Configurazione dell'autenticazione basata su certificato o smart card per l'amministrazione di ISE

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione basata su certificati client per l'accesso alla gestione di Identity Services Engine (ISE). Nell'esempio, l'amministratore ISE esegue l'autenticazione in base al certificato utente per ottenere l'accesso come amministratore alla GUI di gestione di Cisco Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione ISE per l'autenticazione di password e certificati.
- Microsoft Active Directory (AD)

Componenti usati

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

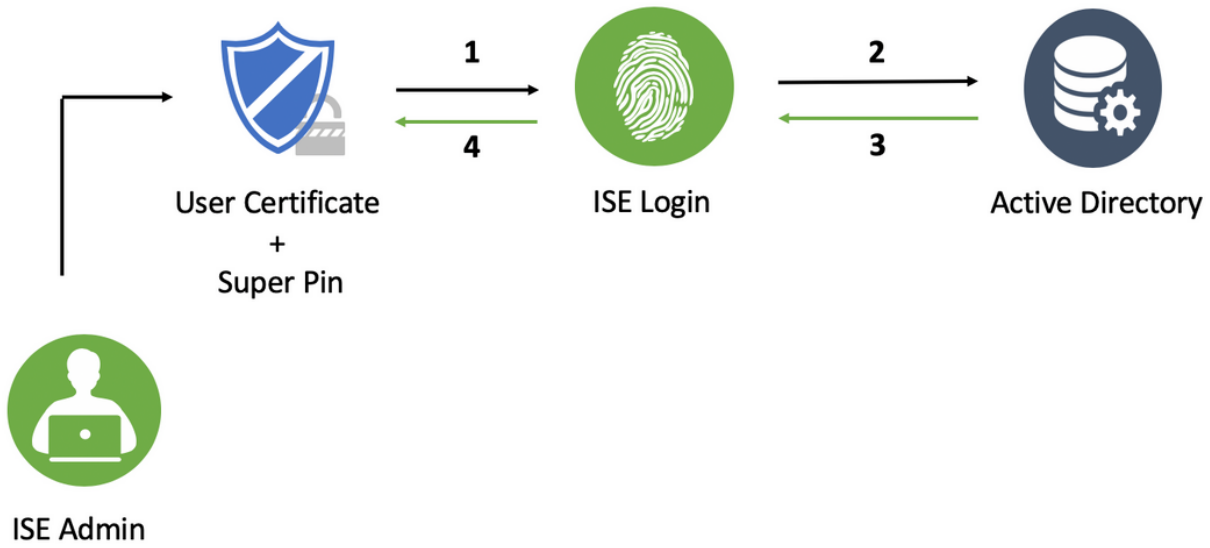
- Cisco Identity Services Engine (ISE) versione 2.6
- Windows Active Directory (AD) Server 2008 release 2
- Certificato

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 dalla configurazione.

Configurazione

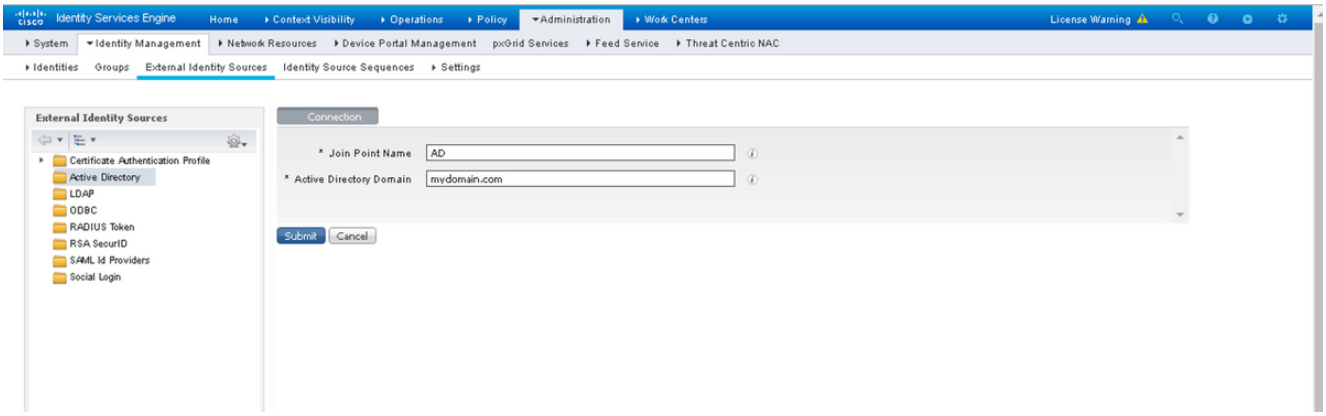
Utilizzare questa sezione per configurare il certificato client o la smart card come identità esterna per l'accesso amministrativo alla GUI di gestione di Cisco ISE.

Esempio di rete

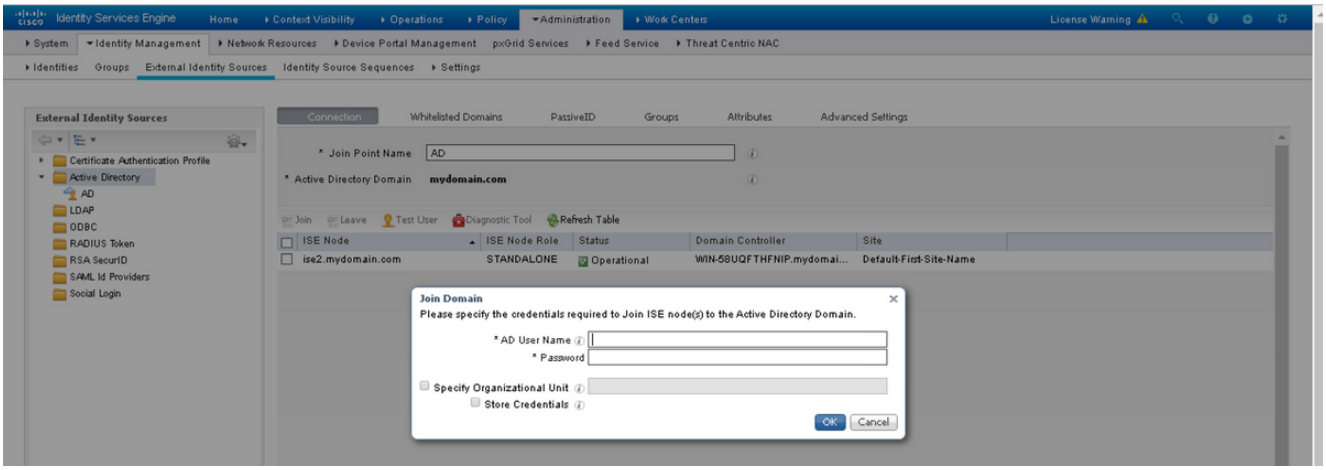


Partecipa ad ISE e Active Directory

1. Scegliere **Amministrazione > Gestione identità > Origini identità esterne > Active Directory.**
2. Creare un'istanza di Active Directory con il **nome del punto di join** e il **dominio AD** in Cisco ISE.
3. Fare clic su **Invia**.



4. Unire tutti i nodi con il **nome utente** e la **password** appropriati nel prompt.



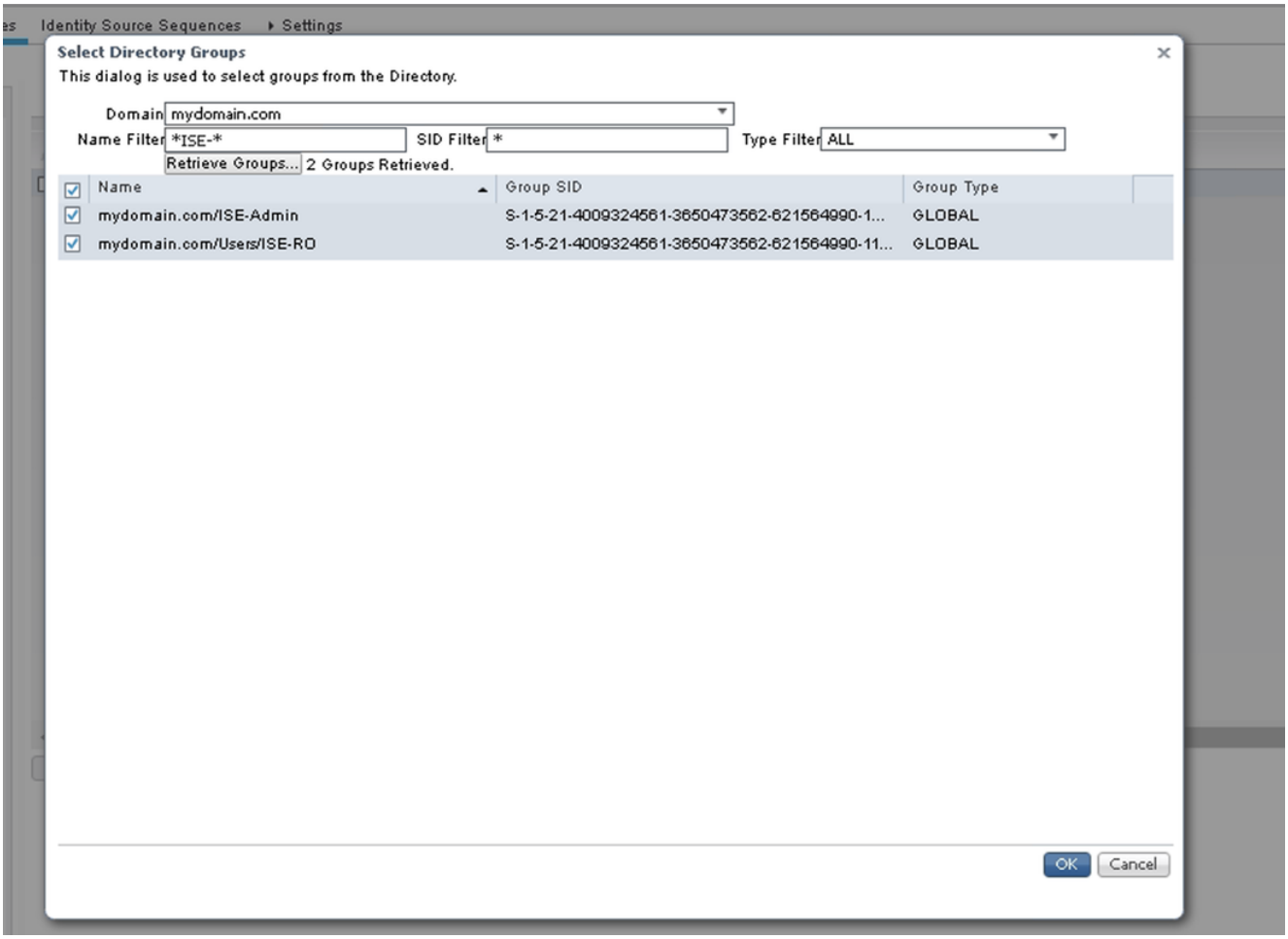
5. Fare clic su **Salva**.

Seleziona gruppi di directory

1. Creare un gruppo di amministratori esterno e mapparlo al gruppo di Active Directory.

2. Scegliere **Amministrazione >Gestione identità > Origini identità esterne > Active Directory > Gruppi > Seleziona gruppi dalla directory.**

3. Recuperare almeno un gruppo AD a cui appartiene l'amministratore.

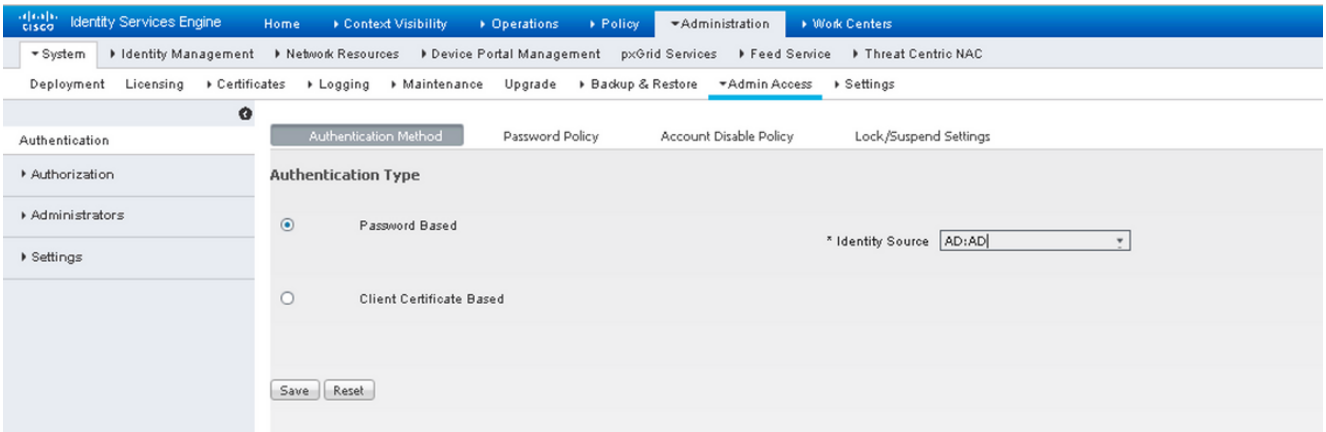


4. Fare clic su **Salva**.

Abilita autenticazione basata su password di Active Directory per l'accesso amministrativo

1. Abilitare l'istanza di Active Directory come metodo di autenticazione basato su password che è stato aggiunto ad ISE in precedenza.

2. Scegliere **Amministrazione > Sistema > Accesso amministratore > Autenticazione**, come mostrato nell'immagine.



3. Fare clic su **Salva**.

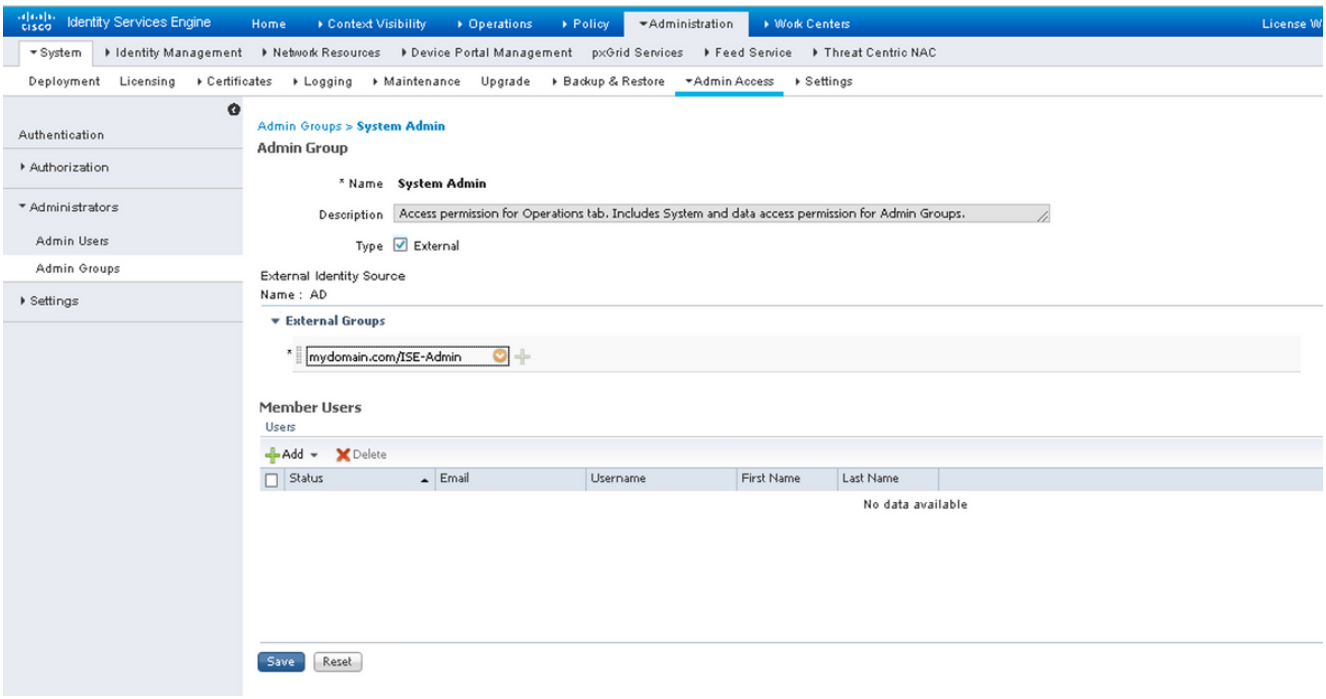
Nota: La configurazione dell'autenticazione basata su password è necessaria per abilitare l'autenticazione basata su certificati. È necessario ripristinare questa configurazione dopo aver configurato correttamente l'autenticazione basata su certificati.

Mapping dei gruppi di identità esterni ai gruppi amministrativi

In questo esempio, il gruppo AD esterno è mappato al gruppo Admin predefinito.

1. Scegliere **Amministrazione > Sistema > Accesso amministratore >Amministratori >Gruppi amministrativi > Amministratore privilegiato.**

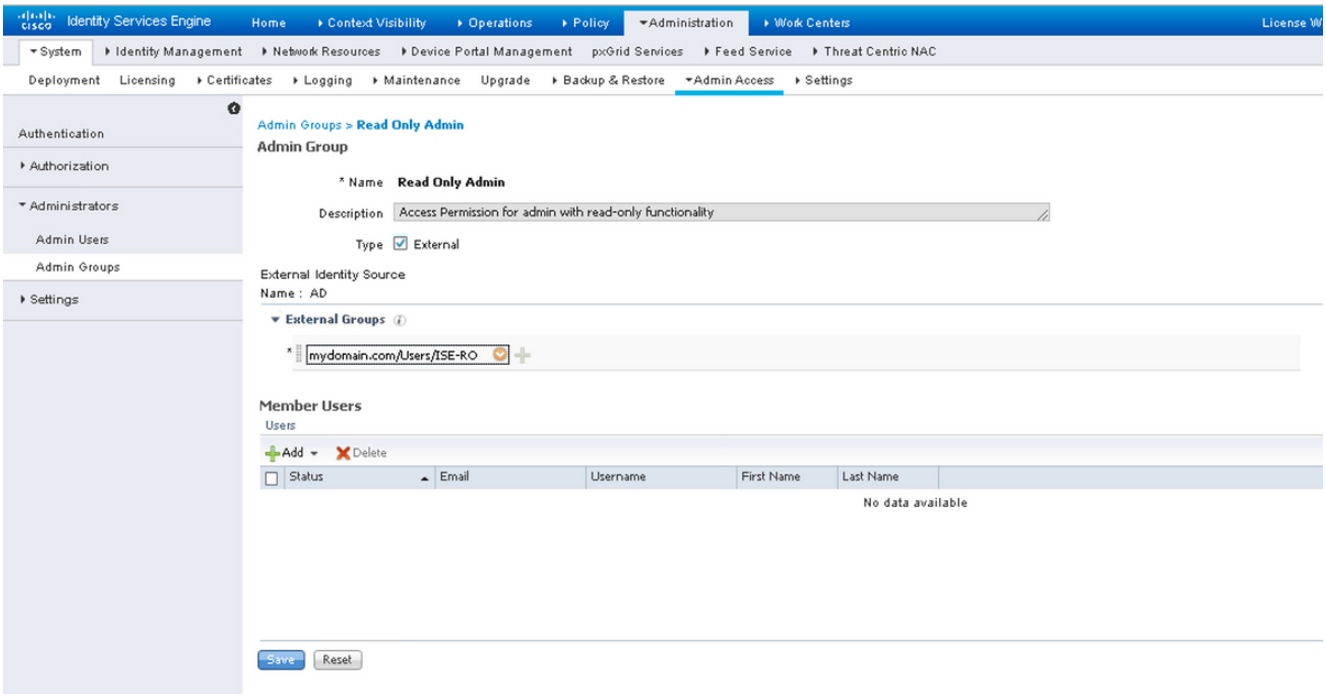
2. Selezionare l'opzione Type as **External** (Tipo come esterno) e selezionare il gruppo AD in **External groups** (Gruppi esterni).



3. Fare clic su **Salva**.

4. Scegliere **Amministrazione > Sistema > Accesso amministratore > Amministratori > Gruppi amministratori > Amministratore di sola lettura**.

5. Selezionare l'opzione Type as **External** (Tipo come esterno) e selezionare il gruppo AD in **External groups** (Gruppi esterni), come illustrato nell'immagine.



6. Fare clic su **Salva**.

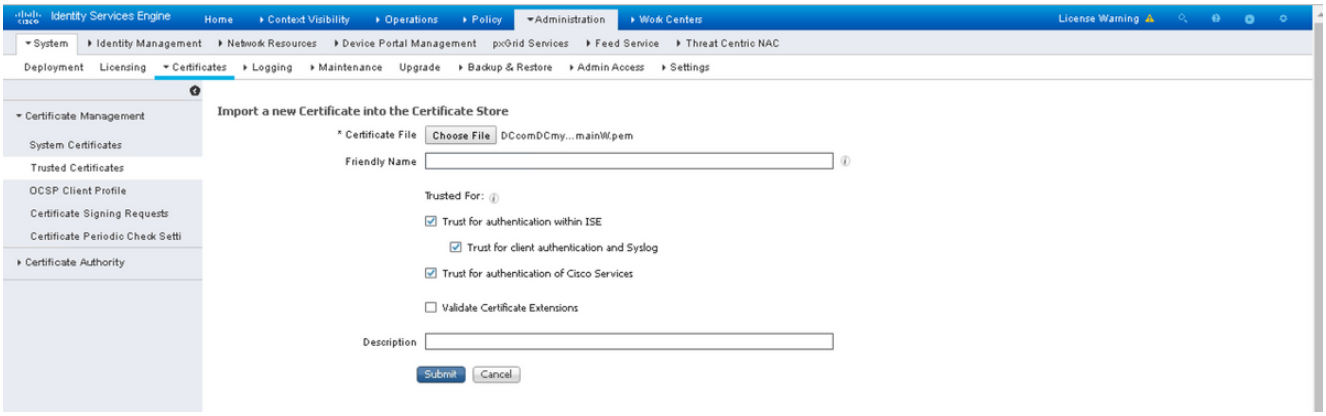
Importa certificato protetto

1. Importare il certificato dell'Autorità di certificazione (CA) che firma il certificato client.

2. Scegli **Amministratore > Sistema > Certificati > Certificato protetto > Importa.**

3. Fare clic su Sfoglia e scegliere il certificato CA.

4. Selezionare la **casella di controllo Considera attendibile l'autenticazione del client e Syslog**, come mostrato nell'immagine.



5. Fare clic su **Invia.**

Configura profilo di autenticazione certificato

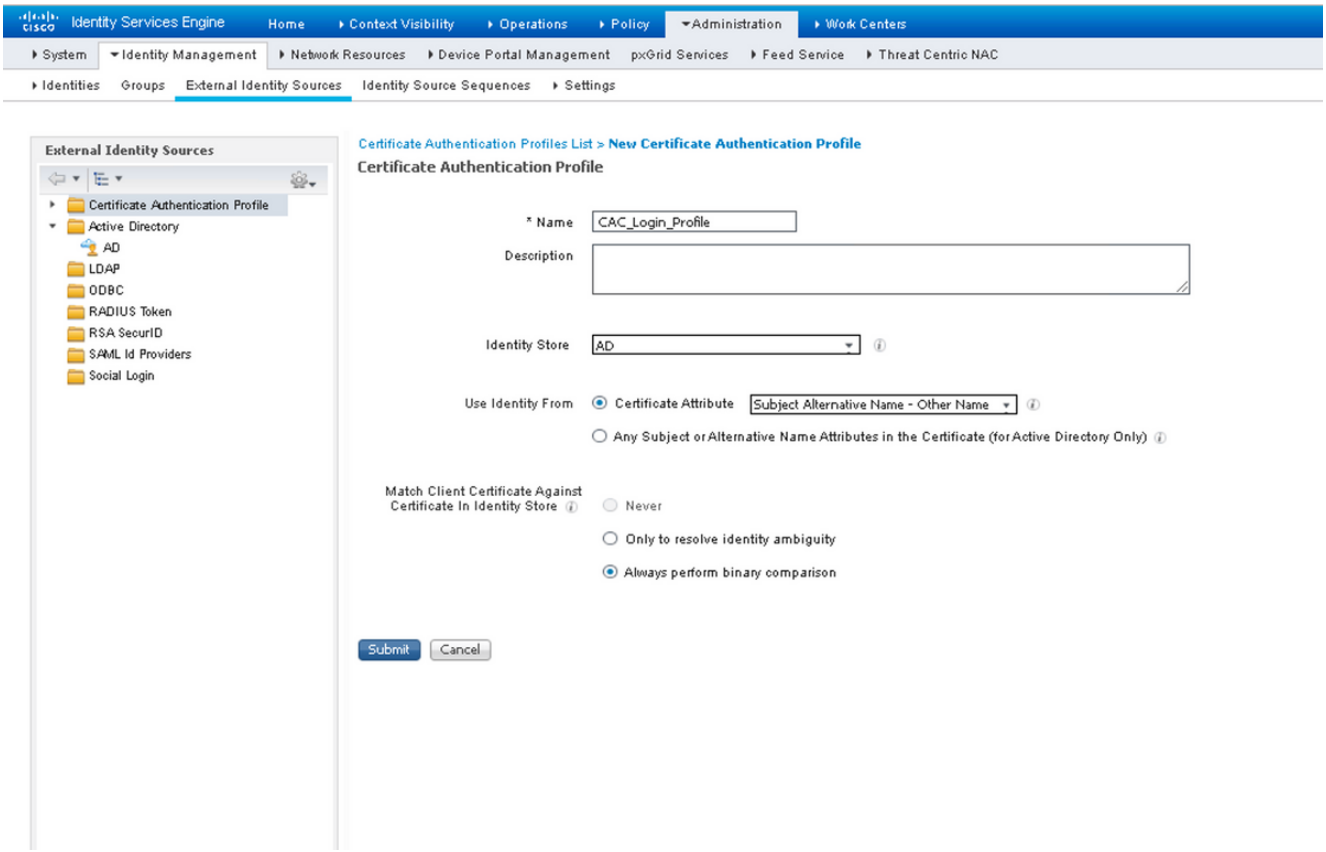
1. Per creare il profilo di autenticazione certificato per l'autenticazione basata su certificati client, scegliere **Amministrazione >Gestione delle identità > Origini identità esterne > Profilo**

di autenticazione certificato > Aggiungi.

2. Aggiungere il nome del profilo.

3. Selezionare l'attributo appropriato che contiene il nome utente dell'amministratore nell'attributo del certificato.

4. Se il record AD per l'utente contiene il certificato dell'utente e si desidera confrontare il certificato ricevuto dal browser con quello in Active Directory, selezionare la casella di controllo **Esegui sempre confronto binario** e selezionare il nome dell'istanza di Active Directory specificato in precedenza.

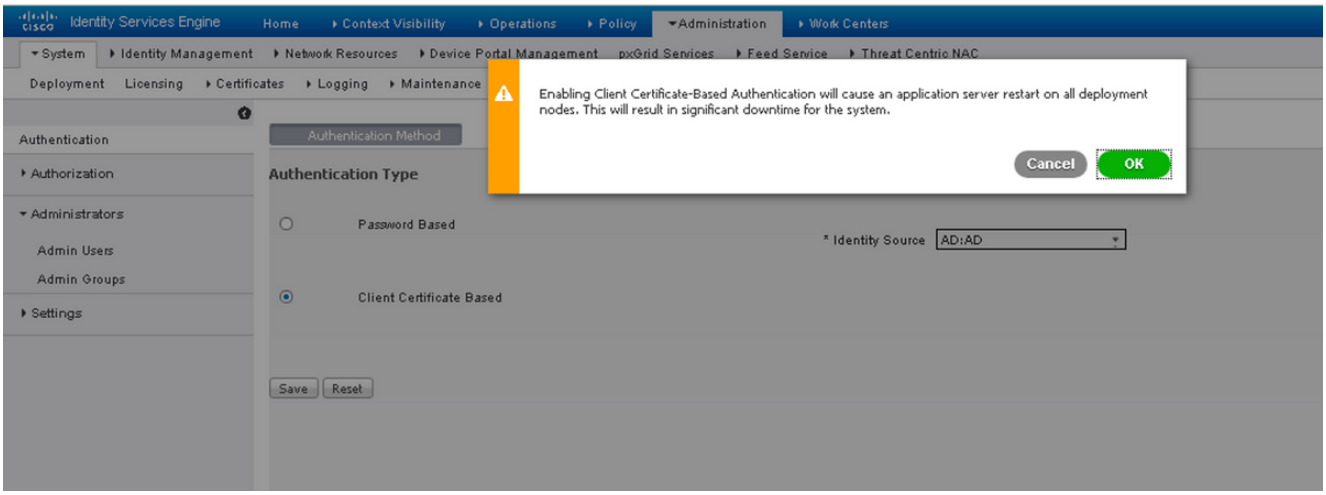


5. Fare clic su **Invia.**

Nota: Lo stesso profilo di autenticazione certificato può essere utilizzato anche per l'autenticazione basata sull'identità dell'endpoint.

Abilita autenticazione basata su certificati client

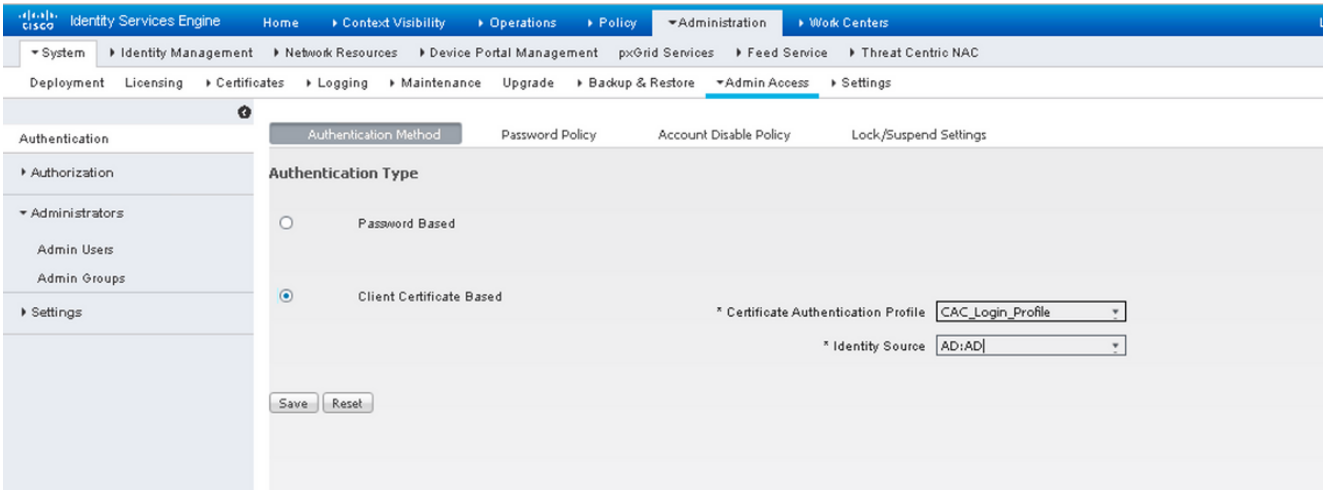
1. Scegli **Amministrazione > Sistema > Accesso amministratore > Autenticazione > Basato su certificato client metodo di autenticazione.**



2. Fare clic su **OK**.

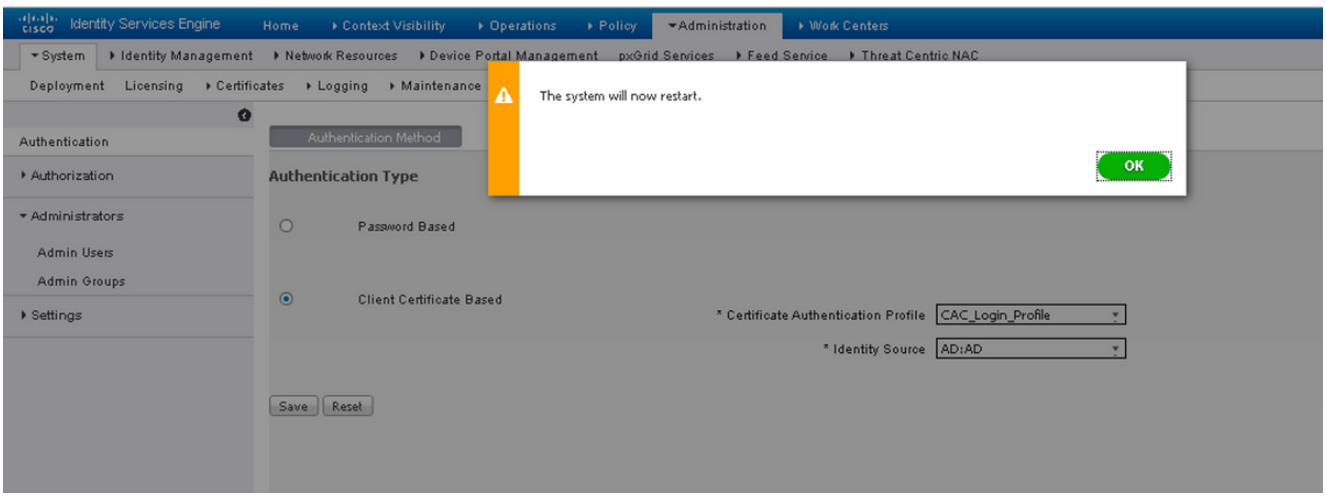
3. Scegliere il **profilo di autenticazione certificato** configurato in precedenza.

4. Selezionare il nome dell'istanza di Active Directory.



5. Fare clic su **Salva**.

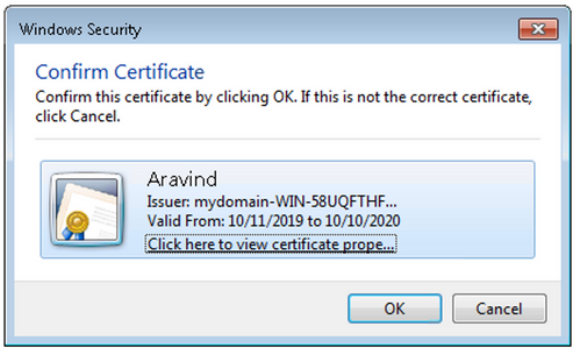
6. I servizi ISE vengono riavviati su tutti i nodi dell'implementazione.

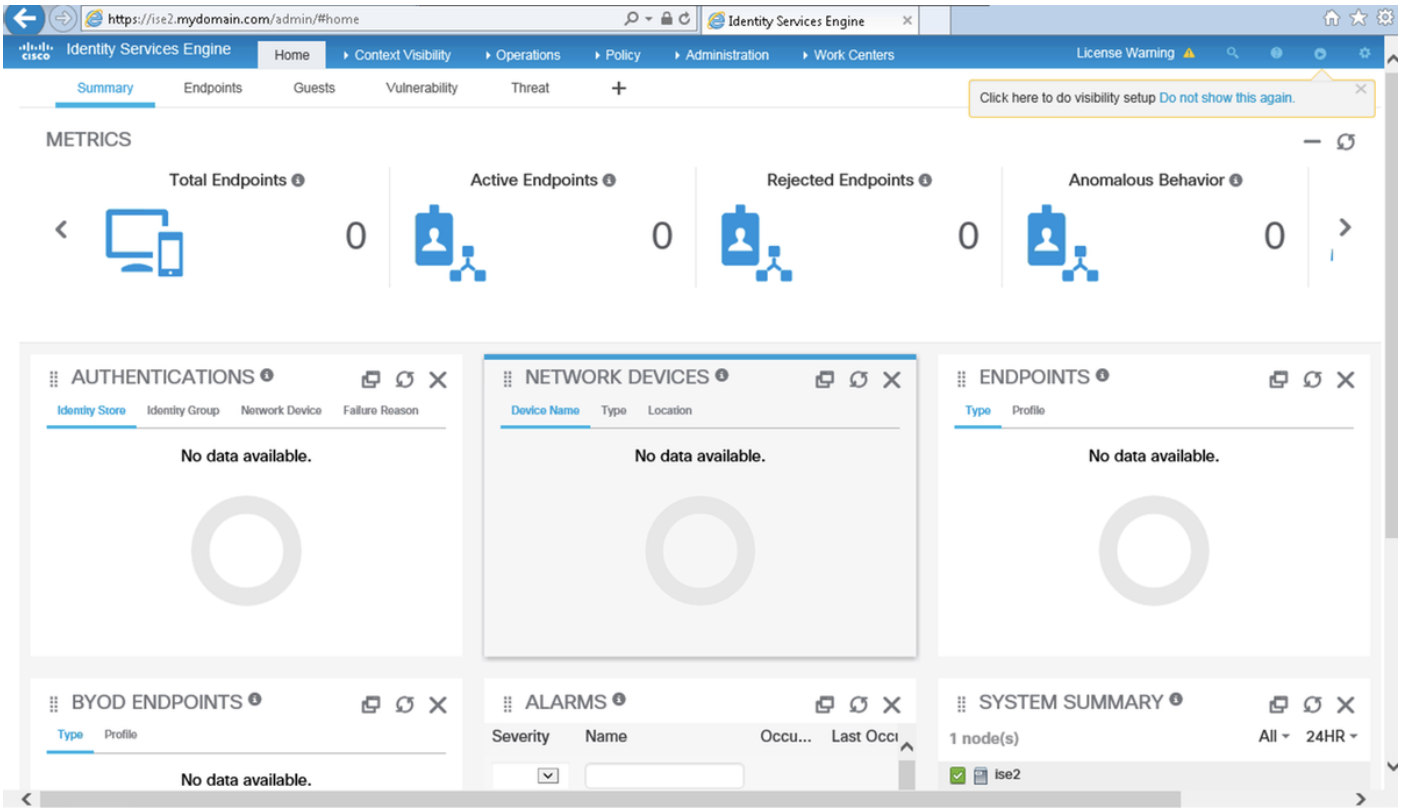


Verifica

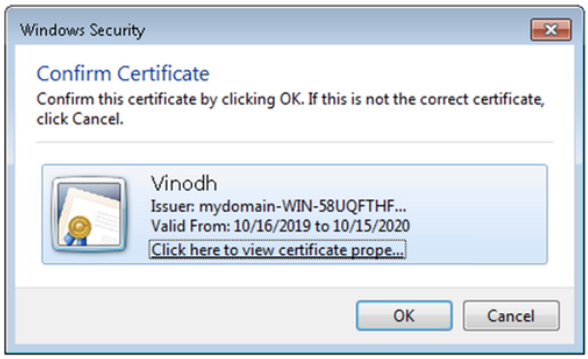
Verificare l'accesso all'interfaccia grafica di ISE dopo che lo stato del servizio **Application Server** è cambiato in **In esecuzione.**

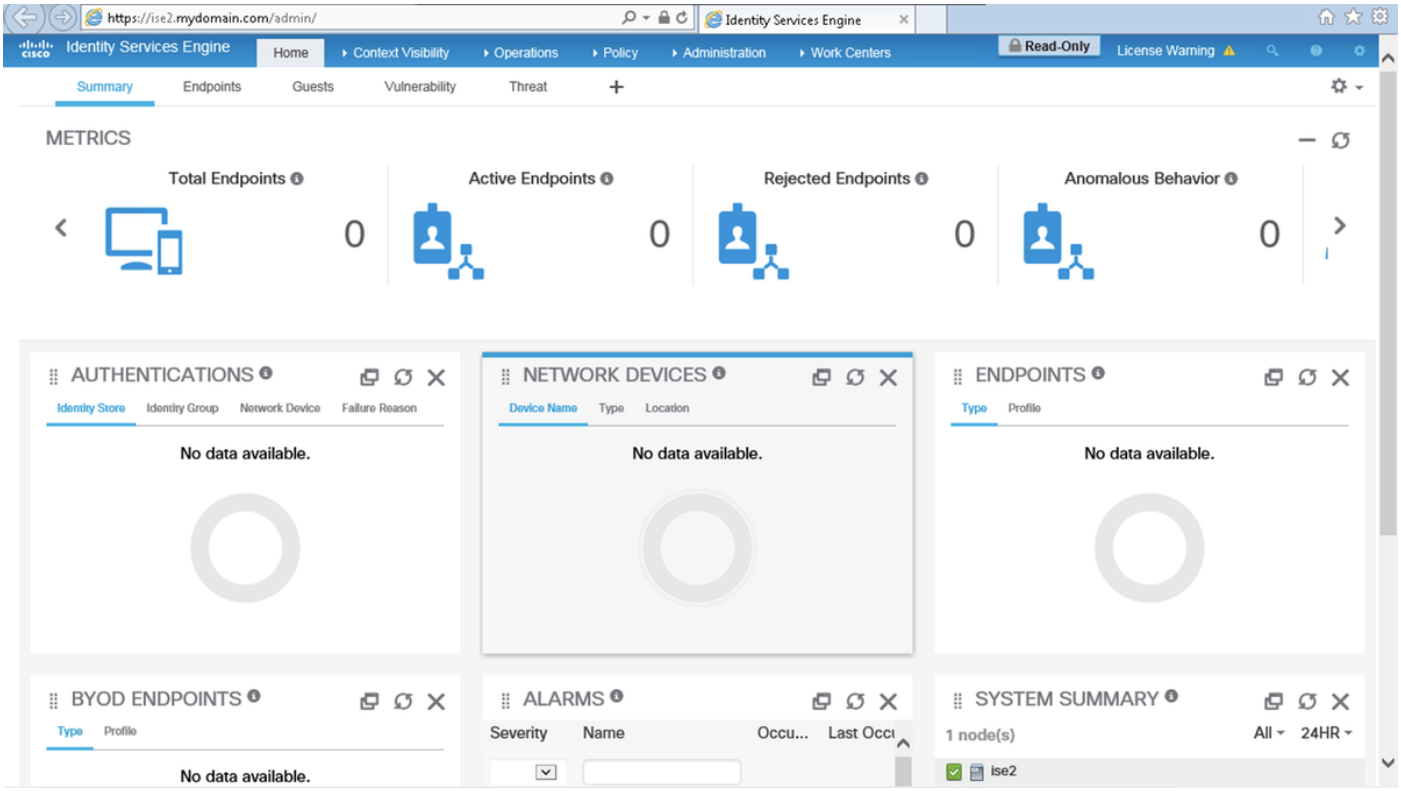
Utente con privilegi di amministratore privilegiato: verificare che all'utente venga richiesto di scegliere un certificato per accedere alla GUI ISE e che disponga dei privilegi di amministratore privilegiato se il certificato appartiene a un utente del gruppo di identità esterna con privilegi di amministratore privilegiato.





Admin User di sola lettura: verificare che all'utente venga richiesto di scegliere un certificato per accedere alla GUI di ISE e che disponga dei privilegi Admin di sola lettura se il certificato appartiene a un utente che fa parte del gruppo Admin External Identity di sola lettura.





Nota: Se è in uso una scheda CAC (Common Access Card), la smart card presenta il certificato utente ad ISE dopo che l'utente ha immesso il proprio super pin valido.

Risoluzione dei problemi

1. Utilizzare il comando **application start ise safe** per avviare Cisco ISE in una modalità provvisoria che consente di disabilitare temporaneamente il controllo dell'accesso al portale di amministrazione e correggere la configurazione e riavviare i servizi di ISE con il comando **application stop ise** seguito dal comando **application start ise.**
2. L'opzione safe consente il ripristino se un amministratore blocca inavvertitamente l'accesso al portale Cisco ISE Admin per tutti gli utenti. Questo evento può verificarsi se l'amministratore ha configurato un elenco di **accesso IP** errato nella **pagina Amministrazione > Accesso amministratore > Impostazioni > Accesso**. L'opzione **safe ignora** inoltre **l'autenticazione basata su certificati** e ripristina l'autenticazione predefinita di nome utente e password per accedere al portale Cisco ISE Admin.