Konfigurieren der Authentifizierung für ISE-Administration auf Zertifikats- oder Smartcard-Basis

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Client-Certificate-basierte Authentifizierung für den ISE-Managementzugriff (Identity Services Engine) konfiguriert wird. In diesem Beispiel authentifiziert sich der ISE-Administrator anhand des Benutzerzertifikats, um Administratorzugriff auf die Verwaltungs-GUI der Cisco Identity Services Engine (ISE) zu erhalten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, die folgenden Themen zu kennen:

- ISE-Konfiguration für Passwort und Zertifikatsauthentifizierung.
- Microsoft Active Directory (AD)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

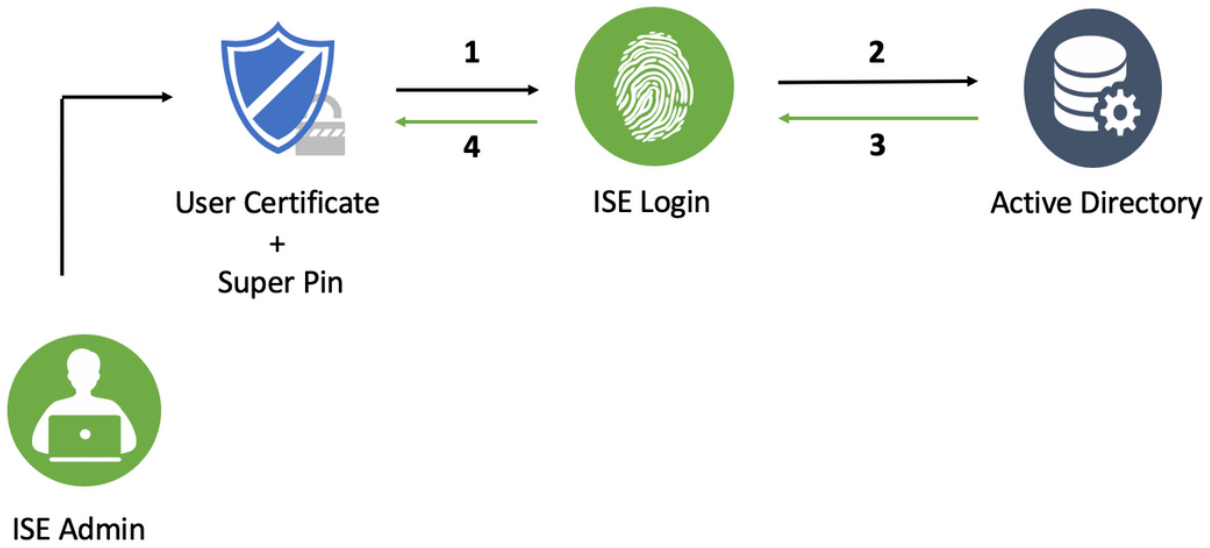
- Cisco Identity Services Engine (ISE) Version 2.6
- Windows Active Directory (AD) Server 2008, Version 2
- Zertifikat

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn das Netzwerk in Betrieb ist, sollten Sie die potenziellen Auswirkungen einer Konfiguration verstehen.

Konfigurieren

In diesem Abschnitt können Sie das Client-Zertifikat oder die Smart Card als externe Identität für den Administratorzugriff auf die Cisco ISE-Verwaltungs-GUI konfigurieren.

Netzwerkdiagramm

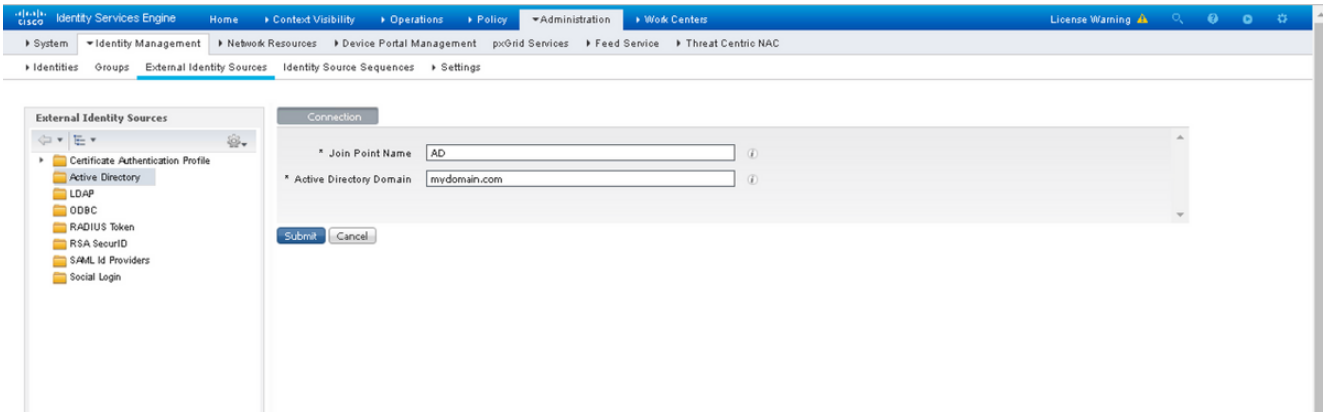


Beitritt zur ISE zu Active Directory

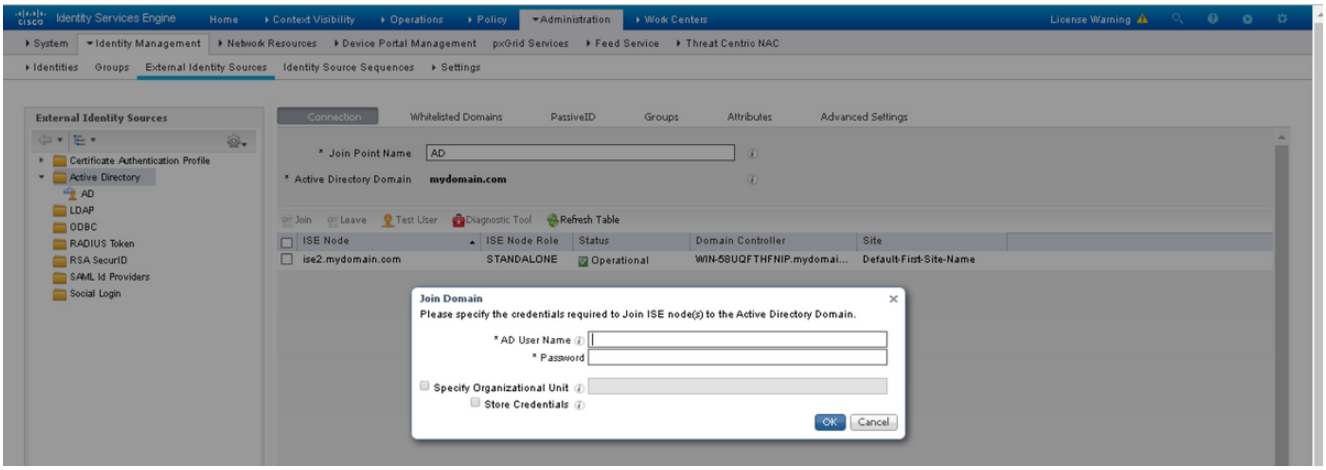
1. Wählen Sie **Administration > Identitätsmanagement > Externe Identitätsquellen > Active Directory.**

2. Erstellen Sie eine Active Directory-Instanz mit dem **Join Point-Namen** und der **AD-Domäne** in der Cisco ISE.

3. Klicken Sie auf **Senden**.



4. Verbinden Sie alle Knoten mit dem entsprechenden **Benutzernamen** und **Kennwort** in der Eingabeaufforderung.



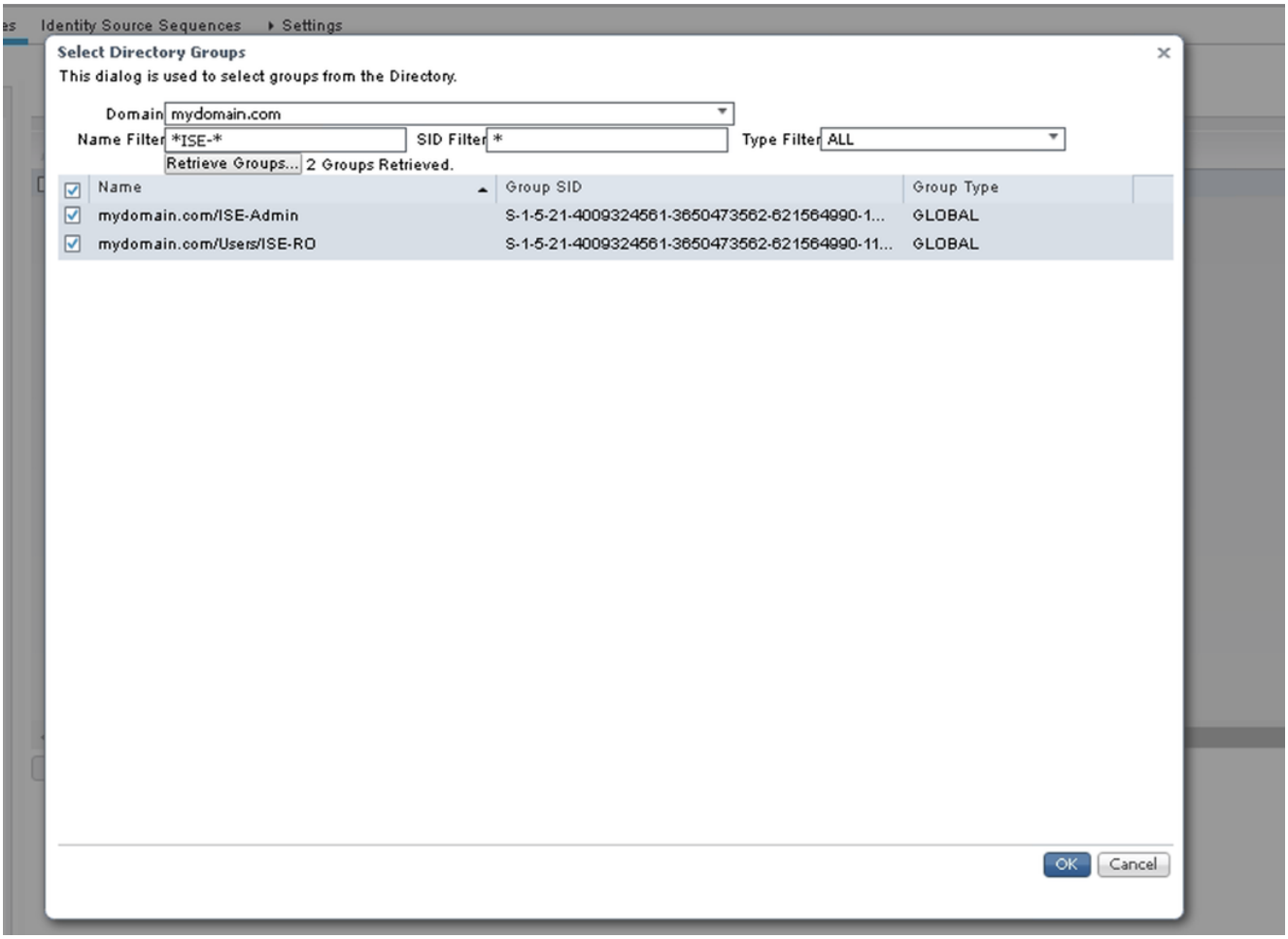
5. Klicken Sie auf **Speichern**.

Verzeichnisgruppen auswählen

1. Erstellen Sie eine externe Administratorgruppe, und ordnen Sie diese der aktiven Verzeichnisgruppe zu.

2. Wählen Sie **Administration >Identitätsmanagement > Externe Identitätsquellen > Active Directory > Gruppen > Wählen Sie Gruppen aus dem Verzeichnis aus.**

3. Rufen Sie mindestens eine AD-Gruppe ab, der der Administrator angehört.

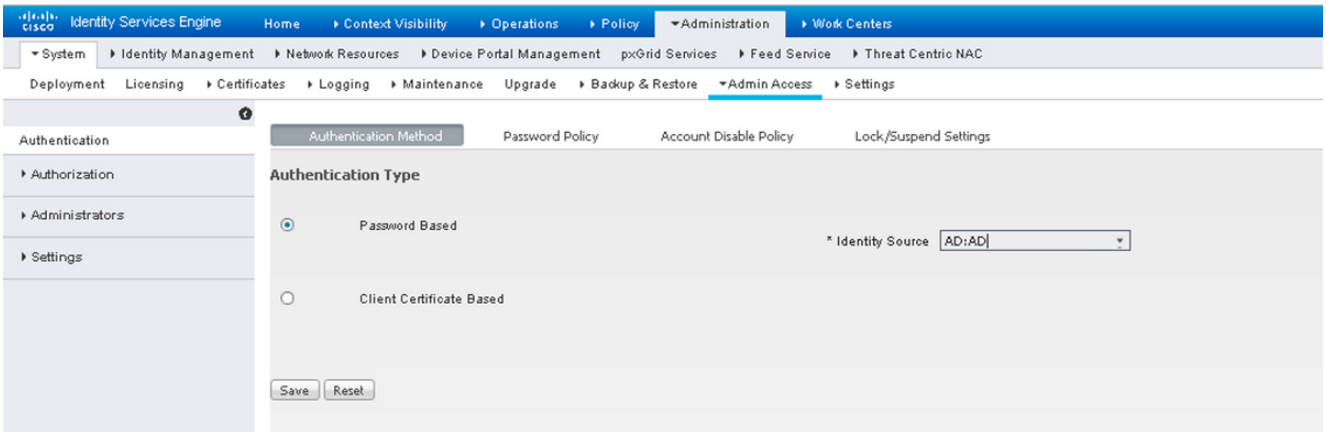


4. Klicken Sie auf **Speichern**.

Aktivieren der auf Active Directory-Kennwörtern basierenden Authentifizierung für den Administratorzugriff

1. Aktivieren Sie die Active Directory-Instanz als kennwortbasierte Authentifizierungsmethode, die der ISE bereits zuvor beigetreten ist.

2. Wählen Sie **Administration > System > Admin access > Authentication** (Verwaltung > System > Administratorzugriff > Authentifizierung) aus, wie im Bild gezeigt.



3. Klicken Sie auf **Speichern**.

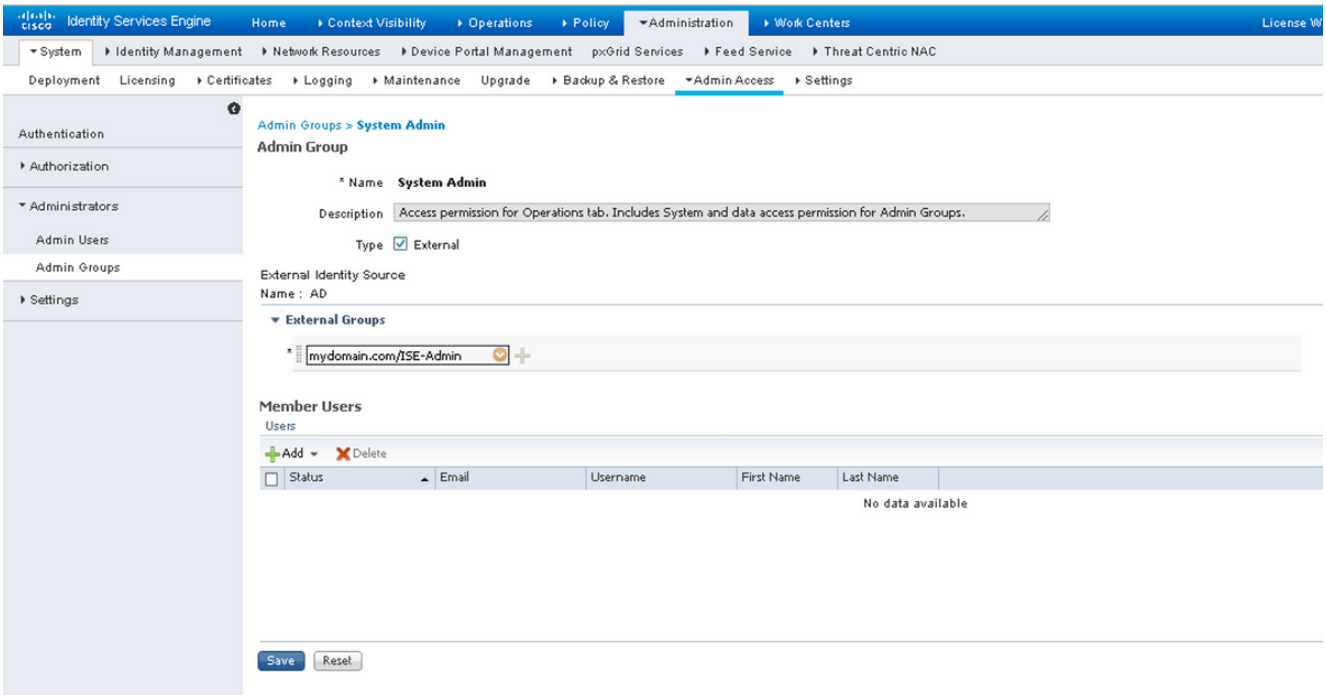
Hinweis: Zur Aktivierung der zertifikatbasierten Authentifizierung ist eine kennwortbasierte Authentifizierungskonfiguration erforderlich. Diese Konfiguration sollte nach erfolgreicher Konfiguration der zertifikatbasierten Authentifizierung zurückgesetzt werden.

Externe Identitätsgruppen Administratorgruppen zuordnen

In diesem Beispiel wird die externe AD-Gruppe der standardmäßigen Admin-Gruppe zugeordnet.

1. Wählen Sie **Administration > System >Admin Access >Administrator >Admin Groups > Super Admin.**

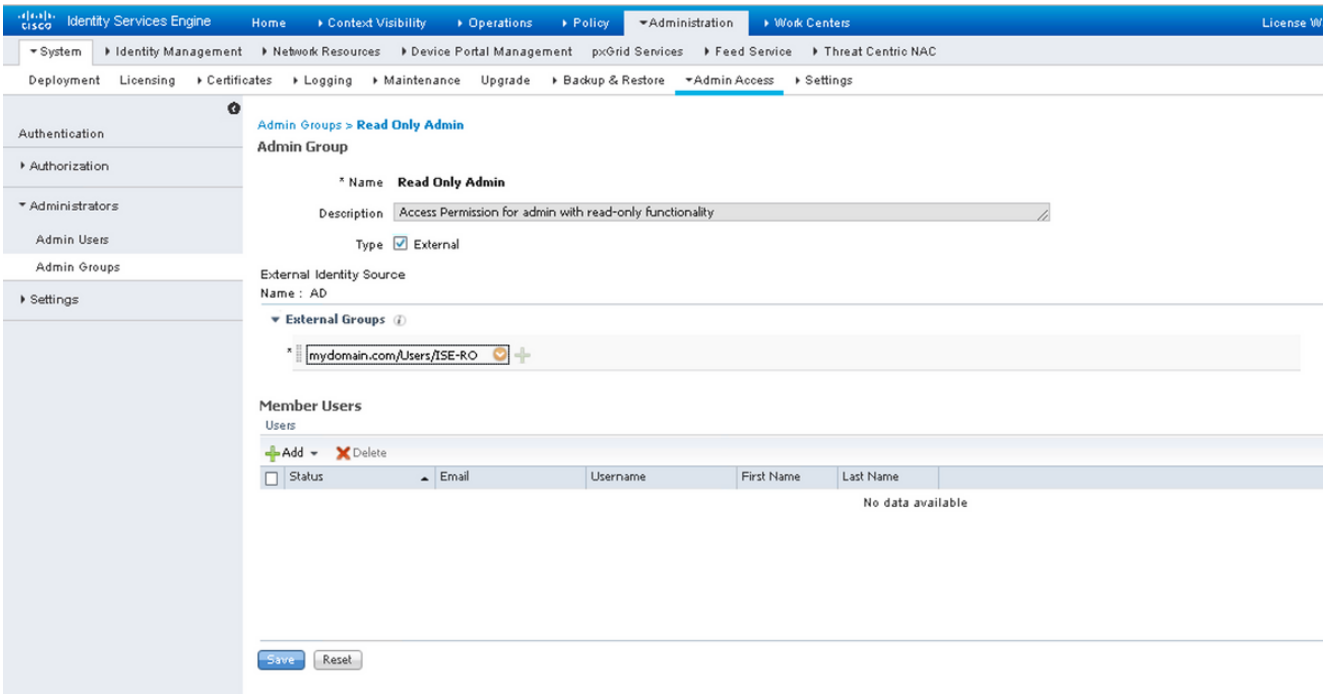
2. Aktivieren Sie Typ als **Extern** und wählen Sie unter **Externe Gruppen** die AD-Gruppe aus.



3. Klicken Sie auf **Speichern**.

4. Wählen Sie **Administration > System > Admin Access > Administrator Groups > Read Only Admin (Nur Lesezugriff) aus**.

5. Aktivieren Sie Type as **External** und wählen Sie unter **External groups** die AD-Gruppe aus, wie im Bild gezeigt.



6. Klicken Sie auf **Speichern**.

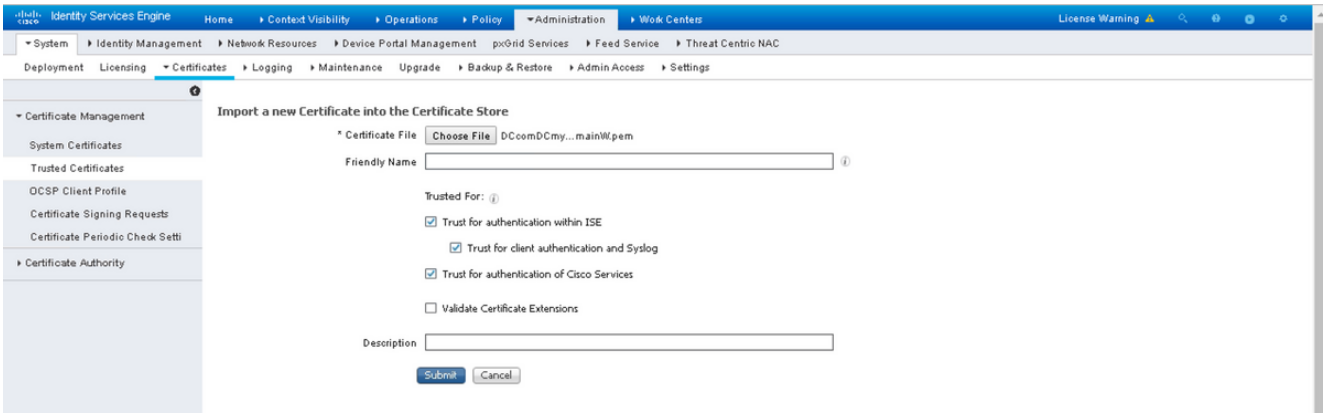
Vertrauenswürdiges Zertifikat importieren

1. Importieren Sie das Zertifikat der Zertifizierungsstelle (Certificate Authority, CA), das das Clientzertifikat signiert.

2. Auswählen **Administrator > System > Certificates > Trusted Certificate > Import.**

3. Klicken Sie auf Durchsuchen, und wählen Sie das Zertifizierungsstellenzertifikat aus.

4. Aktivieren Sie das **Kontrollkästchen Vertrauenswürdig für Client-Authentifizierung und Syslog**, wie im Bild gezeigt.



5. Klicken Sie auf **Senden.**

Zertifikatauthentifizierungsprofil konfigurieren

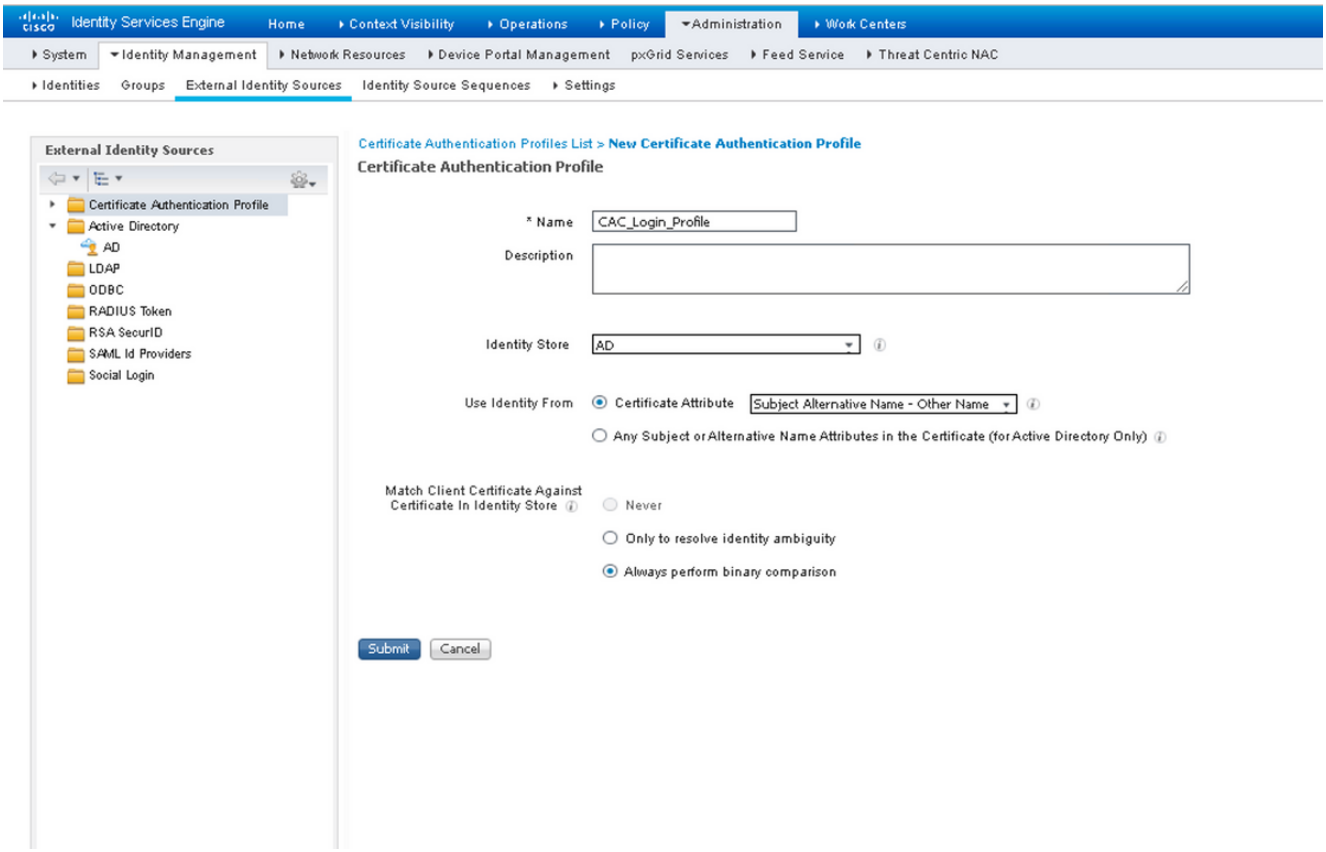
1. Um ein Zertifikatauthentifizierungsprofil für die zertifikatbasierte Authentifizierung des Clients

zu erstellen, wählen Sie **Administration >Identitätsmanagement > Externe Identitätsquellen > Zertifikatauthentifizierungsprofil > Hinzufügen.**

2. Profilname hinzufügen

3. Wählen Sie das entsprechende Attribut aus, das den Administratorbenutzernamen im Zertifikatattribut enthält.

4. Wenn der AD-Datensatz für den Benutzer das Benutzerzertifikat enthält und das vom Browser erhaltene Zertifikat mit dem Zertifikat in AD vergleichen möchte, aktivieren Sie das Kontrollkästchen **Immer Binärvergleich durchführen** und wählen den zuvor angegebenen Active Directory-Instanznamen aus.

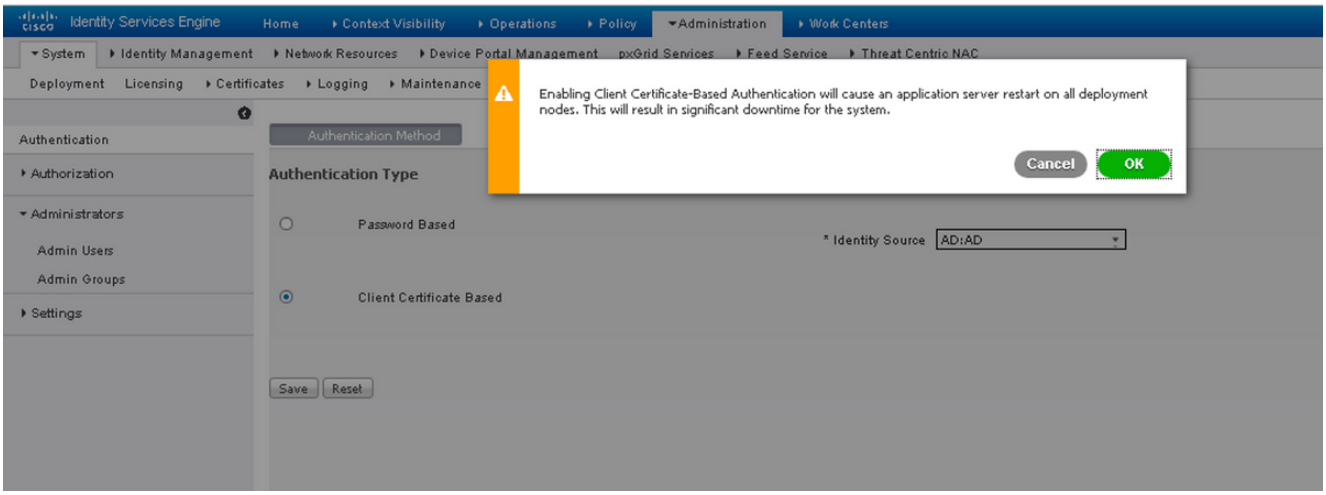


5. Klicken Sie auf **Senden.**

Hinweis: Das gleiche Zertifikatauthentifizierungsprofil kann auch für die identitätsbasierte Endpunkt-Authentifizierung verwendet werden.

Clientzertifikatbasierte Authentifizierung aktivieren

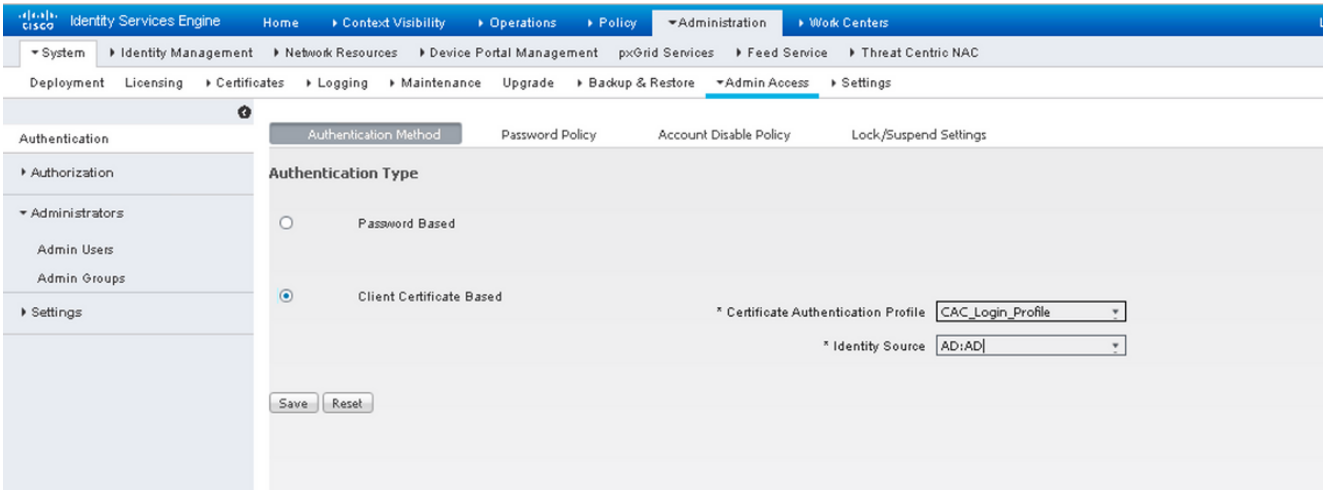
1. Auswählen **Administration > System > Admin Access > Authentication > Authentication Method Client Certificate Based.**



2. Klicken Sie auf **OK**.

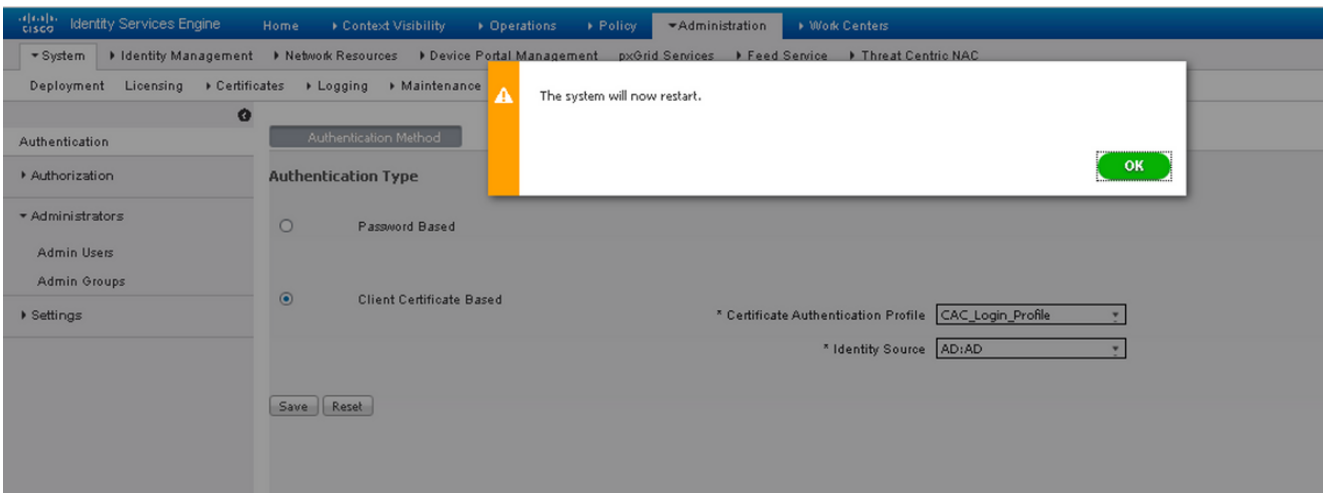
3. Wählen Sie das zuvor konfigurierte **Zertifikatauthentifizierungsprofil aus**.

4. Wählen Sie den Instanznamen der Active Directory-Instanz aus.



5. Klicken Sie auf **Speichern**.

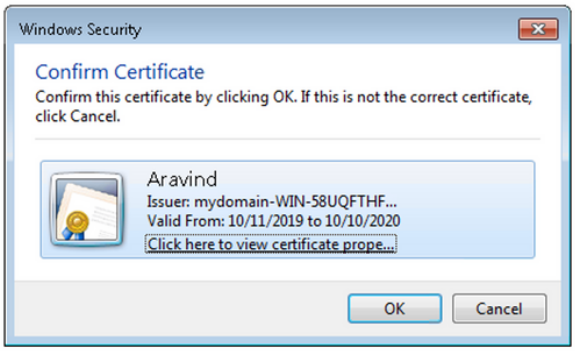
6. ISE-Services auf allen Knoten, die bei der Bereitstellung neu gestartet werden.

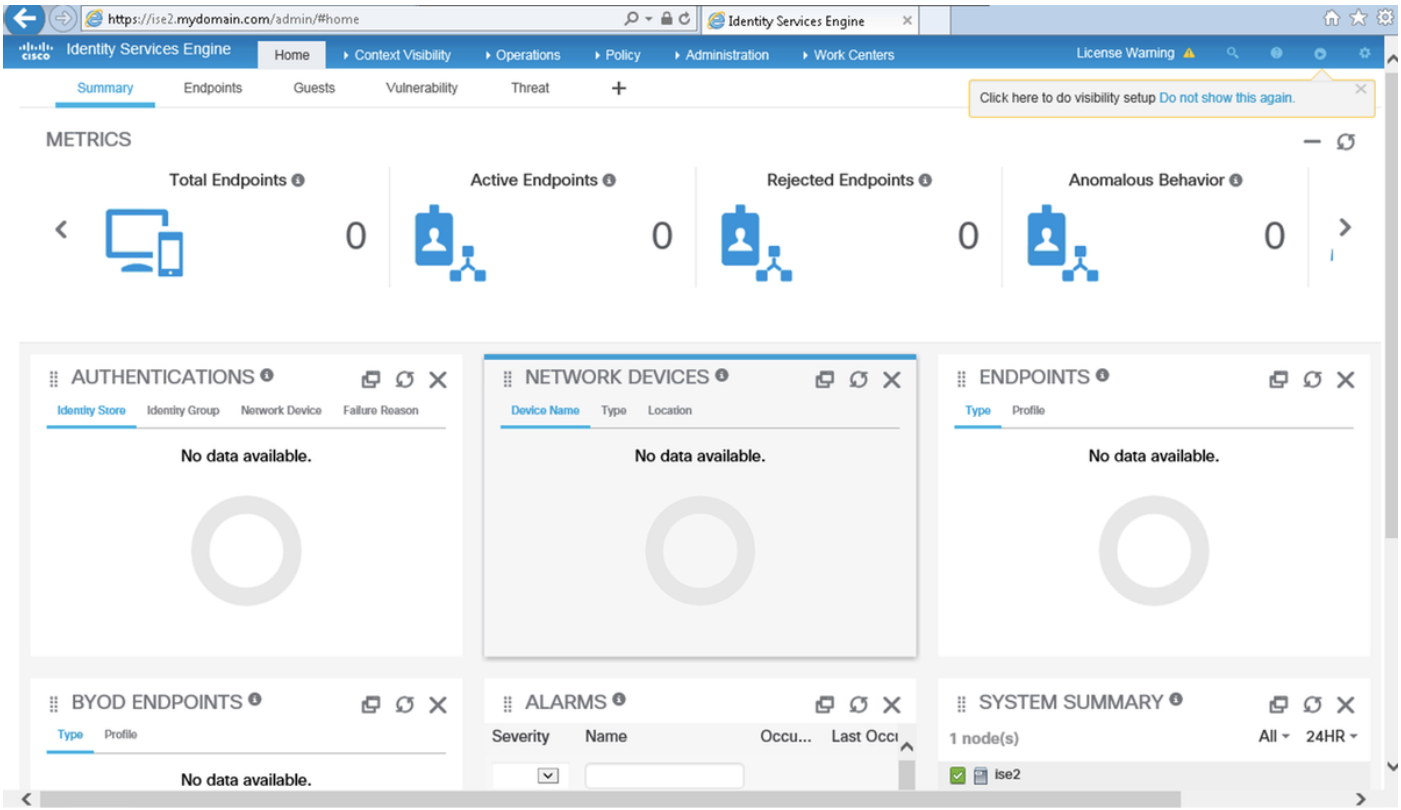


Überprüfen

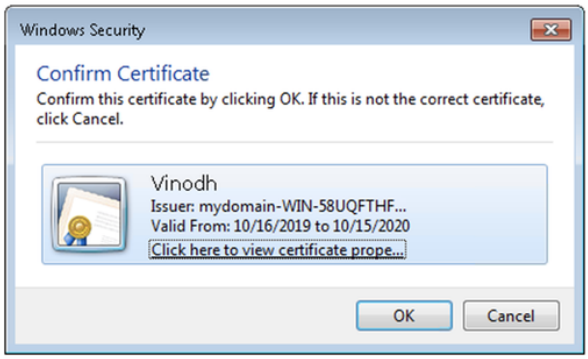
Überprüfen Sie den Zugriff auf die ISE-GUI, nachdem sich der Dienststatus des **Anwendungsservers** in **Ausführung** geändert hat.

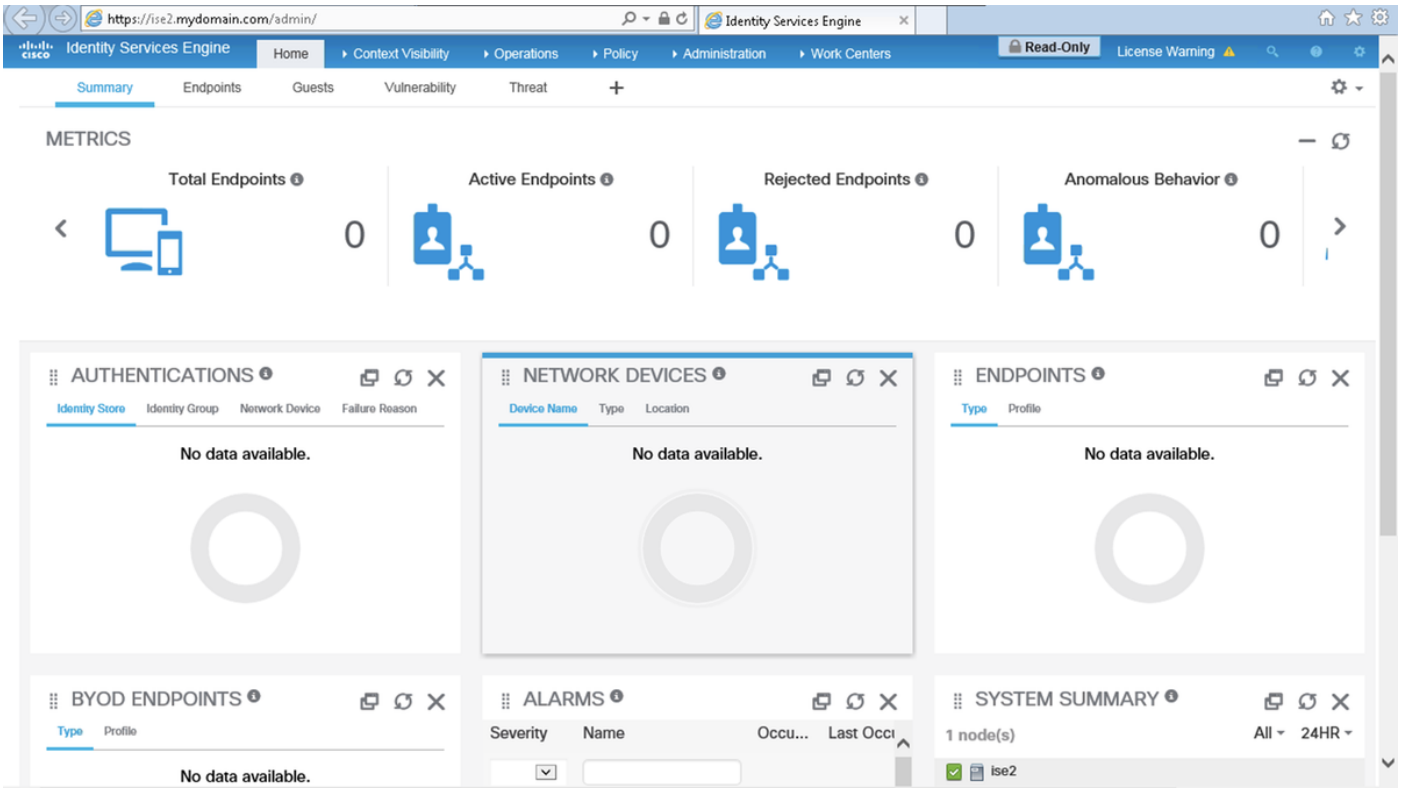
Super Admin User (Super-Admin-Benutzer): Stellen Sie sicher, dass der Benutzer aufgefordert wird, ein Zertifikat für die Anmeldung bei der ISE-GUI auszuwählen, und dass er Super Admin-Berechtigungen erhält, wenn das Zertifikat ein Benutzer der Super Admin External Identity-Gruppe ist.





Schreibgeschützter Admin-Benutzer: Vergewissern Sie sich, dass der Benutzer aufgefordert wird, ein Zertifikat für die Anmeldung bei der ISE-GUI auszuwählen, und dass ihm Schreibschutzberechtigungen gewährt werden, wenn das Zertifikat einem Benutzer angehört, der zur Gruppe "Schreibgeschützt" der externen Administrator-Identität gehört.





Hinweis: Wenn eine Common Access Card (CAC) verwendet wird, legt Smartcard das Benutzerzertifikat der ISE vor, nachdem der Benutzer seinen gültigen Super-Pin eingegeben hat.

Fehlerbehebung

1. Verwenden Sie den Befehl **application start ise safe**, um die Cisco ISE im abgesicherten Modus zu starten, der es ermöglicht, die Zugriffskontrolle für das Admin-Portal vorübergehend zu deaktivieren und die Konfiguration zu korrigieren und die Dienste der ISE mit dem Befehl **application stop ise** gefolgt von **application start ise** neu zu starten..
2. Die Option "safe" bietet eine Möglichkeit zur Wiederherstellung, wenn ein Administrator versehentlich den Zugriff auf das Cisco ISE-Admin-Portal für alle Benutzer sperrt. Dieses Ereignis kann auftreten, wenn der Administrator auf der **Seite Administration > Admin Access > Settings > Access (Administration > Administratorzugriff > Einstellungen > Zugriff)** eine falsche **IP-Zugriffsliste** konfiguriert hat. Die **Option "safe" umgeht außerdem die zertifikatsbasierte Authentifizierung** und kehrt zur Standard-Benutzernamen- und Kennwortauthentifizierung für die Anmeldung beim Cisco ISE Admin-Portal zurück.