Configurazione dell'autenticazione EAP-TLS con ISE

Sommario

Introduzione

Questo documento descrive la configurazione iniziale come esempio per introdurre l'autenticazione EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) con Cisco Identity Services Engine (ISE). L'attenzione è rivolta principalmente alla configurazione ISE, che può essere applicata a più scenari, come (ma non solo) l'autenticazione con un IP-Phone/endpoint connesso via cavo o wireless.

Ai fini della presente guida, è importante comprendere le seguenti fasi del flusso di autenticazione ISE (RADIUS):

- Autenticazione: identificazione e convalida dell'identità finale (computer, utente e così via) che richiede l'accesso alla rete.

- Autorizzazione: determinare le autorizzazioni/l'accesso all'identità finale che verranno concesse sulla rete.
- Accounting: report e monitoraggio dell'attività di rete dell'identità finale dopo il completamento dell'accesso alla rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di base del flusso di comunicazioni EAP e RADIUS.
- Conoscenze base di autenticazione RADIUS con metodi di autenticazione basati su certificati in termini di flusso di comunicazione.
- Informazioni sulle differenze tra Dot1x e MAC Authentication Bypass (MAB).
- Conoscenza di base dell'infrastruttura a chiave pubblica (PKI).
- Familiarità con le modalità di ottenimento di certificati firmati da un'Autorità di certificazione (CA) e di gestione di certificati negli endpoint.
- Configurazione delle impostazioni relative a Autenticazione, Autorizzazione e Accounting (AAA) (RADIUS) su un dispositivo di rete (cablato o wireless).
- Configurazione del supplicant (sull'endpoint) per l'utilizzo con RADIUS/802.1x.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE release 3.x.
- CA - per rilasciare certificati (può essere una CA dell'organizzazione, una CA pubblica/di terze parti o utilizzare il portale di provisioning dei certificati).
- Active Directory (origine identità esterna) - da Windows Server; ove compatibile con ISE.
- Dispositivo di accesso alla rete (NAD): può essere switch (cablato) o controller WLC (wireless) configurato per 802.1x/AAA.
- Endpoint: certificati rilasciati all'identità (utente) e alla configurazione del supplicant che verranno autenticati per l'accesso alla rete tramite RADIUS/802.1x: Autenticazione utente. È possibile ottenere un certificato del computer, ma non viene utilizzato in questo esempio.

> **Nota:** Poiché questa guida utilizza ISE release 3.1, tutti i riferimenti alla documentazione si basano su questa versione. Tuttavia, una configurazione simile/simile è possibile e supportata completamente nelle versioni precedenti di Cisco ISE.

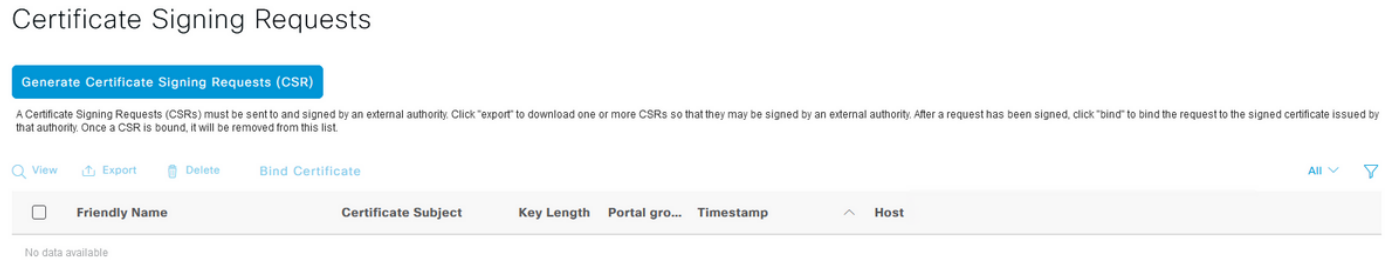
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Ottenere certificati server e client

Passaggio 1. Generare una richiesta di firma del certificato da ISE

Il primo passaggio consiste nel generare una richiesta di firma del certificato (CSR) da ISE e inviarla all'autorità di certificazione (server) per ottenere il certificato firmato rilasciato ad ISE come certificato di sistema. Questo certificato verrà presentato come certificato server da ISE durante l'autenticazione EAP-TLS. Questa operazione viene eseguita nell'interfaccia utente ISE. Passa a **Administration > System: Certificates > Certificate Management > Certificate Signing Requests**. Sotto **Certificate Signing Requests**, fare clic su **Generate Certificate Signing Requests (CSR)** come mostrato nell'immagine.



I tipi di certificato richiedono utilizzi chiave estesi diversi. In questo elenco vengono descritti gli utilizzi chiave estesi necessari per ogni tipo di certificato:

Certificati di identità ISE

- Multiuso (amministrazione, EAP, portale, pxGrid) - Autenticazione client e server
- Admin - Autenticazione server
- Autenticazione EAP - Autenticazione server
- Autenticazione DTLS (Datagram Transport Layer Security) - Autenticazione server
- Portale - Autenticazione server
- pxGrid - Autenticazione client e server
- SAML (Security Assertion Markup Language) - Certificato di firma SAML
- ISE Messaging Service - Genera un certificato di firma o genera un nuovo certificato di messaggistica

Per impostazione predefinita, il certificato di sistema "ISE Messaging Service" è destinato alla replica dei dati su ciascun nodo ISE nell'implementazione, nella registrazione dei nodi e in altre comunicazioni tra nodi e sarà presente e rilasciato dal server ISE Internal Certificate Authority (interno di ISE). Non è necessario completare alcuna azione con questo certificato.

Il certificato di sistema "Admin" viene utilizzato per identificare ogni nodo ISE, ad esempio quando viene utilizzata l'API associata all'interfaccia utente (gestione) di Admin, e per alcune comunicazioni tra nodi. Per configurare ISE per la prima volta, configurare il certificato di sistema "Admin". Questa azione non è direttamente correlata alla presente guida alla configurazione.

per eseguire IEEE 802.1x tramite EAP-TLS (autenticazione basata su certificati), intervenire sul certificato di sistema "autenticazione EAP" in quanto sarà utilizzato come certificato server presentato all'endpoint/client durante il flusso EAP-TLS; il risultato sarà protetto all'interno del tunnel TLS. Per iniziare, creare un CSR per creare il certificato di sistema di autenticazione EAP e assegnarlo al personale che gestisce i server CA dell'organizzazione (o al provider CA pubblico) per la firma. Il risultato finale sarà il certificato firmato dalla CA che verrà associato al CSR e ad ISE con questi passaggi.

Nel modulo Richiesta di firma del certificato (CSR) scegliere le opzioni seguenti per completare il CSR e ottenerne il contenuto:

- Utilizzo certificato, per questo esempio di configurazione scegliere **EAP Authentication**.
- Se si prevede di utilizzare un'istruzione con caratteri jolly nel certificato, ***.example.com**, è necessario controllare anche il **Allow Wildcard Certificate** casella di controllo. La posizione migliore è il campo del certificato SAN (Subject Alternative Name) per la compatibilità con qualsiasi utilizzo e tra più tipi diversi di sistemi operativi endpoint presenti nell'ambiente.
- Se non si è scelto di inserire un'istruzione con caratteri jolly nel certificato, scegliere i nodi ISE a cui si desidera associare il certificato con firma CA (dopo la firma). Nota: Quando si associa il certificato firmato dall'autorità di certificazione contenente l'istruzione con caratteri jolly a più nodi all'interno del CSR, il certificato verrà distribuito a ogni nodo ISE (o ai nodi selezionati) nella distribuzione ISE e i servizi potrebbero essere riavviati. Tuttavia, il riavvio dei servizi verrà limitato automaticamente a un nodo alla volta. Monitorare il riavvio dei servizi tramite **show application status ise** ISE CLI.Successivamente, sarà necessario completare il modulo per definire l'oggetto. Sono inclusi i campi Nome comune (CN), Unità organizzativa (OU), Organizzazione (O), Città (L), Stato (ST) e Paese (C). La variabile *$FQDN$* è il valore che rappresenta il nome di dominio completo (nome host + nome di dominio) di gestione associato a ciascun nodo ISE.
- OSPF (Open Shortest Path First) **Subject Alternative Name (SAN)** devono inoltre essere compilati in modo da includere tutte le informazioni necessarie e desiderate da utilizzare per stabilire la fiducia. Come requisito, sarà necessario definire la voce DNS che punta all'FQDN dei nodi ISE che verranno associati a questo certificato, dopo che il certificato sarà stato firmato.
- Infine, accertarsi di definire il "Tipo di chiave", la "Lunghezza della chiave" e il "Digest to Sign With" appropriati, in conformità alle funzionalità dei server CA e tenendo presenti le buone prassi di sicurezza. I valori predefiniti sono: RSA, 4096 bit, e SHA-384, rispettivamente. Le opzioni disponibili e la compatibilità verranno visualizzate in questa pagina all'interno dell'interfaccia utente di ISE Admin.

Questo è un esempio di modulo CSR completato senza l'utilizzo di un'istruzione wildcard. Assicurarsi di utilizzare valori effettivi specifici dell'ambiente:

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)
$FQDN$

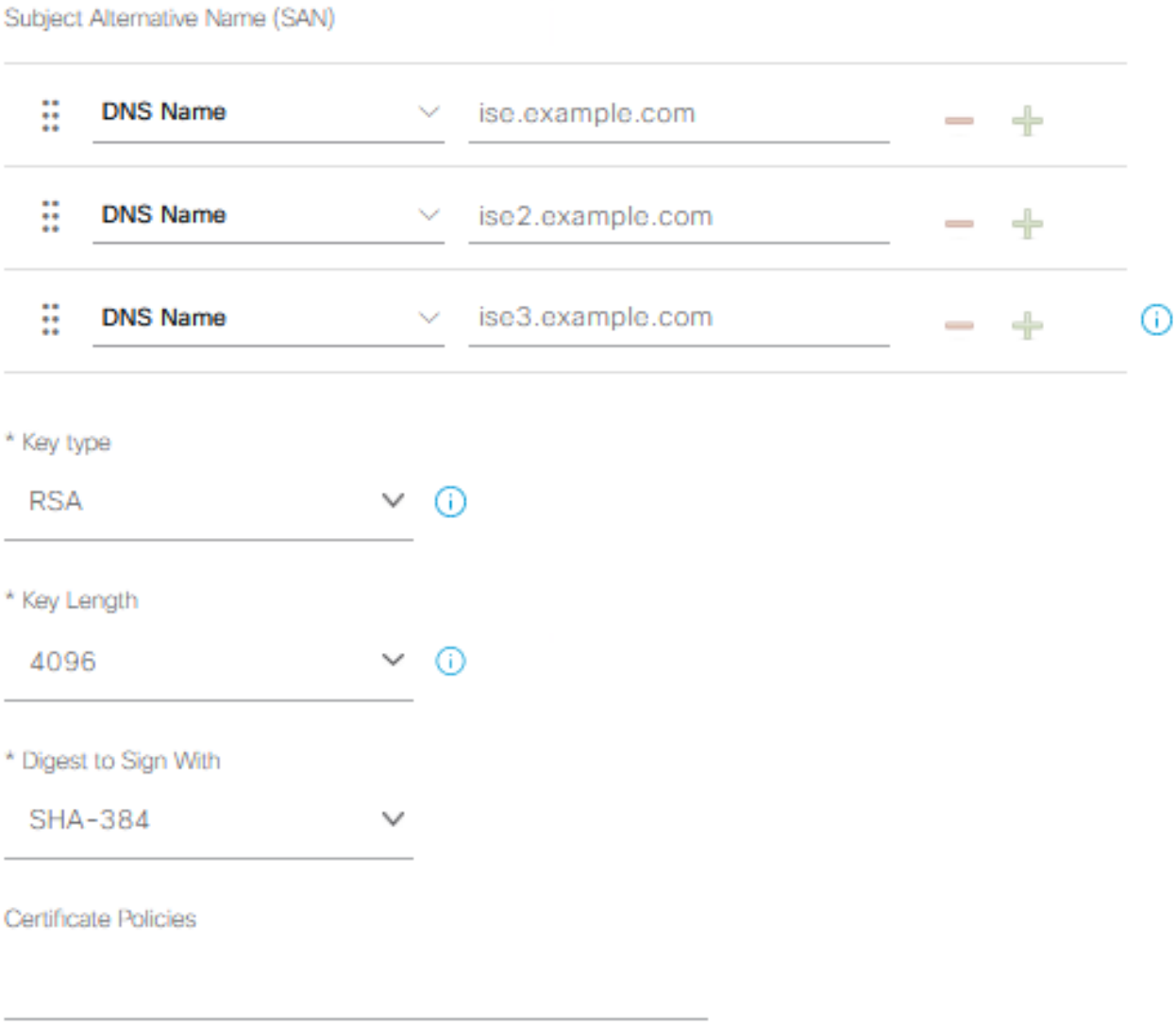
Organizational Unit (OU)

Organization (O)
Example Company

City (L)
San Jose

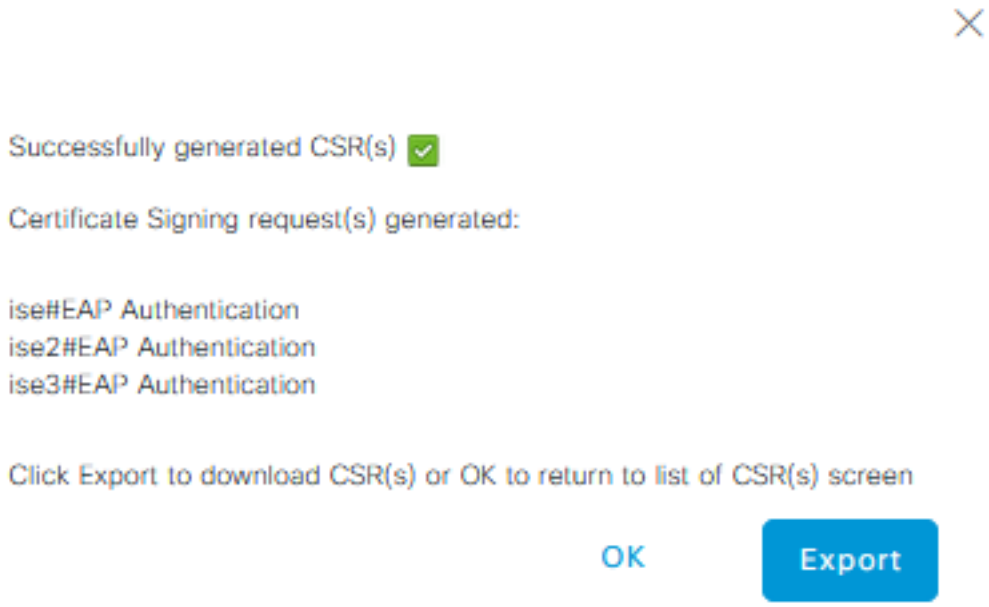
State (ST)
California

Country (C)
US



Esempio di CSR

Per salvare il CSR, fare clic su **Generate**. Clic **Export**, posizionato in basso a destra, per esportare i file CSR dal prompt:



Esempio di esportazione di CSR

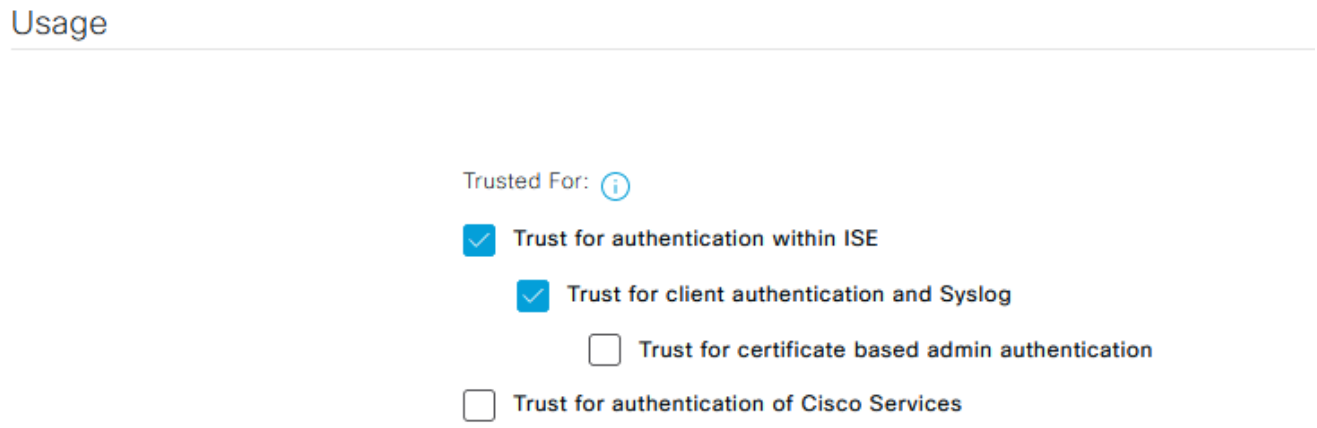
Per ulteriori informazioni sui certificati per l'uso con ISE, consultare il *Cisco Identity Services Engine Administrator Guide, Release 3.1 > Capitolo: Installazione di base >* [*Gestione certificati in Cisco ISE*] e installazione di un certificato firmato da un'autorità di certificazione di terze parti in ISE.

Passaggio 2. Importazione dei certificati CA in ISE

Dopo che la CA ha restituito il certificato firmato, includerà anche la catena completa della CA, costituita da un certificato radice e da uno o più certificati intermediari. L'interfaccia utente di ISE Admin consente di importare tutti i certificati nella catena CA prima dell'associazione o del caricamento di qualsiasi certificato di sistema. Questa operazione viene eseguita per garantire che ogni certificato di sistema sia associato correttamente alla catena di CA (nota anche come certificato protetto) all'interno del software ISE.

Questi passaggi rappresentano il modo migliore per importare i certificati CA e il certificato di sistema in ISE:

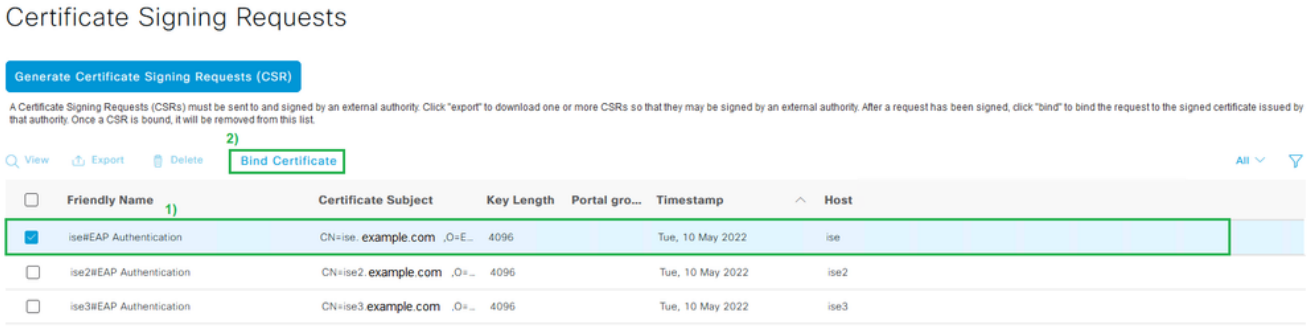
1. Per importare il certificato radice nella GUI di ISE, selezionare **Administration > System: Certificates > Certificate Management**. Sotto **Trusted Certificates**, fare clic su **Import** e selezionare le caselle di controllo **Trust for authentication within ISE** (Infrastructure) and **Trust for client authentication and Syslog** (Endpoints).



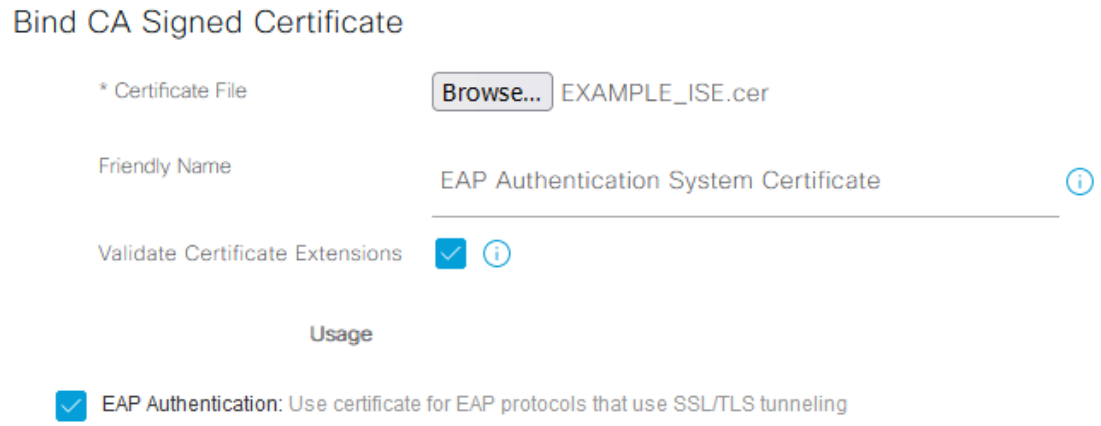
Utilizzo certificati per catena CA

2. Ripetere il passaggio precedente per ogni certificato intermedio come parte della catena di certificati CA.

3. Dopo aver importato tutti i certificati come parte della catena completa di CA nell'archivio dei certificati attendibili di ISE, tornare alla GUI di ISE e selezionare **Administration > System: Certificates > Certificate Management: Certificate Signing Requests**. Individuare la voce CSR in **Nome descrittivo** corrispondente al certificato firmato, fare clic sulla casella di controllo del certificato e quindi su **Bind Certificate**.



*Associa certificato a CSR***Nota:** È necessario associare un singolo certificato firmato dalla CA a ciascun CSR uno alla volta. Ripetere l'operazione per tutti i CSR rimanenti creati per altri nodi ISE nell'implementazione.Nella pagina successiva fare clic su **Browse** e scegliere il file del certificato firmato, definire un nome descrittivo desiderato e scegliere Uso certificato. Invia per salvare le
modifiche.



Selezionare il certificato da associare a CSR

4. A questo punto, il certificato firmato viene spostato nella GUI ISE. Passa a **Administration > System: Certificates > Certificate Management: System Certificates** e assegnare allo stesso nodo per cui

è stato creato il CSR. Ripetere la stessa procedura per altri nodi e/o altri utilizzi di certificati.

Passaggio 3. Ottenere il certificato client per l'endpoint

Ènecessario eseguire un processo simile sull'endpoint per la creazione di un certificato client da utilizzare con EAP-TLS. Per questo esempio, è necessario un certificato client firmato e rilasciato all'account utente per eseguire l'autenticazione utente con ISE. Un esempio di come ottenere un certificato client per l'endpoint da un ambiente Active Directory è disponibile in: Comprendere e configurare EAP-TLS utilizzando WLC e **ISE > Configure >** Client for EAP-TLS.

A causa dei diversi tipi di endpoint e sistemi operativi, poiché il processo può essere diverso, non vengono forniti ulteriori esempi. Tuttavia, il processo complessivo è concettualmente lo stesso. Generare un CSR che disponga di tutte le informazioni rilevanti da includere nel certificato e che lo faccia firmare dall'autorità di certificazione, sia che si tratti di un server interno nell'ambiente o di un'azienda pubblica/terza che fornisce questo tipo di servizio.

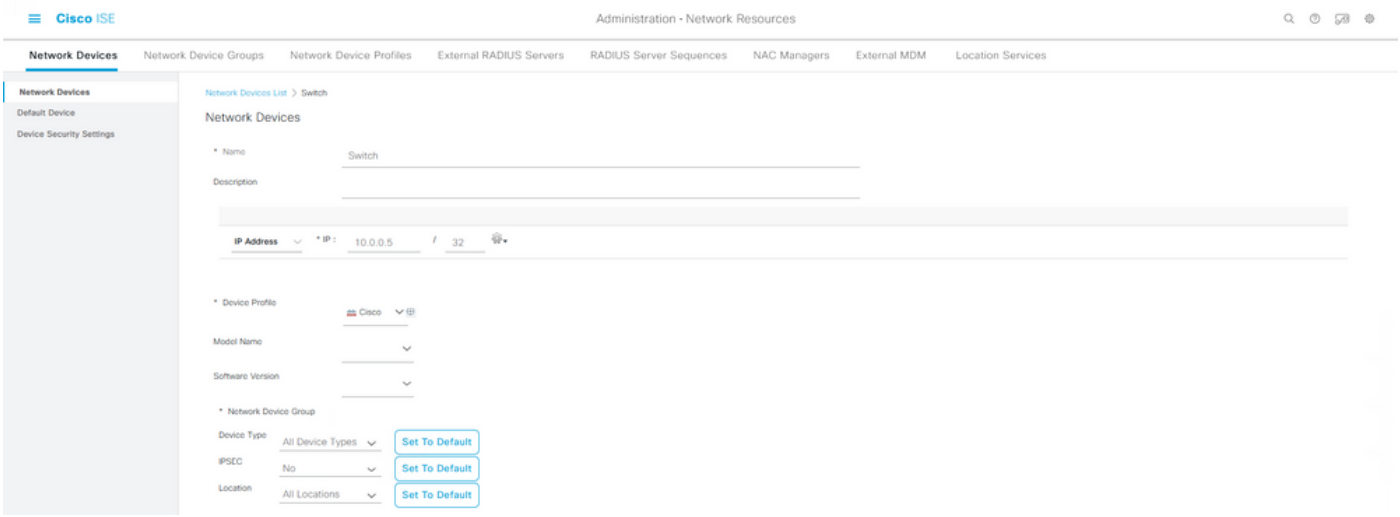
Inoltre, i campi Nome comune (CN) e Nome alternativo soggetto (SAN) includono l'identità in cui utilizzare durante il flusso di autenticazione. Questo determina anche come il supplicant deve essere configurato per EAP-TLS in termini di identità: Autenticazione computer e/o utente, Autenticazione computer o Autenticazione utente. In questo esempio viene utilizzata solo l'autenticazione utente nel resto del documento.

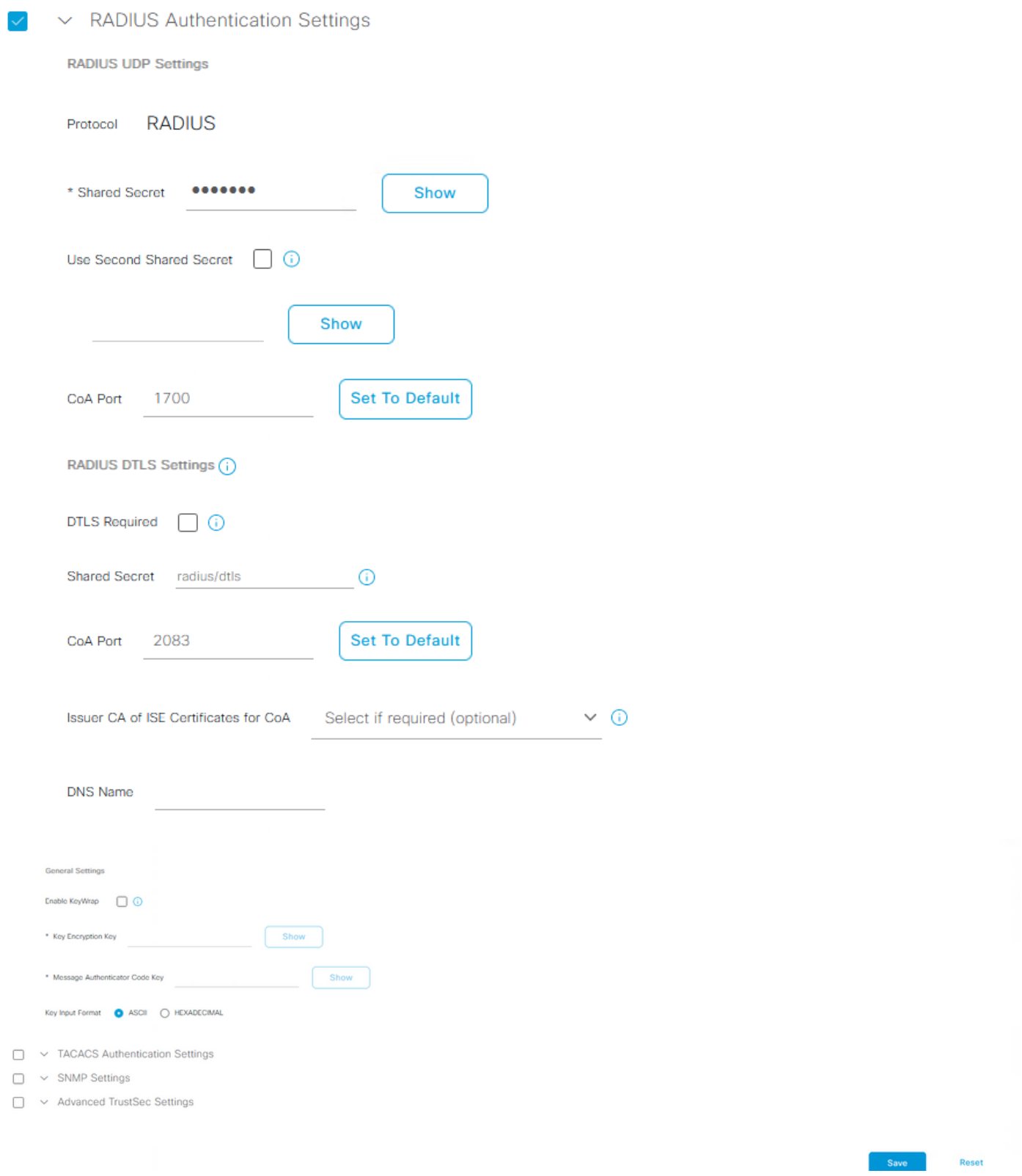
Dispositivi di rete

Passaggio 4. Aggiungere il dispositivo di accesso alla rete ad ISE

Anche il dispositivo di accesso alla rete (NAD) a cui è connesso un endpoint è configurato in ISE in modo da consentire la comunicazione RADIUS/TACACS+ (Device Admin). Tra NAD e ISE, viene utilizzato un segreto/password condiviso per scopi di attendibilità.

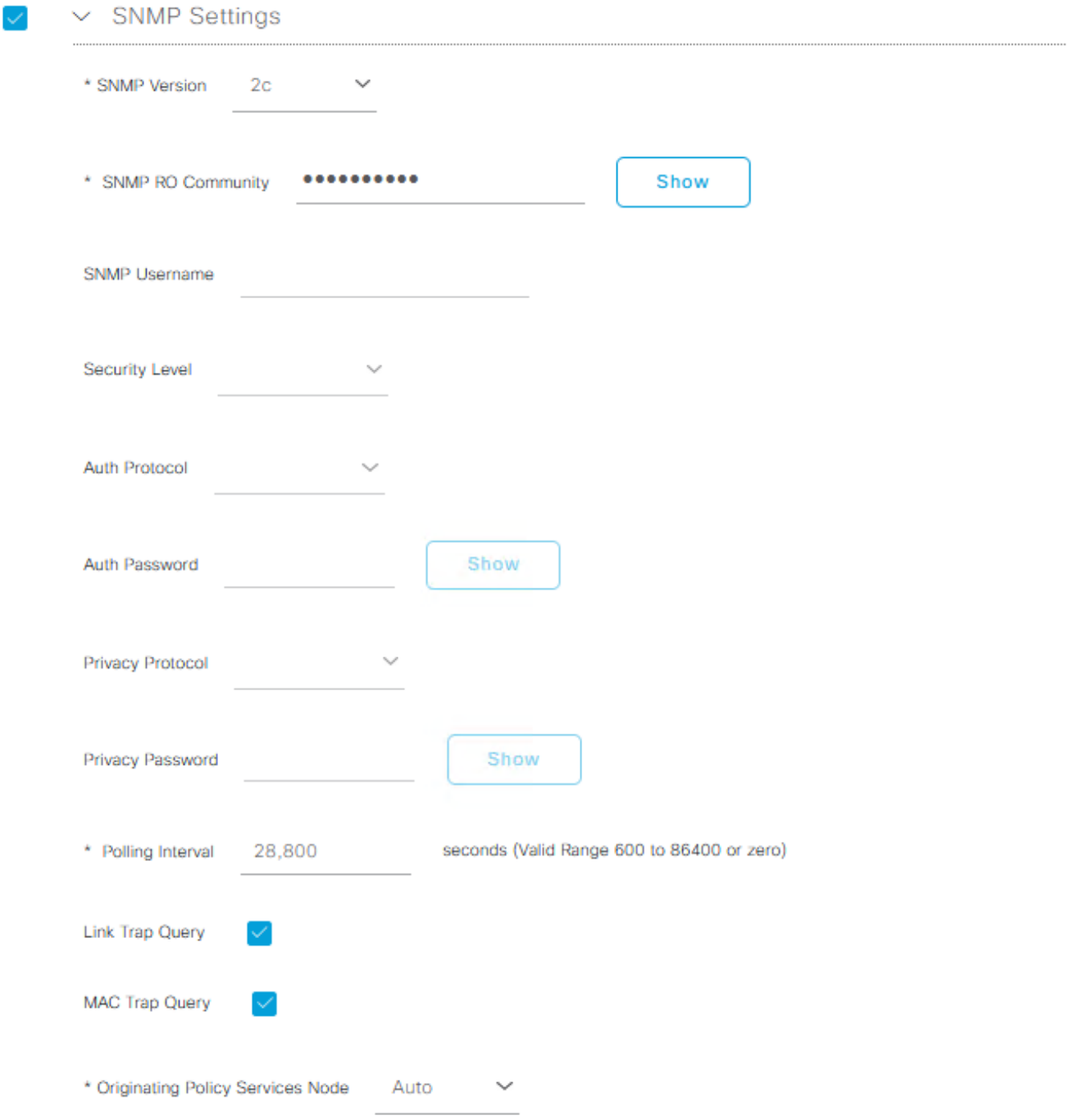
Per aggiungere un indirizzo NAD tramite l'interfaccia utente grafica di ISE, selezionare **Administration > Network Resources: Network Devices > Network Devices** e fare clic su **Add**, illustrato nell'immagine.





Esempio di configurazione di un dispositivo di rete

Da utilizzare con ISE Profiling, è possibile configurare anche SNMPv2c o SNMPv3 (più sicuro) per consentire ad ISE Policy Service Node (PSN) di contattare NAD tramite query SNMP che riguardano l'autenticazione dell'endpoint ad ISE al fine di raccogliere gli attributi per prendere decisioni accurate sul tipo di endpoint utilizzato. Nell'esempio seguente viene illustrato come configurare SNMP (v2c), dalla stessa pagina dell'esempio precedente:



Esempio di configurazione di SNMPv2c

Per ulteriori informazioni, consultare il *Cisco Identity Services Engine Administrator Guide*, *versione 3.1 > Capitolo: Secure Access >* [*Definizione dei dispositivi di rete in Cisco ISE*].

Ora, se non è già stato fatto, è necessario configurare tutte le impostazioni relative al server AAA sul server NAD per autenticarsi e autorizzare l'autenticazione con Cisco ISE.

Elementi criteri

Queste impostazioni sono elementi che finiscono per essere associati al criterio di autenticazione o al criterio di autorizzazione. In questa guida viene generato principalmente ogni elemento di criterio, che viene quindi mappato nel criterio di autenticazione o di autorizzazione. È importante tenere presente che il criterio non è attivo fino a quando non viene completato correttamente il binding al criterio di autenticazione/autorizzazione.

Passaggio 5. Usa origine identità esterna

Un'origine di identità esterna è semplicemente un'origine in cui risiede l'account di identità finale (computer o utente) utilizzato durante la fase di autenticazione ISE. Active Directory viene in genere utilizzato per supportare l'autenticazione computer con l'account computer e/o l'autenticazione utente con l'account utente finale in Active Directory. L'origine degli endpoint interni (interna) non memorizza l'account computer/nome host, pertanto non può essere utilizzata con l'autenticazione del computer.

Di seguito sono elencate le origini identità supportate con ISE e i protocolli (tipo di autenticazione) che possono essere utilizzati con ciascuna origine identità:

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

Funzionalità archivio identità

Per ulteriori informazioni sugli elementi dei criteri, consultare il *Cisco Identity Services Engine Administrator Guide, Release 3.1 > Capitolo: Segmentazione >* [Set di criteri](#).

Aggiungi gruppi di sicurezza Active Directory ad ISE

Per utilizzare i gruppi di sicurezza di Active Directory nei criteri ISE, è necessario innanzitutto aggiungere il gruppo al punto di join di Active Directory. Dall'interfaccia grafica di ISE, scegliere **Administration > Identity Management: Active Directory > {select AD instance name / join point} > tab: Groups > Add > Select Groups From Directory**.

Per ulteriori informazioni e requisiti sull'integrazione di ISE 3.x con Active Directory, consultare il documento: *Integrazione di Active Directory con Cisco ISE 2.x*.

> **Nota:** La stessa azione è applicabile per aggiungere gruppi di sicurezza a un'istanza LDAP. Dalla GUI di ISE, selezionare **Administration > Identity Management: External Identity Sources > LDAP > *LDAP instance name* > tab: Groups > Add > Select Groups From Directory**.

Passaggio 6. Creare il profilo di autenticazione del certificato

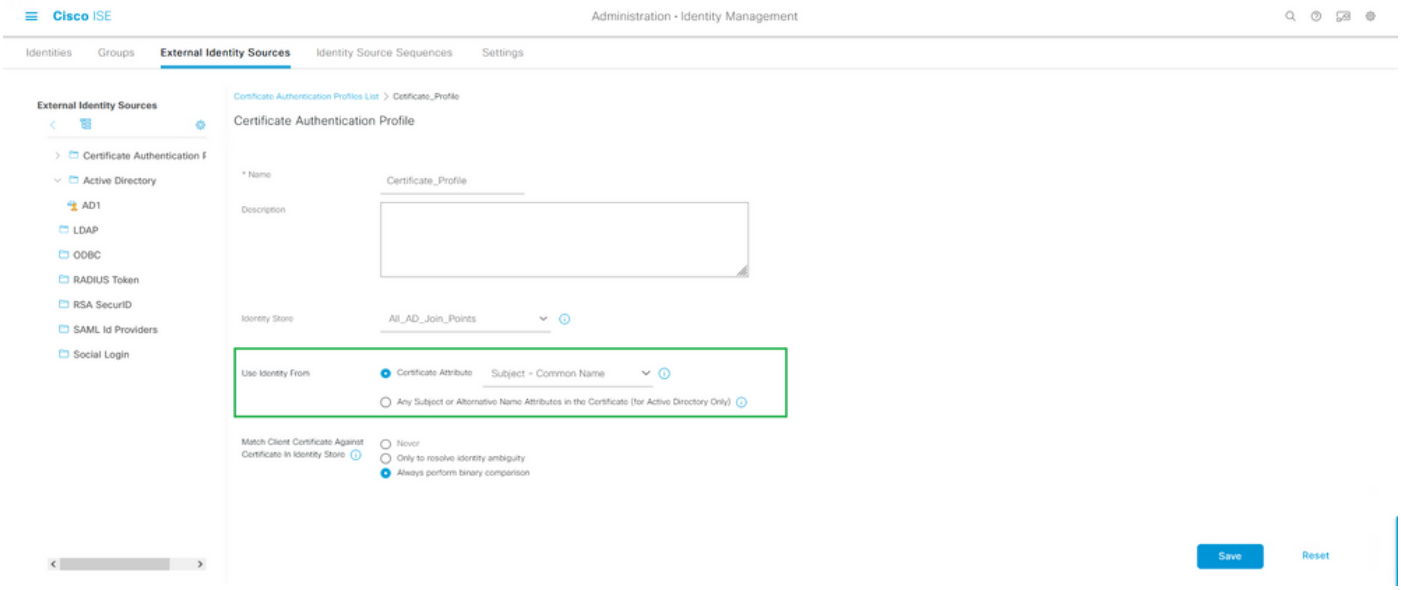
Lo scopo del profilo di autenticazione del certificato è quello di informare ISE su quale campo di certificato è possibile trovare l'identità (computer o utente) sul certificato client (certificato di identità finale) presentato ad ISE durante EAP-TLS (anche durante altri metodi di autenticazione basati sul certificato). Queste impostazioni verranno associate ai criteri di autenticazione per autenticare l'identità. Dalla GUI ISE, selezionare **Administration > Identity Management: External Identity Sources > Certificate Authentication Profile** e fare clic su **Add**.

Usa identità da consente di scegliere l'attributo del certificato da cui è possibile trovare un campo specifico per l'identità. Le opzioni sono:

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

Se l'archivio identità deve essere puntato ad Active Directory o LDAP (origine identità esterna), è possibile utilizzare una funzionalità denominata Confronto binario. Il confronto binario esegue una ricerca dell'identità in Active Directory ottenuta dal certificato client dalla selezione **Usa identità da**, che si verifica durante la fase di autenticazione ISE. Senza il confronto binario, l'identità viene ottenuta semplicemente dal certificato del client e non viene cercata in Active Directory fino alla fase di autorizzazione ISE, quando come condizione viene utilizzato un gruppo esterno di Active Directory, o a qualsiasi altra condizione che dovrebbe essere eseguita esternamente ad ISE. Per utilizzare Confronto binario, nell'**archivio identità** scegliere l'origine identità esterna (Active Directory o LDAP) in cui è possibile trovare l'account di identità finale.

Questo è un esempio di configurazione quando l'identità si trova nel campo Nome comune (CN) del certificato client, con Confronto binario abilitato (facoltativo):



Profilo di autenticazione certificato

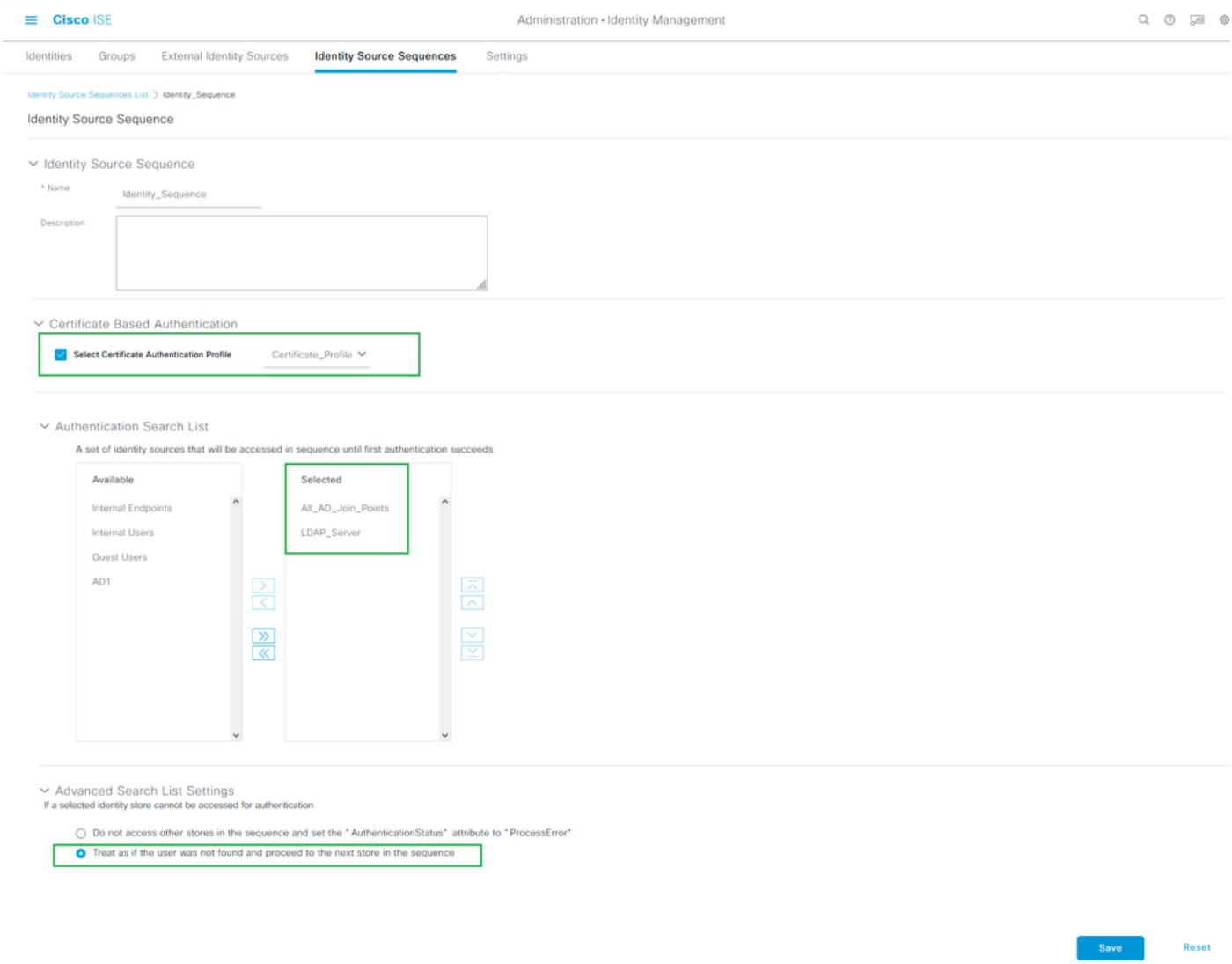
Per ulteriori informazioni, consultare il *Cisco Identity Services Engine Administrator Guide, release 3.1 > Chapter: Configurazione di base > Servizio CA Cisco ISE > Configurazione di Cisco ISE per l'utilizzo dei certificati per l'autenticazione dei dispositivi personali > Creazione di un profilo di autenticazione certificato per l'autenticazione basata su TLS*.

Passaggio 7. Aggiunta a una sequenza di origine identità

La sequenza di origine delle identità può essere creata dalla GUI di ISE. Passa a **Administration > Identity Management**. Sotto **Identity Source Sequences** , fare clic su **Add**.

Il passaggio successivo consiste nell'aggiungere il profilo di autenticazione del certificato a una sequenza di origini di identità che consente di includere più punti di join di Active Directory o di raggruppare una combinazione di origini di identità interne/esterne, in base alle esigenze, che quindi si associa al criterio di autenticazione in **Use** colonna.

L'esempio riportato di seguito consente di eseguire prima la ricerca in Active Directory, quindi se l'utente non viene trovato, verrà eseguita la ricerca in un server LDAP. Per più origini di identità. assicurarsi sempre che **Treat as if the user was not found and proceed to the next store in the sequence** è selezionata. In questo modo, ogni origine/server di identità viene controllato durante la richiesta di autenticazione.



Sequenza origine identità

In caso contrario, è inoltre possibile associare solo il profilo di autenticazione certificato ai criteri di autenticazione.

Passaggio 8. Definizione del servizio Protocolli consentiti

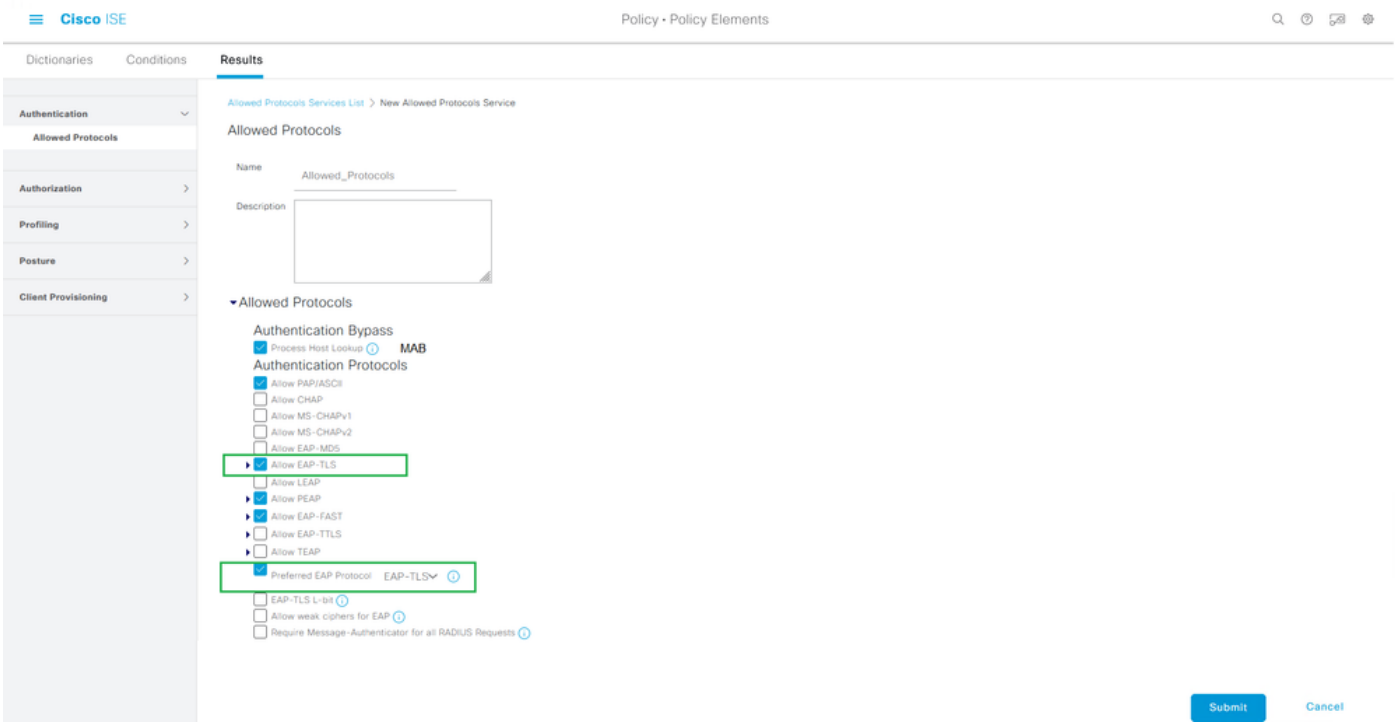
Il servizio Protocolli consentiti abilita solo i metodi/protocolli di autenticazione supportati da ISE durante l'autenticazione RADIUS. Per eseguire la configurazione dalla GUI di ISE, selezionare **Policy > Policy Elements: Risultati > Autenticazione > Protocolli consentiti**, quindi viene eseguito il binding come elemento al criterio di autenticazione.

> **Nota: Authentication Bypass > Process Host Lookup** fa riferimento all'opzione MAB abilitata su ISE.

Queste impostazioni devono corrispondere a quelle supportate e configurate sul supplicant (sull'endpoint). In caso contrario, il protocollo di autenticazione non verrà negoziato come previsto e la comunicazione RADIUS potrebbe non riuscire. In una configurazione ISE reale, si consiglia di abilitare qualsiasi protocollo di autenticazione utilizzato nell'ambiente in modo che ISE e il supplicant possano negoziare e autenticare secondo le previsioni.

Si tratta dei valori predefiniti (compressi) quando viene creata una nuova istanza dei servizi del protocollo consentito.

Nota: Come minimo, è necessario abilitare **EAP-TLS** dal momento che ISE e il supplicant eseguono l'autenticazione tramite EAP-TLS in questo esempio di configurazione.



Protocolli per consentire all'ISE di utilizzare la richiesta di autenticazione al richiedente dell'endpoint

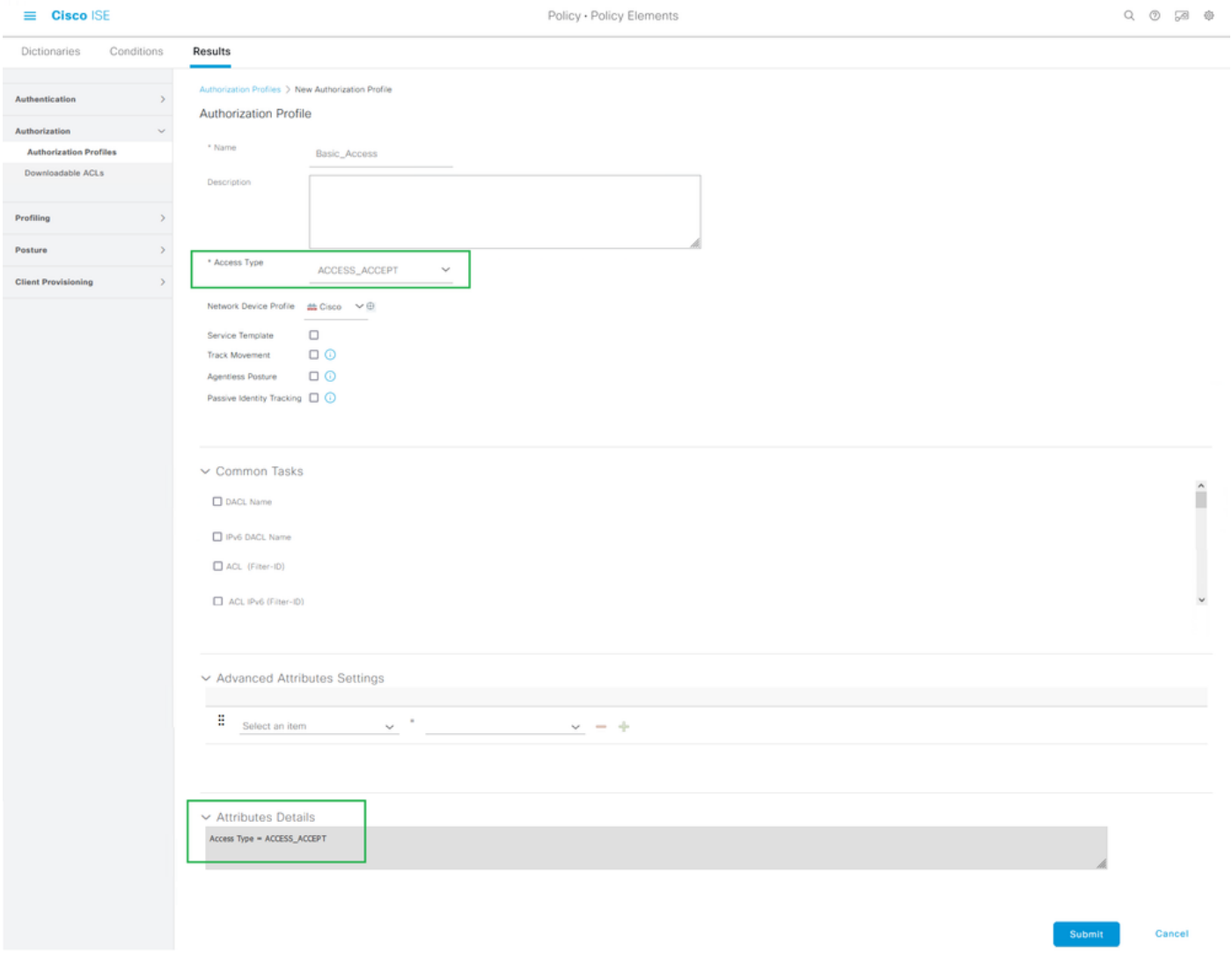
Nota: L'uso del "Protocollo EAP preferito" impostato sul valore "EAP-TLS" farà sì che ISE richieda il protocollo EAP-TLS come primo protocollo offerto al supplicant IEEE 802.1x dell'endpoint. Questa impostazione è utile se si intende eseguire l'autenticazione tramite EAP-TLS spesso sulla maggior parte degli endpoint che verranno autenticati con ISE.

Passaggio 9. Creazione del profilo di autorizzazione

L'ultimo elemento dei criteri da compilare è il profilo di autorizzazione, che si associa al criterio di autorizzazione e fornisce il livello di accesso desiderato. Il profilo di autorizzazione è associato al criterio di autorizzazione. Per configurarla dall'interfaccia utente di ISE, passare alla sezione **Policy > Policy Elements: Results > Authorization > Authorization Profiles** e fare clic su **Add**.

Il profilo di autorizzazione contiene una configurazione che determina gli attributi che vengono passati da ISE al NAD per una determinata sessione RADIUS, in cui questi attributi vengono utilizzati per raggiungere il livello di accesso alla rete desiderato.

Come mostrato di seguito, l'autenticazione passa semplicemente l'autorizzazione di accesso RADIUS come **tipo di accesso**; tuttavia, è possibile utilizzare elementi aggiuntivi dopo l'autenticazione iniziale. Si noti **Attribute Details** (Dettagli attributi) nella parte inferiore, contenente il riepilogo degli attributi inviati da ISE al NAD quando corrisponde a un determinato profilo di autorizzazione.



Profilo autorizzazione - Elemento criterio

Per ulteriori informazioni sul profilo di autorizzazione e la policy ISE, consultare il *manuale Cisco Identity Services Engine Administrator Guide, release 3.1 > capitolo: Segmentazione > Criteri di autorizzazione*.

Criteri di sicurezza

I criteri di autenticazione e autorizzazione vengono creati dalla GUI di ISE, selezionare **Policy > Policy Sets**. Queste funzionalità sono abilitate per impostazione predefinita in ISE 3.x. Quando si installa ISE, viene sempre definito un set di criteri, che è il set di criteri predefinito. Il set di criteri predefinito contiene regole predefinite e predefinite per l'autenticazione, l'autorizzazione e le eccezioni.

I Policy Set sono configurati in modo gerarchico, il che consente all'amministratore ISE di raggruppare criteri simili, in termini di finalità, in set diversi da utilizzare all'interno di una richiesta di autenticazione. Le regole di personalizzazione e raggruppamento sono praticamente illimitate. Pertanto, è possibile utilizzare un set di criteri per l'autenticazione degli endpoint wireless per l'accesso alla rete, mentre un altro set di criteri per l'autenticazione degli endpoint cablati per l'accesso alla rete. o per qualsiasi altro modo unico e differenziante di gestire le regole.

Cisco ISE valuterà i set di criteri e i criteri all'interno utilizzano l'approccio dall'alto verso il basso, in modo da corrispondere prima a un determinato set di criteri quando tutte le condizioni di tale set valutano che è True; in base a cui ISE valuta ulteriormente i criteri di autenticazione e i criteri di

autorizzazione che corrispondono al set di criteri, come indicato di seguito:

1. Valutazione del set di criteri e delle relative condizioni
2. Criteri di autenticazione nel set di criteri corrispondente
3. Criteri di autorizzazione - Eccezioni locali
4. Criteri di autorizzazione - Eccezioni globali
5. Criteri di autorizzazione

Le eccezioni dei criteri esistono globalmente per tutti i set di criteri o localmente all'interno di un set di criteri specifico. Queste eccezioni dei criteri vengono gestite come parte dei criteri di autorizzazione, poiché riguardano le autorizzazioni o i risultati forniti per l'accesso alla rete per un determinato scenario temporaneo.

La sezione successiva illustra come combinare gli elementi di configurazione e policy con il binding alle policy di autenticazione e autorizzazione ISE per autenticare un endpoint tramite EAP-TLS.

Passaggio 10. Creazione del set di criteri

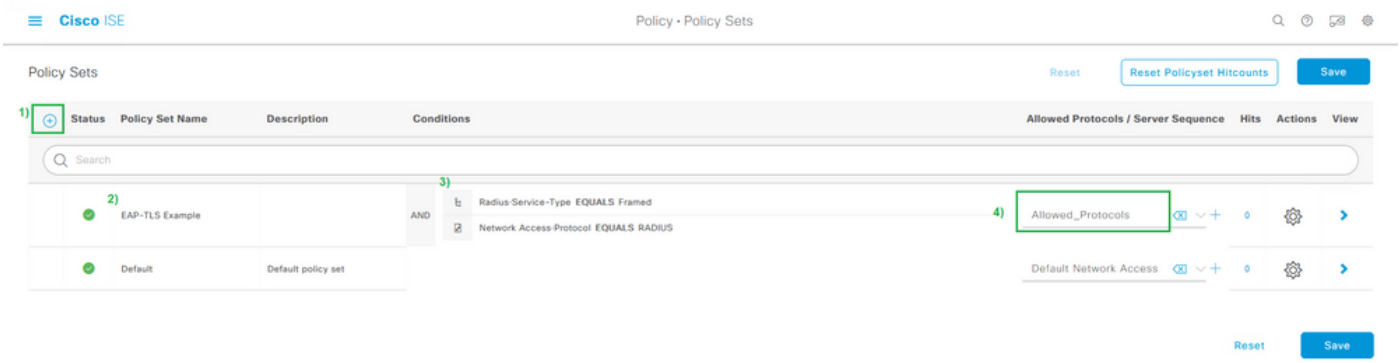
Un set di criteri è un contenitore gerarchico costituito da una singola regola definita dall'utente che indica il protocollo o la sequenza di server consentiti per l'accesso alla rete, nonché i criteri di autenticazione e autorizzazione e le eccezioni dei criteri, tutti configurati con regole basate su condizioni definite dall'utente.

Per creare un set di criteri dall'interfaccia utente di ISE, selezionare **Policy > Policy Set** quindi fare clic sul pulsante più (**+**) nell'angolo superiore sinistro, come mostrato nell'immagine.

Aggiunta di un nuovo set di criteri

Il set di criteri associa/combina questo elemento di criteri configurato in precedenza e viene utilizzato per determinare il set di criteri da abbinare in una determinata richiesta di autenticazione RADIUS (Access-Request):

- Associa: Servizi per protocolli consentiti



Definizione delle condizioni del set di criteri e dell'elenco dei protocolli consentiti

In questo esempio vengono utilizzati attributi e valori specifici che verrebbero visualizzati nella sessione RADIUS per applicare IEEE 802.1x (attributo framed), anche se è possibile che sia

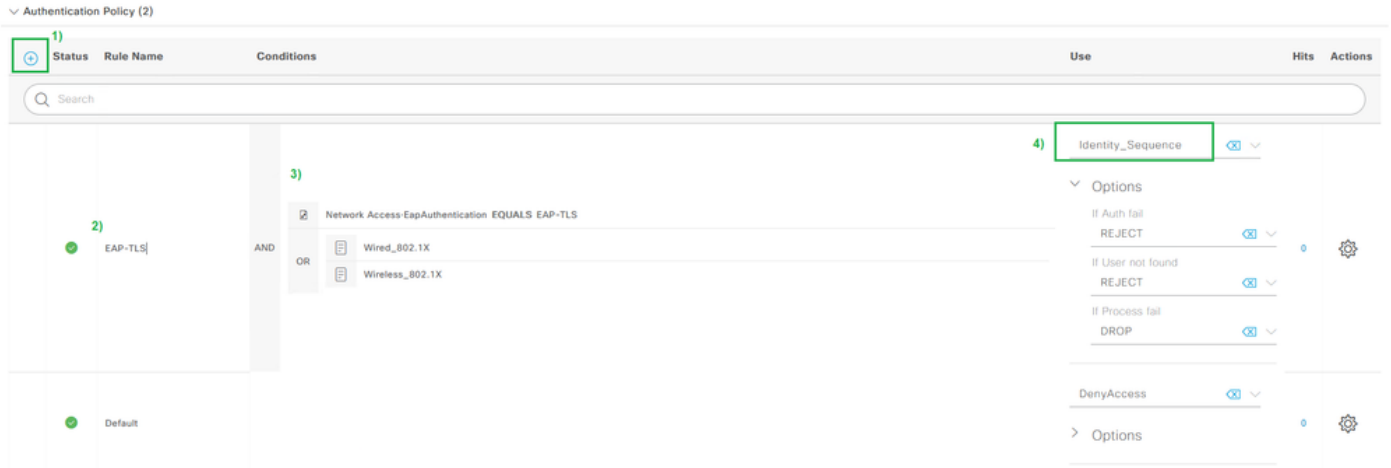
ridondante rafforzare il protocollo RADIUS. Per ottenere risultati ottimali, utilizzare solo attributi di sessione RADIUS univoci applicabili all'intento desiderato, ad esempio Gruppi di dispositivi di rete o specifici per Wired 802.1x, Wireless 802.1x o Wired 802.1x e Wireless 802.1x.

Per ulteriori informazioni sui set di criteri per ISE, consultare la *Guida dell'amministratore di Cisco Identity Services Engine, Release 3.1 > Capitolo: Segmentazione >* [Set di criteri](), [Criteri di autenticazione]() *e sezioni* [Criteri di autorizzazione]().

Passaggio 11. Creazione di un criterio di autenticazione

All'interno del set di criteri, il criterio di autenticazione associa/combina questi elementi di criteri configurati in precedenza per l'utilizzo con condizioni per determinare quando una regola di autenticazione deve essere soddisfatta.

- Associa: Profilo di autenticazione certificato o sequenza di origine identità.

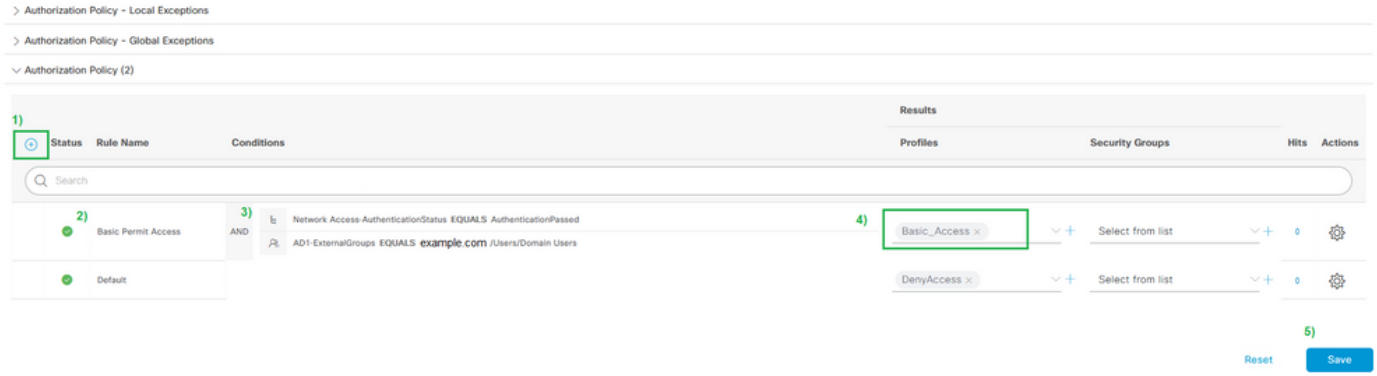


Esempio di regola dei criteri di autenticazione

Passaggio 12. Creazione dei criteri di autorizzazione

All'interno del set di criteri, il criterio di autorizzazione associa/combina questi elementi di criteri configurati in precedenza per l'utilizzo con condizioni per determinare quando una regola di autorizzazione deve essere soddisfatta. L'esempio riportato di seguito riguarda l'**autenticazione utente** poiché le condizioni fanno riferimento al gruppo di sicurezza **Domain Users** in Active Directory.

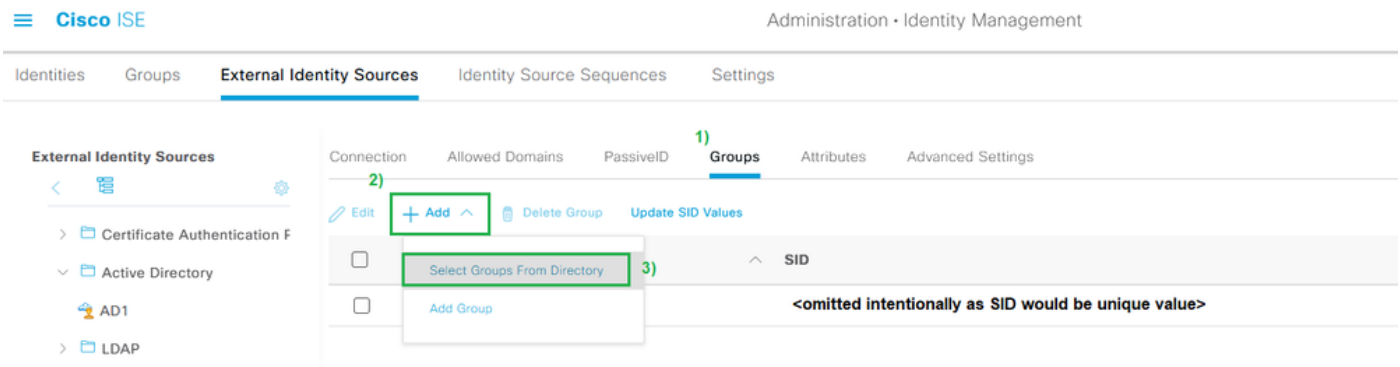
- Associa: Profilo di autorizzazione



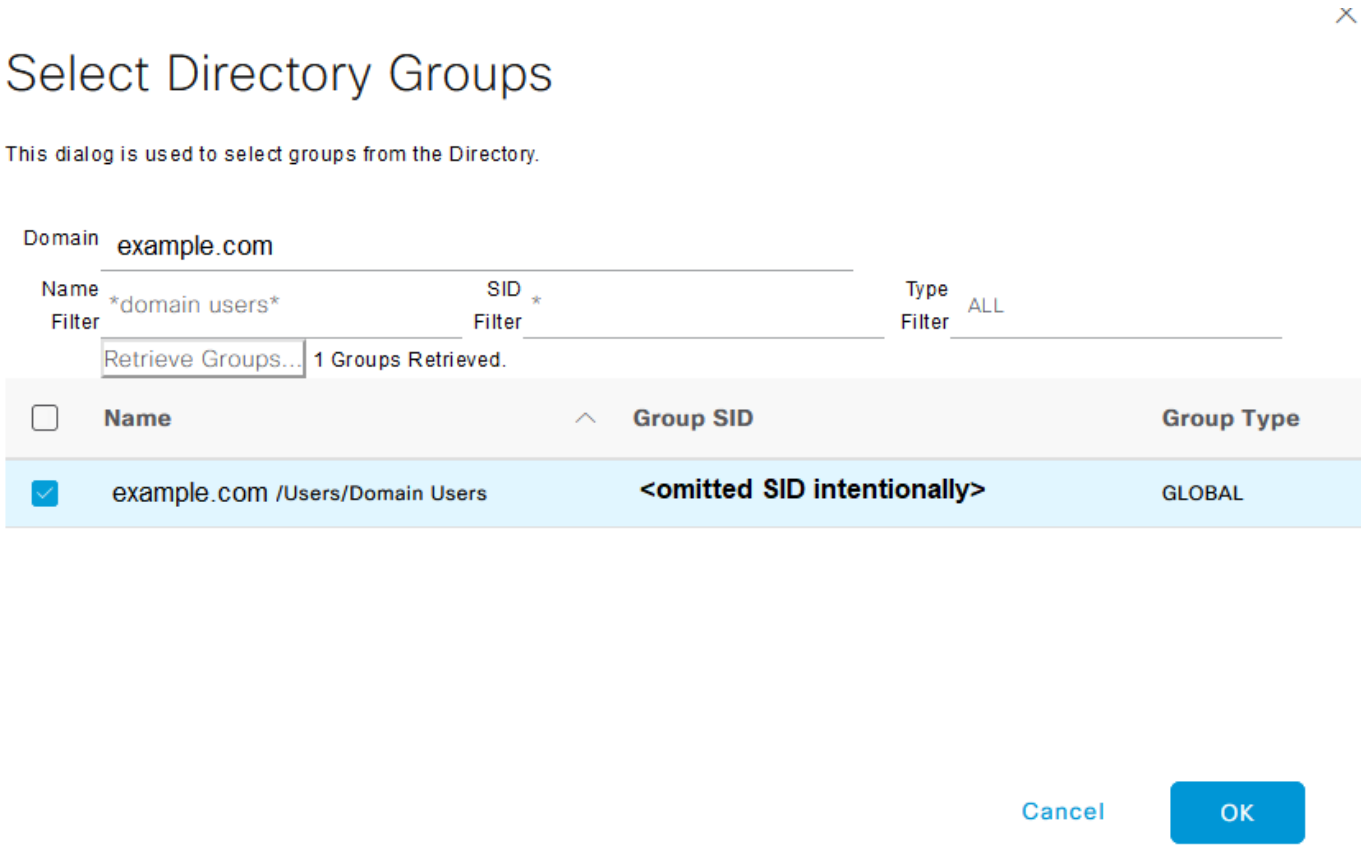
Esempio di regola dei criteri di autorizzazione

Per aggiungere un gruppo esterno, ad esempio da Active Directory o LDAP, è necessario aggiungere il gruppo dall'istanza del server esterno. Nell'esempio, verrà generato dall'interfaccia

utente di ISE: **Administration > Identity Management: External Identity Sources > Active Directory {AD Join Point Name} > Groups**. Nella scheda Gruppo scegliere **Add > Select Groups from Directory** e utilizzare il filtro Nome per cercare tutti i gruppi (*) o gruppi specifici, ad esempio Utenti del dominio (*utenti del dominio*) per recuperare i gruppi.



Per usare i gruppi esterni nei criteri ISE, aggiungere un gruppo dalla directory



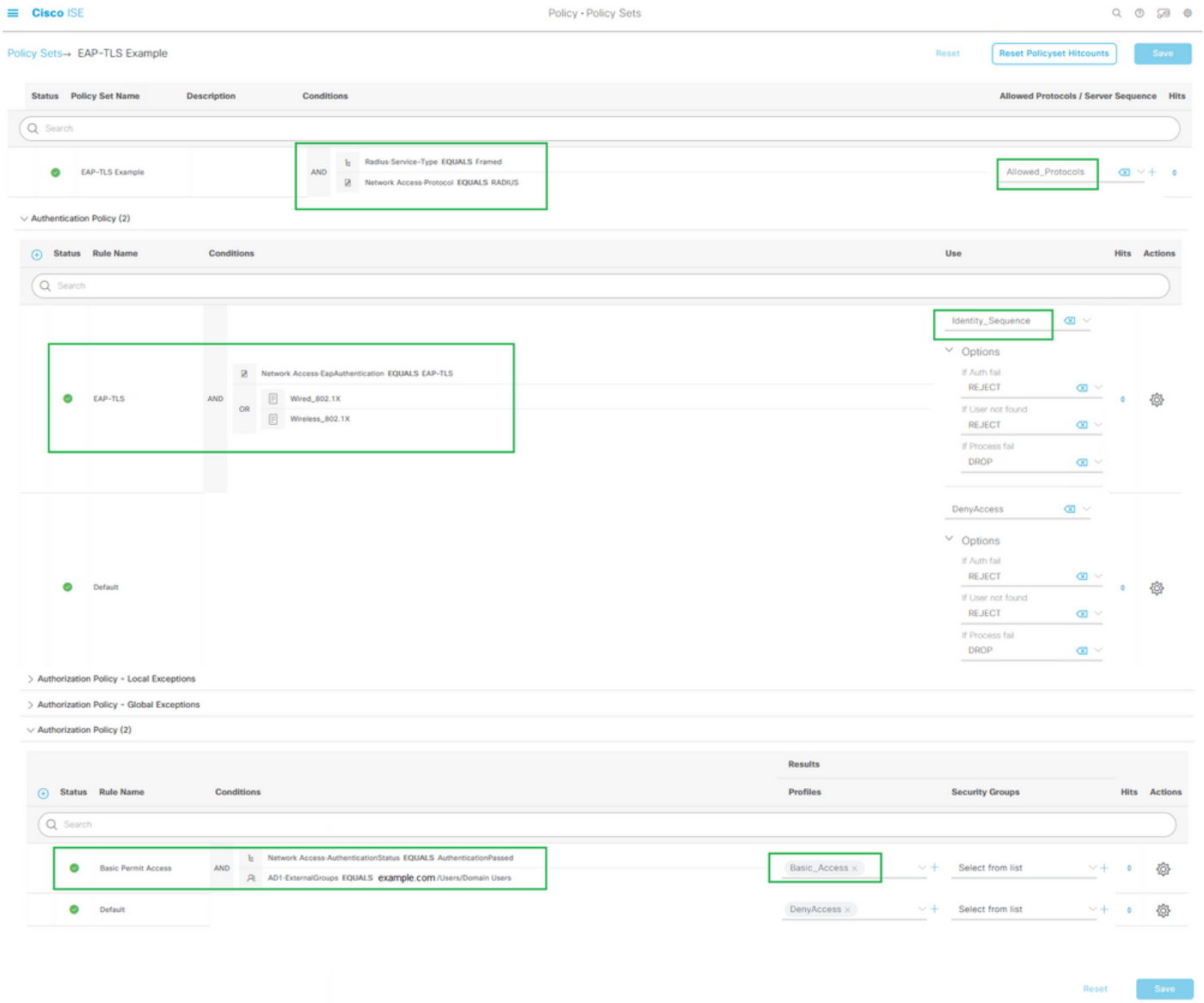
Ricerca nella directory esterna - Esempio di Active Directory

Dopo aver selezionato la casella di controllo accanto a ciascun gruppo che si desidera utilizzare nelle Policies (Regolamenti) di ISE, non dimenticare di fare clic su **Ok** e/o su **Salva** per salvare le modifiche.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Una volta che tutti gli elementi di configurazione e criteri globali hanno associato il set di criteri, la configurazione è simile a questa immagine per l'autenticazione utente tramite EAP-TLS:

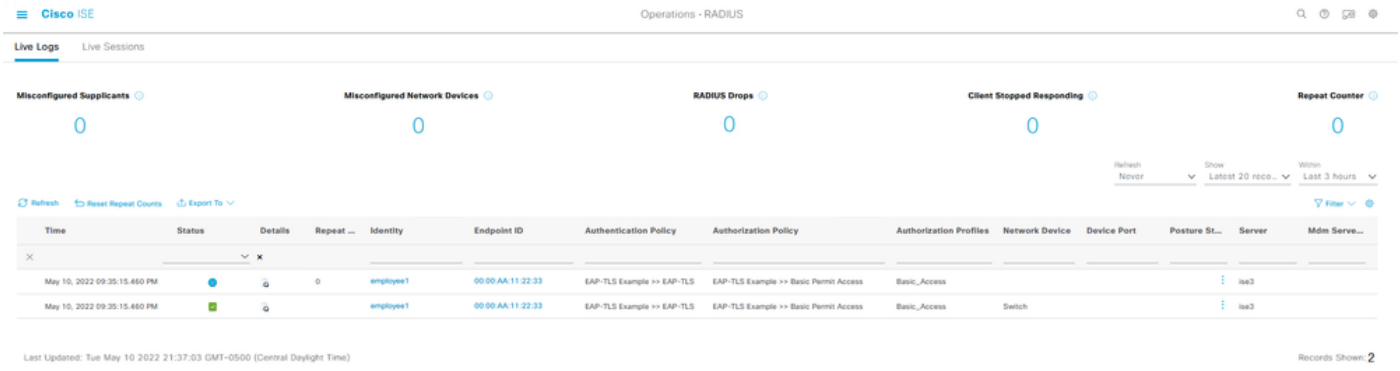


Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Al termine della configurazione, connettere l'endpoint per verificare l'autenticazione. I risultati sono disponibili nella GUI di ISE. Scegli **Operations > Radius > Live Logs**, come mostrato nell'immagine.

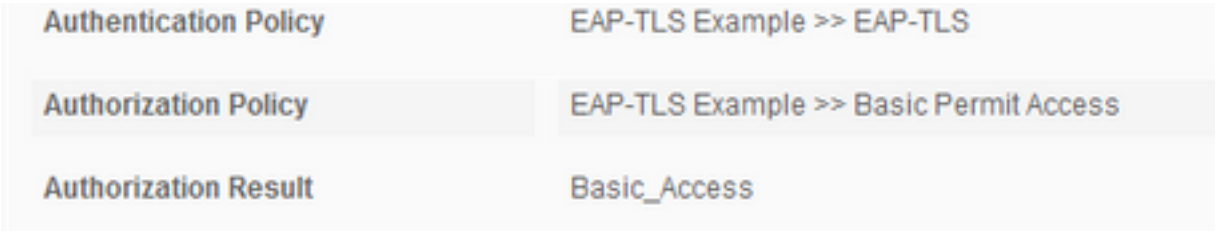
Per maggiore consapevolezza, i Live Log per RADIUS e TACACS+ (Device Admin) sono disponibili per i tentativi di autenticazione e le attività eseguite fino alle ultime 24 ore e per gli ultimi 100 record. Se si desidera visualizzare questo tipo di dati di report oltre questo intervallo di tempo, sarà necessario utilizzare i report, in particolare: **ISE UI: Operations > Reports > Reports: Endpoints and Users > RADIUS Authentications**.



Live Logs" />*Output di esempio da Radius > Live Logs*

In RADIUS Live Logs in ISE ci si aspetta di trovare informazioni sulla sessione RADIUS, che includono attributi della sessione, e altre informazioni utili per diagnosticare il comportamento osservato durante un flusso di autenticazione. Fare clic sul pulsante **details** per aprire la vista dettagliata della sessione e visualizzare gli attributi della sessione e le informazioni correlate specifiche di questo tentativo di autenticazione.

Per risolvere i problemi, è importante verificare che siano soddisfatti i criteri corretti. Per questo esempio di configurazione i criteri di autenticazione e autorizzazione desiderati vengono associati come previsto, come mostrato nell'immagine:



Nella vista dettagliata, questi attributi vengono controllati per verificare che l'autenticazione funzioni come previsto dal progetto come parte di questo esempio di configurazione:

- **Evento**
  Indica se l'autenticazione è riuscita o meno.In uno scenario di lavoro il valore è: **Autenticazione 5200 riuscita**.

- **Username**
  inclusa l'identità finale estratta dal certificato client presentato ad ISE.In uno scenario di lavoro, questo è il nome utente dell'utente connesso all'endpoint, ovvero employee1 dall'immagine precedente.

- **ID endpoint**
  Per Wired/Wireless, questo valore corrisponde all'indirizzo MAC della scheda di interfaccia di rete (NIC) dell'endpoint.In uno scenario di lavoro, questo indirizzo diventa l'indirizzo MAC dell'endpoint a meno che la connessione non sia su VPN, nel qual caso potrebbe essere l'indirizzo IP dell'endpoint.

- **Criteri di autenticazione**
  Mostra i criteri di autenticazione corrispondenti per la sessione specificata in base agli attributi della sessione che soddisfano le condizioni dei criteri.In uno scenario di lavoro, questo è il criterio di autenticazione previsto come configurato.Se viene visualizzato un altro

criterio, significa che il criterio previsto non è stato valutato come vero rispetto alle condizioni del criterio. In questo caso, esaminare gli attributi della sessione e verificare che ogni criterio contenga condizioni diverse ma univoche per ogni criterio.

- **Criteri di autorizzazione**
  Mostra il criterio di autorizzazione corrispondente per la sessione specificata in base agli attributi della sessione che soddisfano le condizioni del criterio.In uno scenario di lavoro, questo è il criterio di autorizzazione previsto configurato.Se viene visualizzato un altro criterio, significa che il criterio previsto non è stato valutato come vero rispetto alle condizioni del criterio. In questo caso, esaminare gli attributi della sessione e verificare che ogni criterio contenga condizioni diverse ma univoche per ogni criterio.

- **Risultato autorizzazione**
  In base al criterio di autorizzazione corrispondente, mostra il profilo di autorizzazione utilizzato nella sessione specificata.In uno scenario di lavoro, questo valore corrisponde a quello configurato nel criterio. È consigliabile eseguire l'analisi a scopo di audit e verificare che sia stato configurato il profilo di autorizzazione corretto.

- **Policy Server**
  Incluso il nome host del PSN (Policy Service Node) di ISE coinvolto nel tentativo di autenticazione.In uno scenario di lavoro, è possibile visualizzare solo le autenticazioni che passano al primo nodo PSN come configurato nel NAD (noto anche come dispositivo perimetrale), a meno che il PSN non sia stato operativo o se si è verificato il failover, ad esempio a causa di una latenza maggiore del previsto o se si verifica un timeout di autenticazione.

- **Metodo di autenticazione**
  Mostra il metodo di autenticazione utilizzato nella sessione specificata. In questo esempio il valore visualizzato è **dot1x**.In uno scenario di lavoro basato su questo esempio di configurazione, il valore visualizzato è **dot1x**. Se viene visualizzato un altro valore, è possibile che dot1x non sia riuscito o che non sia stato tentato.

- **Protocollo di autenticazione**
  Mostra il metodo di autenticazione utilizzato nella sessione specificata. In questo esempio, il valore è "EAP-TLS".In uno scenario di lavoro, basato su questo esempio di configurazione, il valore viene sempre visualizzato come "EAP-TLS". Se viene visualizzato un altro valore, il supplicant e ISE non sono riusciti a negoziare EAP-TLS.

- **Dispositivo di rete**
  Mostra il nome del dispositivo di rete, configurato in ISE, per il dispositivo NAD (noto anche come dispositivo perimetrale) coinvolto nel tentativo di autenticazione tra l'endpoint e ISE.In uno scenario di lavoro, questo nome viene sempre assegnato nell'interfaccia utente ISE: **Administration > System: Network Devices.** In base a tale configurazione, l'indirizzo IP del NAD (noto anche come dispositivo perimetrale) viene utilizzato per determinare da quale dispositivo di rete proviene l'autenticazione e che è incluso nell'attributo di sessione **Indirizzo IPv4 NAS**.

In nessun caso si tratta di un elenco completo di tutti gli attributi di sessione possibili da esaminare per la risoluzione dei problemi o altri scopi di visibilità, in quanto vi sono altri attributi utili da verificare. Si consiglia di esaminare tutti gli attributi della sessione per iniziare a familiarizzare con

tutte le informazioni. È possibile vedere di includere la parte destra sotto la sezione **Passi**, che mostra le operazioni o il comportamento assunto dall'ISE.

Problemi comuni e tecniche di risoluzione dei problemi

L'elenco include alcuni problemi comuni e consigli per la risoluzione dei problemi e non deve assolutamente essere un elenco completo. Invece, utilizza questa guida per sviluppare le tue tecniche per risolvere i problemi quando è coinvolto ISE.

Problema: Errore di autenticazione (**autenticazione 5400 non riuscita**) o qualsiasi altro tentativo di autenticazione non riuscito.

- Se si verifica un errore di autenticazione, fare clic sull'icona **dei dettagli** che fornisce informazioni sul motivo dell'errore di autenticazione e sui passaggi eseguiti. Ciò include il motivo dell'errore e la possibile causa principale.

- Poiché ISE decide sul risultato dell'autenticazione, avrà le informazioni per capire la ragione per cui il tentativo di autenticazione non è riuscito.

Problema: L'autenticazione non viene completata correttamente e il motivo dell'errore indica "5440 Endpoint abbandonato sessione EAP e avviato nuovo" o "5411 Supplicant smesso di rispondere ad ISE".

- Questo motivo indica che la comunicazione RADIUS non è stata completata prima del timeout. Poiché EAP si trova tra l'endpoint e NAD, è necessario verificare il timeout utilizzato in NAD e verificare che sia impostato per almeno cinque secondi.

- Se cinque secondi non sono sufficienti per risolvere il problema, si consiglia di aumentarli di cinque secondi alcune volte e di ripetere il test per verificare se questa tecnica risolverà il problema.

- Se il problema non viene risolto nei passaggi precedenti, è consigliabile verificare che l'autenticazione venga gestita dallo stesso nodo PSN ISE corretto e che il comportamento complessivo non indichi comportamenti anomali, ad esempio una latenza superiore alla normale tra i nodi PSN NAD e ISE.

- Inoltre, è consigliabile verificare se l'endpoint invia il certificato client tramite l'acquisizione pacchetti se ISE non riceve il certificato client, l'endpoint (certificati utente) potrebbe non considerare attendibile il certificato di autenticazione ISE EAP. Se il valore è true, importare la catena di CA negli archivi certificati corretti (CA radice = CA radice attendibile) | CA intermediaria = CA intermediaria di fiducia).

Problema: L'autenticazione è riuscita, ma non corrisponde al criterio di autenticazione e/o autorizzazione corretto.

- Se si verifica una richiesta di autenticazione riuscita, ma che non soddisfa le regole di autenticazione e/o autorizzazione corrette, è consigliabile esaminare gli attributi della sessione per verificare che le condizioni utilizzate siano accurate e presenti nella sessione RADIUS.

- ISE valuta queste policy da un approccio top-down (ad eccezione delle policy di postura). È innanzitutto necessario determinare se il criterio corrispondente è superiore o inferiore al criterio desiderato. I criteri di autenticazione vengono valutati per primi e indipendentemente dai criteri di autorizzazione. Se il criterio di autenticazione corrisponde correttamente, significa che l'**autenticazione 22037 è stata superata** nella sezione **Passaggi** nella sezione a destra di Dettagli autenticazione.

- Se il criterio desiderato è superiore al criterio corrispondente, significa che la somma delle condizioni del criterio desiderato non è risultata vera. Vengono esaminati tutti gli attributi e i valori nella condizione e nella sessione per verificare che esista e che non sia presente alcun errore ortografico.

- Se il criterio desiderato è inferiore al criterio corrispondente, significa che è stato trovato un altro criterio (sopra) anziché il criterio desiderato. È possibile che i valori delle condizioni non siano sufficientemente specifici, che le condizioni siano duplicate in un altro criterio o che l'ordine del criterio non sia corretto. Anche se la risoluzione dei problemi diventa più difficile, è consigliabile iniziare a rivedere i criteri per determinare il motivo per cui non è stata trovata una corrispondenza con i criteri desiderati. Ciò consente di identificare le azioni da intraprendere successivamente.

Problema: Il valore dell'identità o del nome utente utilizzato durante l'autenticazione non è quello previsto.

- In questo caso, se l'endpoint invia il certificato client, molto probabilmente ISE non utilizza il campo del certificato corretto nel modello di autenticazione del certificato; valutata durante la fase di autenticazione.

- Esaminare il certificato client per individuare il campo esatto dell'identità/nome utente desiderato e verificare che lo stesso campo sia selezionato da: **ISE UI: Administration > Identity Management: External Identity Sources > Certificate Authentication Profile > (certificate authentication profile used in the Authentication Policy).**

Problema: Autenticazione non riuscita. Motivo dell'errore "**Handshake SSL/TLS 12514 EAP-TLS non riuscito a causa di un'autorità di certificazione sconosciuta nella catena di certificati del client**".

- Questo problema può verificarsi se il certificato client include un certificato nella catena CA non attendibile nell'interfaccia utente ISE: **Administration > System: Certificates > Trusted Certificates.**

- Questa situazione si può verificare in genere quando il certificato client (sull'endpoint) ha una catena di CA diversa da quella firmata per l'autenticazione EAP ad ISE.

- Per la risoluzione, verificare che la catena di CA dei certificati client sia attendibile su ISE e che la catena di CA dei certificati del server di autenticazione EAP ISE sia attendibile sull'endpoint.
  - Per Windows OS e Chrome, passare a **Start > Run MMC > Add/Remove Snap-In > Certificates > User Certificates.**

- Per Firefox: Importare la catena CA (non il certificato di identità finale) da considerare attendibile per il server Web.

Informazioni correlate

- Cisco Identity Services Engine > Guide all'installazione e all'aggiornamento
- Cisco Identity Services Engine > Guide alla configurazione
- Cisco Identity Services Engine > Informazioni sulla compatibilità
- Cisco Identity Services Engine Administrator Guide, release 3.1 > Capitolo: Secure Access > Definizione dei dispositivi di rete in Cisco ISE
- Cisco Identity Services Engine Administrator Guide, release 3.1 > Capitolo: Segmentazione > Set di criteri
- Cisco Identity Services Engine Administrator Guide, release 3.1 > Capitolo: Segmentazione > Criteri di autenticazione
- Cisco Identity Services Engine Administrator Guide, release 3.1 > Capitolo: Segmentazione > Criteri di autorizzazione
- Cisco Identity Services Engine > Guide alla configurazione > Integrazione di Active Directory con Cisco ISE 2.x
- Cisco Identity Services Engine Administrator Guide, release 3.1 > Capitolo: Segmentazione > Servizio di accesso alla rete > Accesso alla rete per gli utenti
- Cisco Identity Services Engine Administrator Guide, release 3.1 > Capitolo: Configurazione di base > Gestione certificati in Cisco ISE
- Cisco Identity Services Engine Administrator Guide, release 3.1 > Capitolo: Configurazione di base > Servizio CA Cisco ISE > Configurazione di Cisco ISE per l'utilizzo dei certificati per l'autenticazione dei dispositivi personali > Creazione di un profilo di autenticazione certificato per l'autenticazione basata su TLS
- Cisco Identity Services Engine > Esempi di configurazione e note tecniche > Configura portale di provisioning certificati ISE 2.0
- Cisco Identity Services Engine > Esempi di configurazione e note tecniche > Installa un certificato firmato da un'autorità di certificazione di terze parti in ISE
- Wireless LAN (WLAN) > Esempi di configurazione e note tecniche > Comprendere e configurare EAP-TLS con WLC e ISE
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).