到身份驗證策略以驗證身份。從ISE GUI導航至 **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** 然後按一下 **Add.**

使用身份自(Use Identity From)用於選擇證書屬性，從中可以找到身份的特定欄位。選項包括：

> Subject - Common Name
> Subject Alternative Name
> Subject - Serial Number
> Subject
> Subject Alternative Name - Other Name
> Subject Alternative Name - EMail
> Subject Alternative Name - DNS

如果要將身份儲存指向Active Directory或LDAP（外部身份源），則可以使用Binary Comparison功能。二進位制比較執行從Use Identity From選擇從客戶端證書獲取的Active Directory中的身份查詢，在ISE身份驗證階段執行。如果不進行二進位制比較，則只需從客戶端證書獲取身份資訊，在將Active Directory外部組用作條件或需要在外部對ISE執行的任何其他條件時，在ISE授權階段之前，不會在Active Directory中查詢身份。若要使用二進位制比較，請在身份庫中選擇可找到終端身份帳戶的外部身份源（Active Directory或LDAP）。

以下是身份位於使用者端憑證的「公用名(CN)」欄位中，且啟用二進位比較時的組態範例（可選）：



證書身份驗證配置檔案

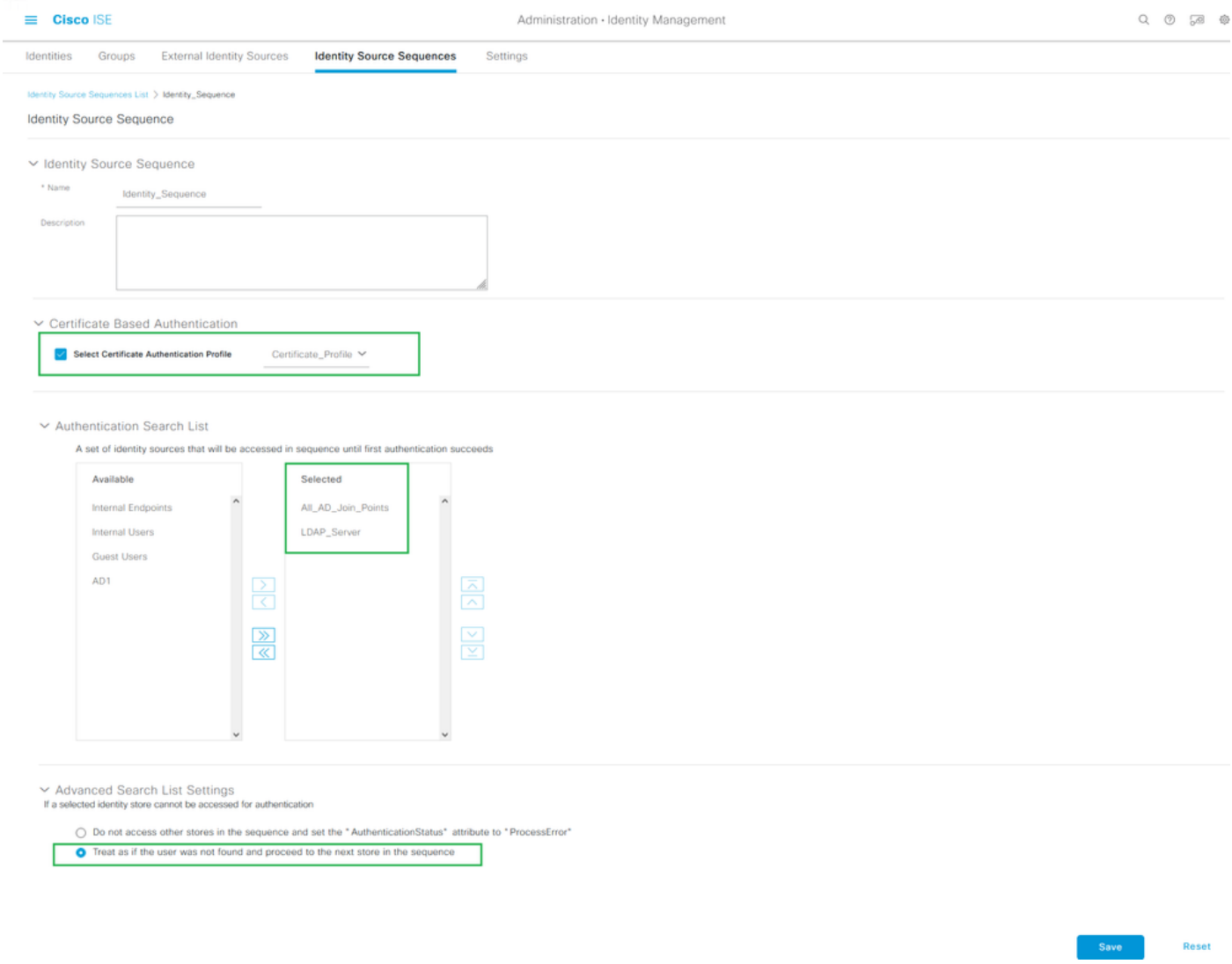
有關詳細資訊，請參閱《思科身份服務引擎管理員指南，版本3.1 >章節：基本設定>思科ISE CA服務>配置思科ISE使用證書驗證個人裝置>建立基於TLS的驗證的證書驗證配置檔案。

步驟 7.新增到身份源序列

可以從ISE GUI建立身份源序列。導航至 **Administration > Identity Management**.在 **Identity Source Sequences** ，按一下 **Add.**

下一步是將證書身份驗證配置檔案新增到身份源序列，該序列可根據需要將多個Active Directory加入點或組合內部/外部身份源的組合包含在一起，然後繫結到 **Use** 列。

此處顯示的示例允許首先對Active Directory執行查詢，如果找不到該使用者，則隨後該使用者在LDAP伺服器上查詢。對於多個身份源。請始終確保 **Treat as if the user was not found and proceed to the next store in the sequence** 覈取方塊。這樣，在身份驗證請求期間會檢查每個身份源/伺服器。



身份源序列

否則，您也可以只將證書身份驗證配置檔案繫結到身份驗證策略。

步驟 8.定義允許的協定服務

Allowed Protocols Service僅啟用ISE在RADIUS身份驗證期間支援的身份驗證方法/協定。若要從ISE GUI進行配置，請導航到Policy > Policy Elements: Results > Authentication > Allowed Protocols，然後作為元素繫結到身份驗證策略。

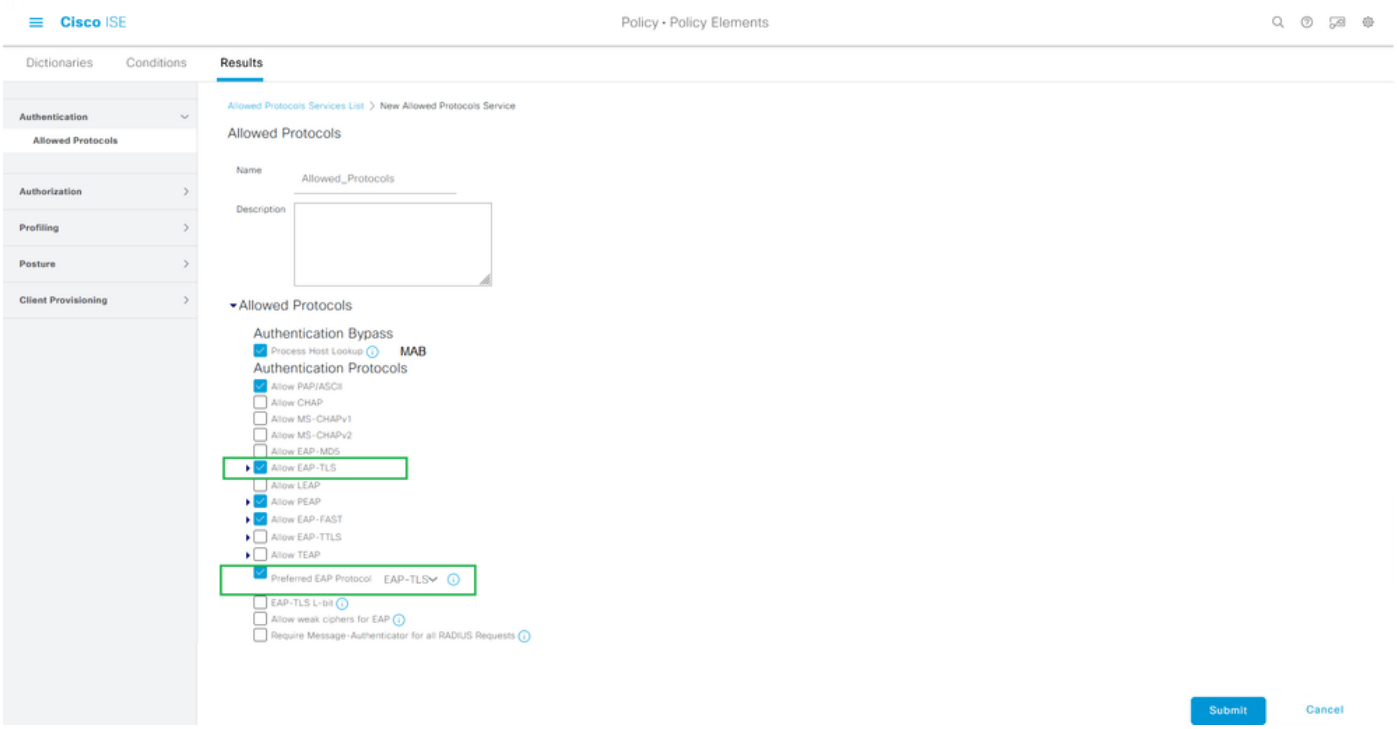
註:Authentication Bypass > Process Host Lookup與ISE上啟用的MAB相關。

這些設定必須與請求方（終端上）支援和配置的設定相同。否則，驗證通訊協定不會按預期方式交涉，RADIUS通訊可能失敗。在實際的ISE配置中，建議啟用環境中使用的任何身份驗證協定，以便ISE和請求方可以按預期協商和身份驗證。

以下是建立允許協定服務的新例項時的預設值（摺疊）。

注意：在此配置示例中，至少必須啟用EAP-TLS，因為ISE和我們的請求方通過EAP-TLS進行

身份驗證。



允許ISE在終端請求方的身份驗證請求期間使用的協定

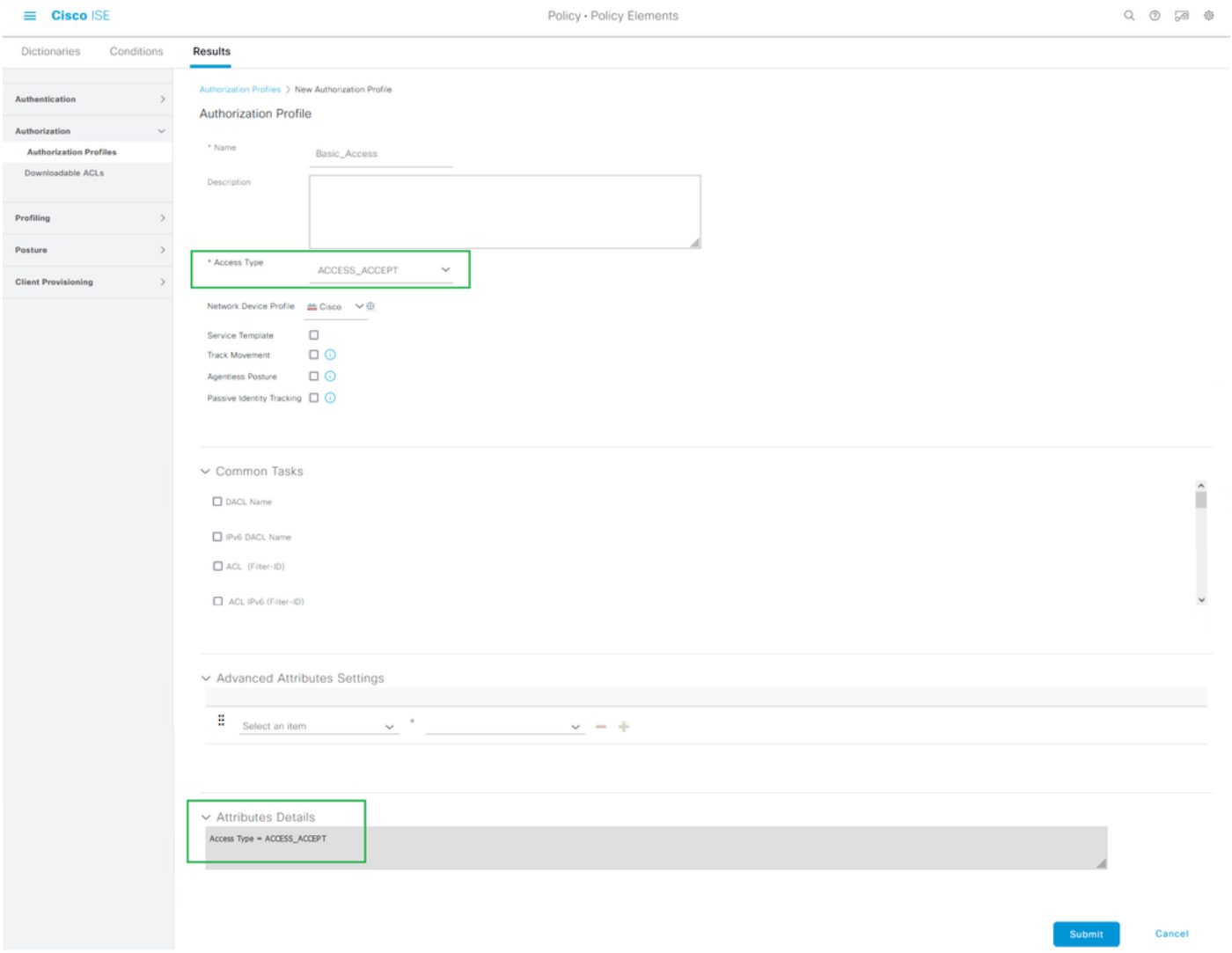
註：使用首選EAP協定設定為EAP-TLS的值會導致ISE請求EAP-TLS協定作為提供給終端IEEE 802.1x請求方的第一個協定。如果您打算經常在通過ISE進行身份驗證的大多數終端上通過EAP-TLS進行身份驗證，此設定非常有用。

步驟 9.建立授權配置檔案

需要構建的最後一個策略元素是授權配置檔案，它繫結到授權策略並提供所需的訪問級別。授權配置檔案已繫結到授權策略。要從ISE GUI對其進行配置，請導航至 **Policy > Policy Elements: Results > Authorization > Authorization Profiles** 然後按一下 **Add.**

授權配置檔案包含一種配置，該配置導致從ISE傳遞至給定RADIUS會話的NAD的屬性，這些屬性用於實現所需的網路訪問級別。

此處所示，它只是將RADIUS Access-Accept作為訪問型別傳遞，但是，在初始身份驗證時可以使用其他專案。注意最底層的屬性詳細資訊，它包含ISE在匹配給定授權配置檔案時傳送到NAD的屬性摘要。



授權配置檔案 — 策略元素

有關ISE授權配置檔案和策略的更多資訊，請參閱Cisco Identity Services Engine Administrator Guide， Release 3.1 > Chapter: Segmentation > Authorization Policies。

安全策略

從ISE GUI建立身份驗證和授權策略，選擇 **Policy > Policy Sets.**預設情況下，在ISE 3.x上啟用這些功能。安裝ISE時，始終定義一個策略集，即預設策略集。預設策略集包含預定義和預設身份驗證、授權和例外策略規則。

策略集按層次進行配置，允許ISE管理員根據意圖將類似的策略組合到不同的策略集，以便在身份驗證請求中使用。自定義和分組策略幾乎是無限的。因此，一個策略集可用於網路訪問的無線端點身份驗證，而另一個策略集可用於網路訪問的有線端點身份驗證；或用於任何其他獨特和獨特的方式來管理策略。

思科ISE可以評估策略集，並且其中的策略使用自上而下的方法，當該策略集的所有條件評估為True時，首先匹配給定的策略集；ISE根據此進一步評估與策略集匹配的身份驗證策略和授權策略，如下所示：

1. 政策集與政策集條件的評價

2. 匹配策略集中的身份驗證策略
3. 授權策略 — 本地例外
4. 授權策略 — 全域性例外
5. 授權策略

策略例外全域性存在於所有策略集中，或者本地存在於特定策略集中。這些策略例外作為授權策略的一部分處理，因為它們涉及為給定臨時場景的網路訪問授予的許可權或結果。

下一部分介紹如何組合配置和策略元素以繫結到ISE身份驗證和授權策略以通過EAP-TLS對終端進行身份驗證。

步驟 10.建立策略集

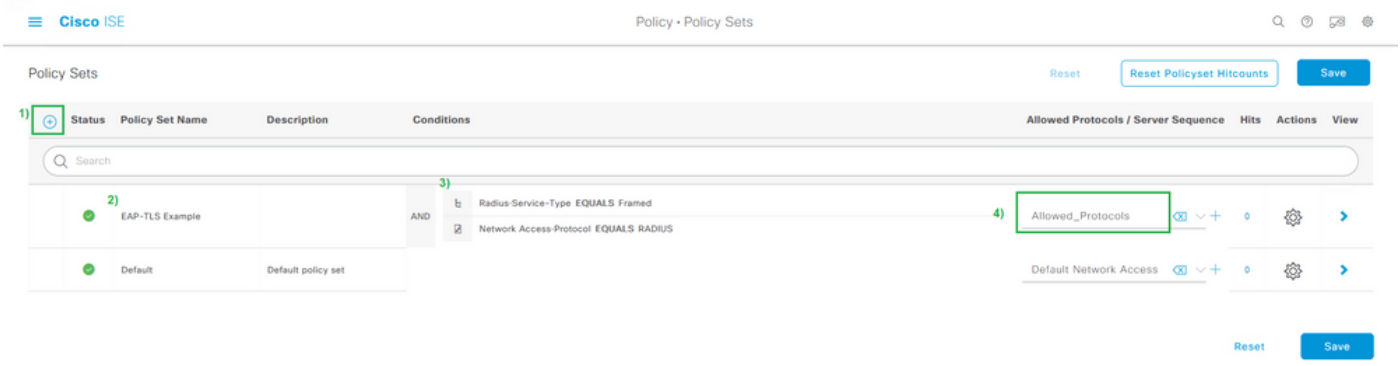
策略集是一個分層容器，由單個使用者定義的規則組成，該規則指示允許的網路訪問協定或伺服器序列，以及身份驗證和授權策略及策略例外，所有這些策略都使用使用者定義的基於條件的規則進行配置。

要從ISE GUI建立策略集，請導航至 **Policy > Policy Set** 然後按一下左上角的加號(+)圖示，如下圖所示。

新增新策略集

策略集可以繫結/組合先前配置的此策略元素，並且用於確定在給定RADIUS身份驗證請求(Access-Request)中要匹配的策略集：

- 繫結：允許的協定服務



定義策略集條件和允許的協定清單

此範例使用在RADIUS作業階段中可能會出現的特定屬性和值來執行IEEE 802.1x（框架屬性），即使重新執行RADIUS通訊協定可能是多餘的。為了取得最佳結果，請僅使用適用於預期目的的唯一RADIUS作業階段屬性，例如網路裝置群或特定用於有線802.1x、無線802.1x或有線的802.1x和無線802.1x。

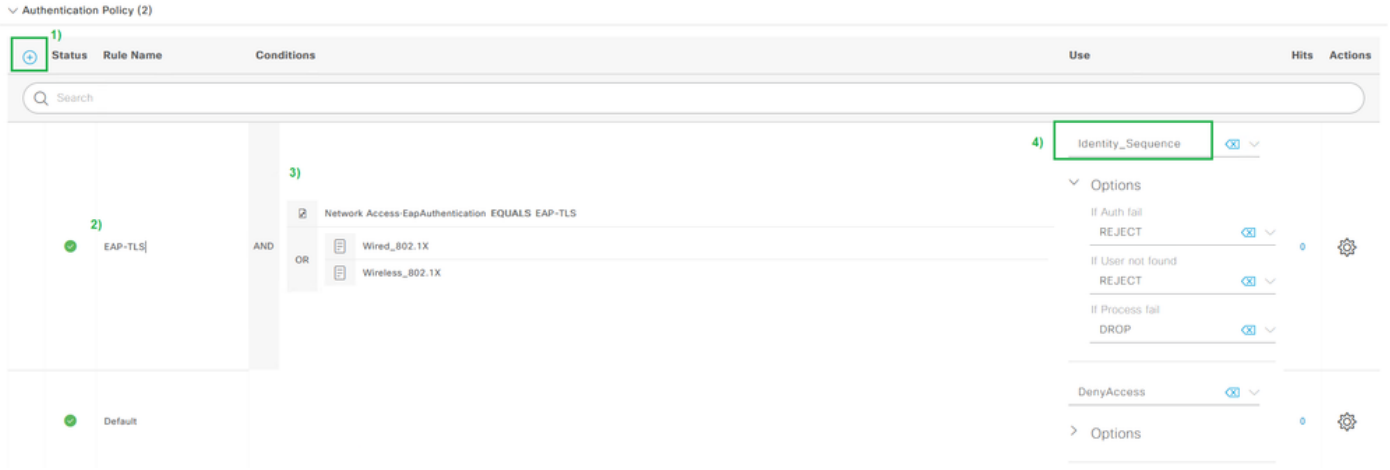
有關ISE策略集的詳細資訊，請參閱《思科身份服務引擎管理員指南，版本3.1 >章節：分段>策略集

、身份驗證策略和授權策略部分。

步驟 11.建立身份驗證策略

在策略集內部，身份驗證策略將之前配置為使用的這些策略元素與條件繫結/合併，以確定何時匹配身份驗證規則。

- 繫結：證書身份驗證配置檔案或身份源序列。

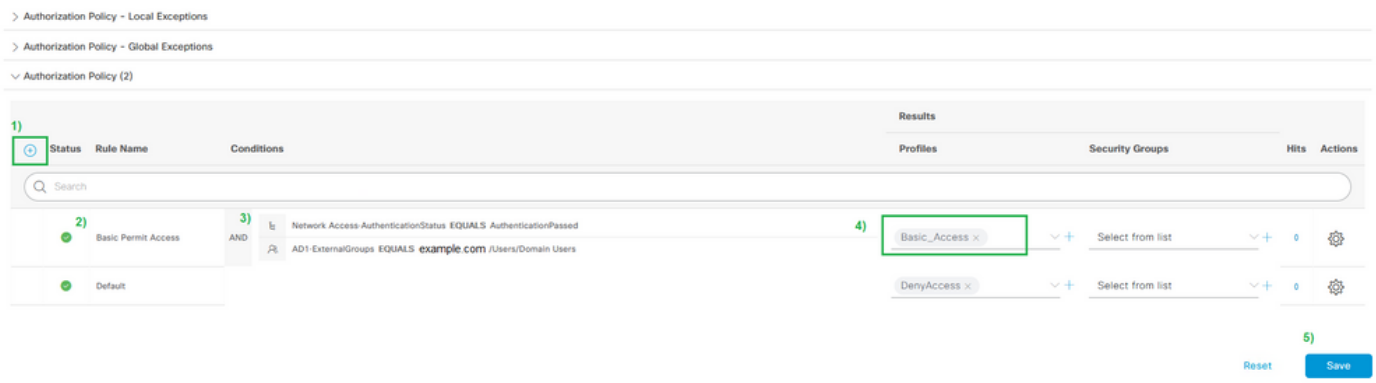


身份驗證策略規則示例

步驟 12.建立授權策略

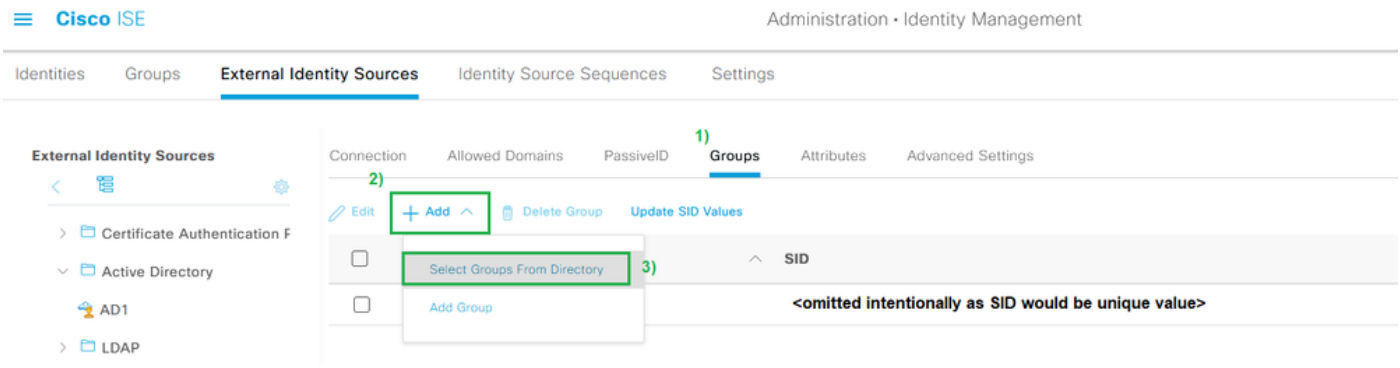
在策略集內部，授權策略繫結/組合先前配置為與條件一起使用的這些策略元素，以確定何時匹配授權規則。此示例針對使用者身份驗證，因為條件指向Active Directory中的Domain Users安全組。

- 繫結：授權配置檔案

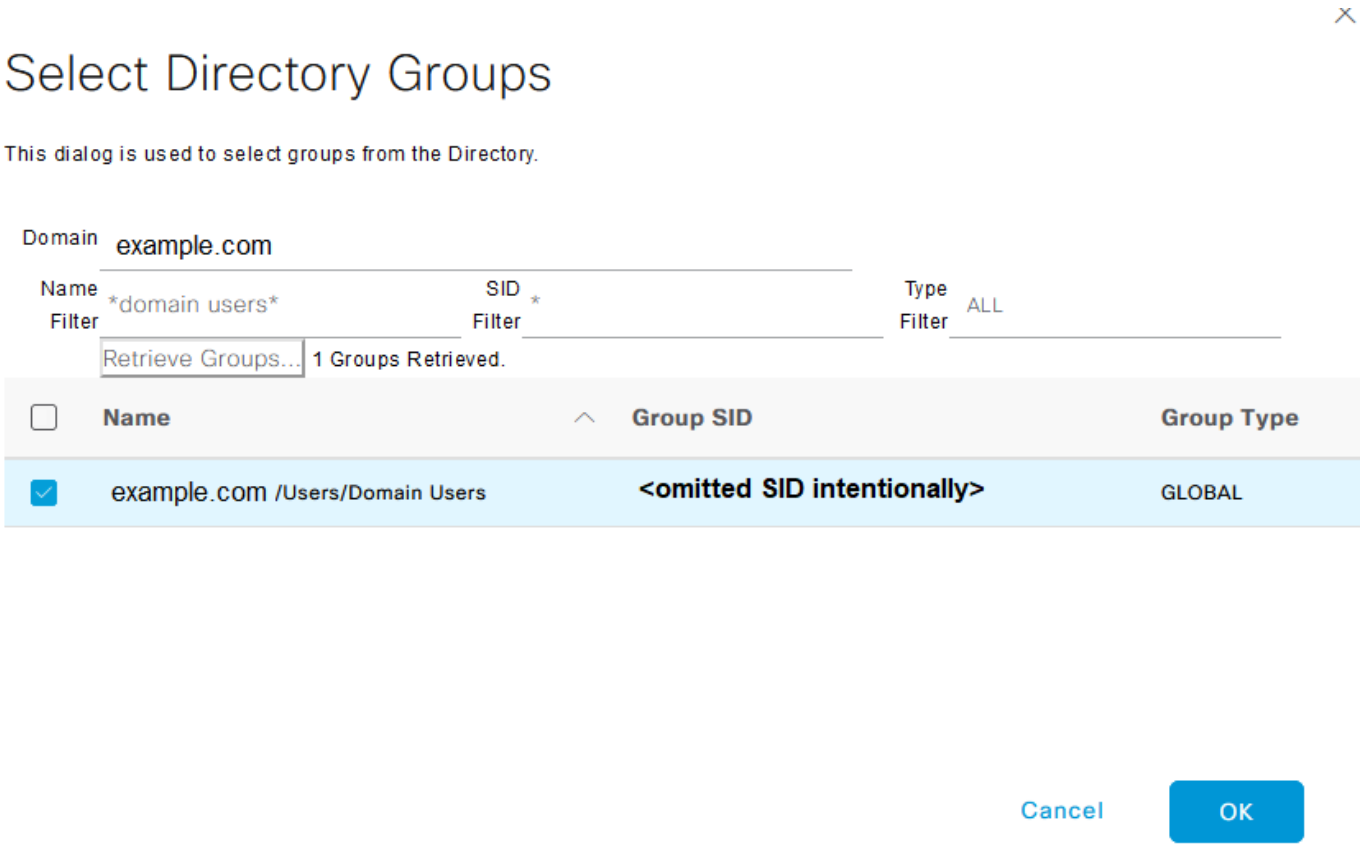


授權策略規則示例

要新增外部組（例如從Active Directory或LDAP），必須從外部伺服器例項新增該組。在本示例中，它來自ISE UI: **Administration > Identity Management: External Identity Sources > Active Directory {AD Join Point Name} > Groups.**在「組」頁籤中選擇 **Add > Select Groups from Directory** 並使用「名稱」篩選器搜尋所有組(*)或特定組，例如「域使用者」（*域使用者*）以檢索組。



要在ISE策略中使用外部組，必須從目錄新增組



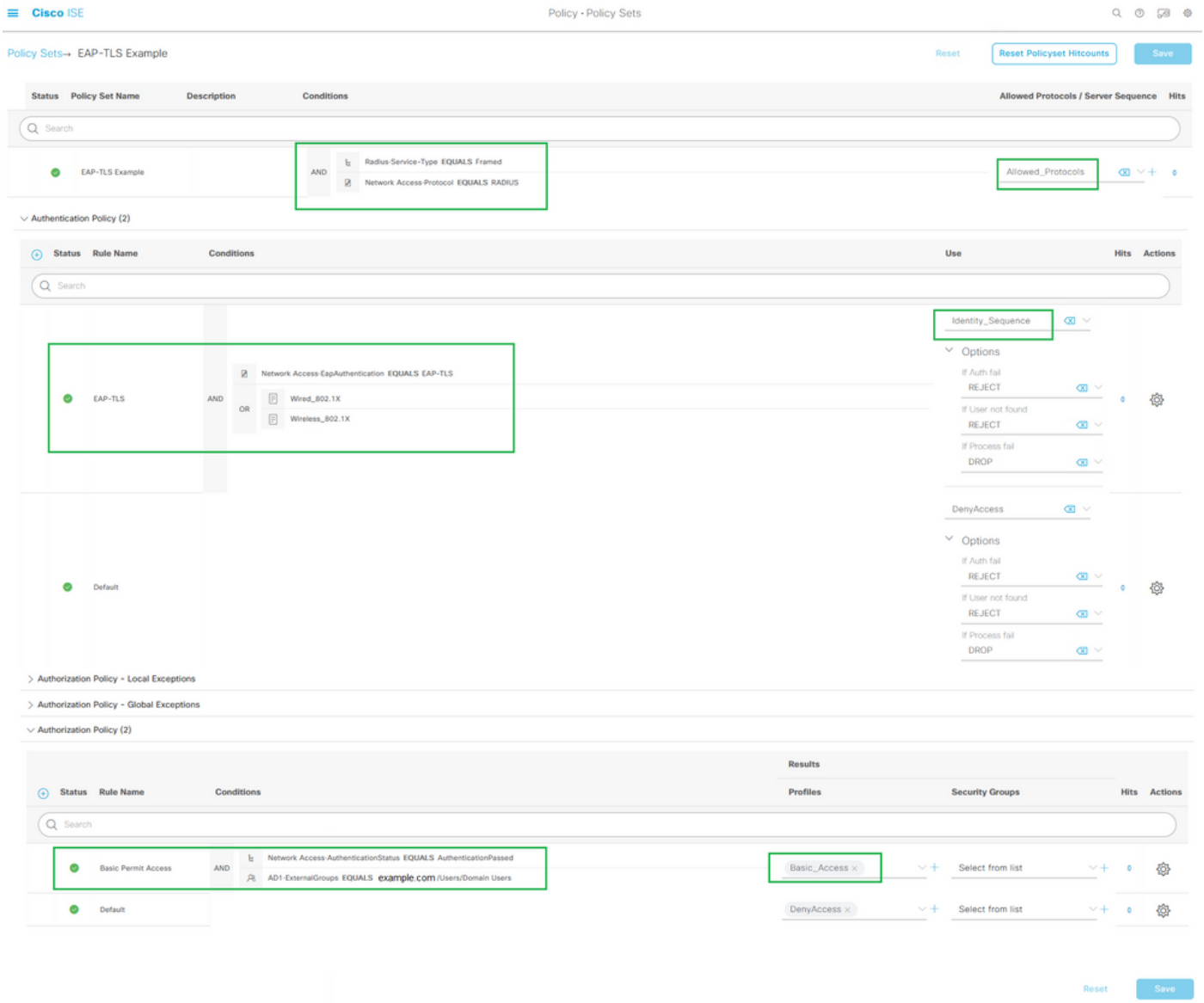
在外部目錄內搜尋 — Active Directory示例

選中每個組旁邊的覈取方塊後，您將在ISE內的策略中使用。若要儲存變更內容，請勿忘記按一下「Ok」和/或「Save」。

驗證

使用本節內容，確認您的組態是否正常運作。

所有全域性配置和策略元素繫結策略集後，通過EAP-TLS進行使用者身份驗證的配置看起來與以下映像類似：

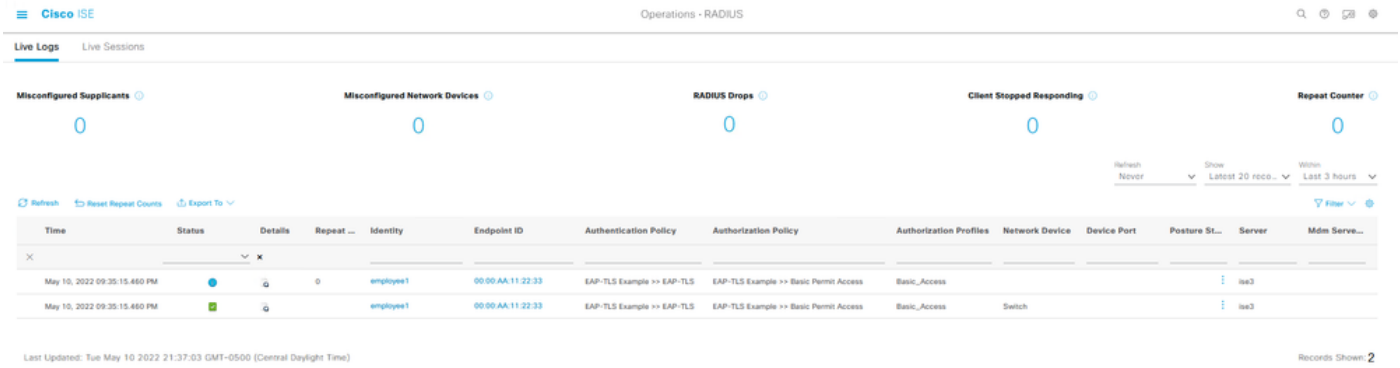


疑難排解

本節提供的資訊可用於對組態進行疑難排解。

配置完成後，連線終端以測試身份驗證。結果可在ISE GUI中找到。選擇 **Operations > Radius > Live Logs**如圖所示。

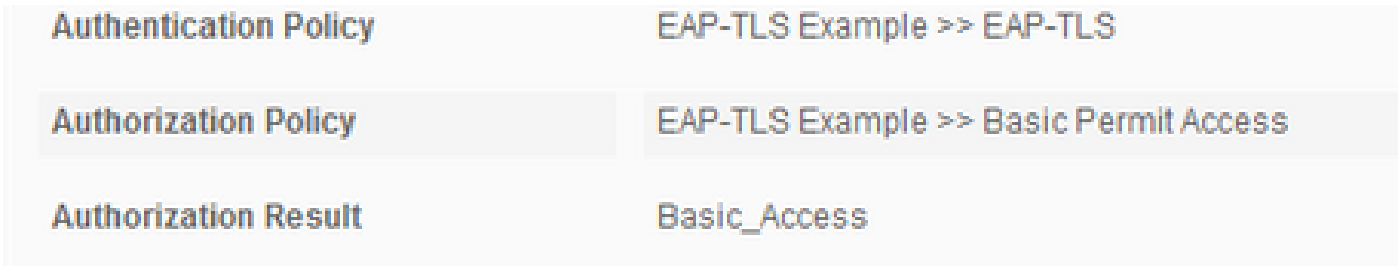
為了便於瞭解，RADIUS和TACACS+（裝置管理）的即時日誌可用於過去24小時內的身份驗證嘗試/活動以及過去100條記錄。如果您希望在此時間範圍之後看到此類報告資料，則需要使用報告，具體為： **ISE UI: Operations > Reports > Reports: Endpoints and Users > RADIUS Authentications.**



Radius > Live Logs的輸出示例

在ISE中的RADIUS即時日誌中，您期望找到有關RADIUS會話的資訊，包括會話屬性和其他有用資訊，以診斷在身份驗證流程期間觀察到的行為。按一下 **details** 圖示可開啟會話的詳細檢視，檢視會話屬性以及特定於此身份驗證嘗試的相關資訊。

為了進行故障排除，必須確保匹配的策略正確。對於此配置示例，所需的身份驗證和授權策略與預期匹配，如下圖所示：



在詳細檢視中，檢查這些屬性以驗證身份驗證是否按照本配置示例中設計預期的方式運行：

- 活動
  - 這包含驗證是否成功。
  - 在工作場景中，值為：5200身份驗證成功。

- 使用者名稱
  - 這包括從呈現給ISE的客戶端證書提取的終端標識。
  - 在工作場景中，這是登入到終結點的使用者的使用者名稱（即，來自上一個映像的employee1）。

- 終端ID
  - 對於有線/無線，此值是來自終端的網路介面卡(NIC)的MAC地址。
  - 在工作場景中，這將成為終端的MAC地址，除非連線通過VPN，在這種情況下，可以是終端的IP地址。

- 身份驗證策略
  - 根據與策略條件匹配的會話屬性顯示給定會話的匹配身份驗證策略。
  - 在工作場景中，這是所配置的預期身份驗證策略。
  - 如果您看到另一個策略，則表示與策略中的條件比較時的預期策略未評估為true。在這種情況下，請檢查會話屬性，並確保每個策略包含每個策略的不同但唯一的條件。

- 授權策略
  - 根據與策略條件匹配的會話屬性顯示給定會話的匹配授權策略。
  - 在工作場景中，這是配置的預期授權策略。
  - 如果看到另一個策略，則表示與策略中的條件相比時的預期策略未評估為真。在這種情況下，請檢查會話屬性，並確保每個策略包含每個策略的不同但唯一的條件。

- 授權結果
  - 根據匹配的授權策略，這顯示給定會話中使用的授權配置檔案。
  - 在工作場景中，此值與策略中配置的值相同。為稽核的目的進行稽核並確保配置正確的授權配置檔案是件好事。

- 策略伺服器
  - 這包括身份驗證嘗試所涉及的ISE策略服務節點(PSN)的主機名。
  - 在工作場景中，您只能看到傳至第一PSN節點的身份驗證（如在NAD上配置的），除非PSN未運行或者發生故障切換（如由於延遲高於預期或身份驗證超時）。

- 驗證方法
  - 顯示給定會話中使用的身份驗證方法。在本例中，您將看到值為dot1x。
  - 在基於此組態範例的正常情況下，您會看到值為dot1x。如果您看到另一個值，可能表示dot1x失敗或未嘗試。

- 驗證通訊協定
  - 顯示給定會話中使用的身份驗證方法。在本例中，您將看到值為EAP-TLS。
  - 在基於此配置示例的工作方案中，您始終看到值為EAP-TLS。如果您看到另一個值，則請求方和ISE未成功協商EAP-TLS。

- 網路裝置
  - 顯示終端與ISE之間身份驗證嘗試所涉及的NAD（也稱為邊緣裝置）的網路裝置名稱（如ISE中配置）。
  - 在工作場景中，此名稱始終在ISE UI中指定： **Administration > System: Network Devices**. 根據該配置，NAD的IP地址（也稱為邊緣裝置）用於確定身份驗證來自哪個網路裝置，該網路裝置包含在NAS IPv4地址會話屬性中。

這絕不是為了進行故障排除或其他可見性而要檢查的所有可能會話屬性的完整清單，因為還有其他要驗證的有用屬性。建議複習所有會話屬性以開始熟悉所有資訊。您可以看到Steps部分下麵包含右側，它顯示了ISE執行的操作或行為。

常見問題和疑難排解技巧

此清單包括一些常見問題和故障排除建議，但無論如何不應成為完整清單。相反，請以此為指南，開發您自己的技術，以便在涉及ISE時排除故障。

問題：遇到身份驗證失敗(5400身份驗證失敗)或任何其他不成功的身份驗證嘗試。

- 如果遇到身份驗證失敗，請按一下details圖示，該圖示提供有關身份驗證失敗的原因和採取的步驟的資訊。其中包括故障原因和可能的根本原因。

- 由於ISE對身份驗證結果做出決策，因此ISE擁有資訊來瞭解身份驗證嘗試失敗的原因。

問題：身份驗證未成功完成，失敗原因顯示為「5440終端已放棄EAP會話並已啟動新」或「5411請求方停止響應ISE」。

- 此故障原因表示RADIUS通訊在超時之前未完成。因為EAP在終端和需要之間，所以您需要檢查需要在NAD上使用的超時並確保它被設定至少五秒。

- 如果五秒還不足以解決此問題，則建議再增加五秒幾次，然後重新測試，以驗證此技術是否解決了此問題。

- 如果上述步驟未解決此問題，則建議確保身份驗證由相同且正確的ISE PSN節點處理，並且整體行為不指示異常行為，例如NAD和ISE PSN節點之間的延遲高於正常值。

- 此外，如果ISE未收到客戶端證書，則最好驗證終端是否通過資料包捕獲傳送客戶端證書，然後終端（使用者證書）不能信任ISE EAP身份驗證證書。如果發現為true，則在正確的證書儲存中匯入CA鏈（根CA =受信任的根CA）| 中介CA =受信任中介CA)。

問題：身份驗證成功，但與正確的身份驗證和/或授權策略不匹配。

- 如果您遇到的身份驗證請求成功，但與正確的身份驗證和/或授權規則不匹配，則建議檢視會話屬性，以確保使用的條件準確且存在於RADIUS會話中。

- ISE從自上而下評估這些策略（安全評估策略除外）。您需要首先確定匹配的策略是否高於或低於要匹配的所需策略。首先評估身份驗證策略，並且獨立於授權策略。如果身份驗證策略正確匹配，則在22037名為Steps的右側Authentication Details部分的Authentication Passed。

- 如果所需策略高於匹配策略，這意味著所需策略上的條件總和未計算為真。它檢查條件和會話中的所有屬性和值，以確保它存在並且不存在拼寫錯誤。

- 如果所需的策略低於匹配的策略，則意味著另一個策略（上述）已匹配，而不是所需的策略。這可能表示條件值不夠具體，條件在另一個策略中重複，或策略順序不正確。雖然故障排除變得更加困難，但建議開始檢查策略，以確定與所需策略不匹配的原因。這有助於確定下一步要執行的操作。

問題：身份驗證期間使用的身份或使用者名稱不是預期值。

- 如果發生這種情況，如果終端傳送客戶端證書，則最有可能的ISE不使用證書身份驗證模板中的正確證書欄位；該欄位在身份驗證階段進行評估。

- 檢視客戶端證書，找到所需的身份/使用者名稱所對應的確切欄位，並確保從中選擇相同的欄位： **ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).**

問題：身份驗證不成功，失敗原因為12514 EAP-TLS由於客戶端證書鏈中的未知CA而未能進行SSL/TLS握手。

- 如果客戶端證書的CA鏈中的證書在ISE UI上不可信，則會發生以下情況： **Administration > System: Certificates > Trusted Certificates.**

- 當客戶端證書（在終端上）的CA鏈與為EAP身份驗證登入到ISE的證書CA鏈不同時，通常會發生這種情況。

- 要解決此問題，請確保在ISE上信任客戶端證書CA鏈，在終端上信任ISE EAP身份驗證伺服器證書CA鏈。
  — 對於Windows OS和Chrome，請導航至 **Start > Run MMC > Add/Remove Snap-In > Certificates > User Certificates.**
  — 對於Firefox：匯入Web伺服器要信任的CA鏈（不是終端身份證書）。

相關資訊

- Cisco Identity Services Engine >安裝和升級指南
- 思科身份服務引擎>配置指南
- Cisco Identity Services Engine >相容性資訊
- 思科身份服務引擎管理員指南，版本3.1 >章節：安全訪問>定義思科ISE中的網路裝置
- Cisco Identity Services Engine管理員指南，版本3.1 >章節：分段>策略集
- Cisco Identity Services Engine管理員指南，版本3.1 >章節：分段>身份驗證策略
- Cisco Identity Services Engine管理員指南，版本3.1 >章節：分段>授權策略
- 思科身份服務引擎>配置指南> Active Directory與思科ISE 2.x的整合
- 思科身份服務引擎管理員指南，版本3.1 >章節：分段>網路訪問服務>用戶的網路訪問
- 思科身份服務引擎管理員指南，版本3.1 >章節：基本設定>思科ISE中的證書管理
- Cisco Identity Services Engine Administrator Guide， Release 3.1 > Chapter: Basic Setup > Cisco ISE CA Service > Configure Cisco ISE to Use Certificates for Authentication Personal Devices > Create a Certificate Authentication Profile for TLS-Based Authentication
- Cisco Identity Services Engine > Configuration Examples and TechNotes > Configure ISE 2.0 Certificate Provisioning Portal
- Cisco Identity Services Engine > Configuration Examples and TechNotes > 在ISE中安裝第三方CA簽名的證書
- 無線LAN(WLAN)>配置示例和TechNotes >使用WLC和ISE瞭解和配置EAP-TLS
- 技術支援與文件 - Cisco Systems

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）。