ISE Administrationの証明書またはスマートカードベースの認証の設定

内容

概要

このドキュメントでは、Identity Services Engine(ISE)管理アクセス用にクライアント証明書ベースの認証を設定する方法について説明します。この例では、ISE管理者がユーザ証明書に対して認証を行い、Cisco Identity Services Engine(ISE)管理GUIへの管理者アクセスを取得します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- パスワードおよび証明書認証のためのISE設定。
- Microsoft Active Directory(AD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine(ISE)バージョン2.6
- Windows Active Directory(AD)Server 2008リリース2
- 証明書

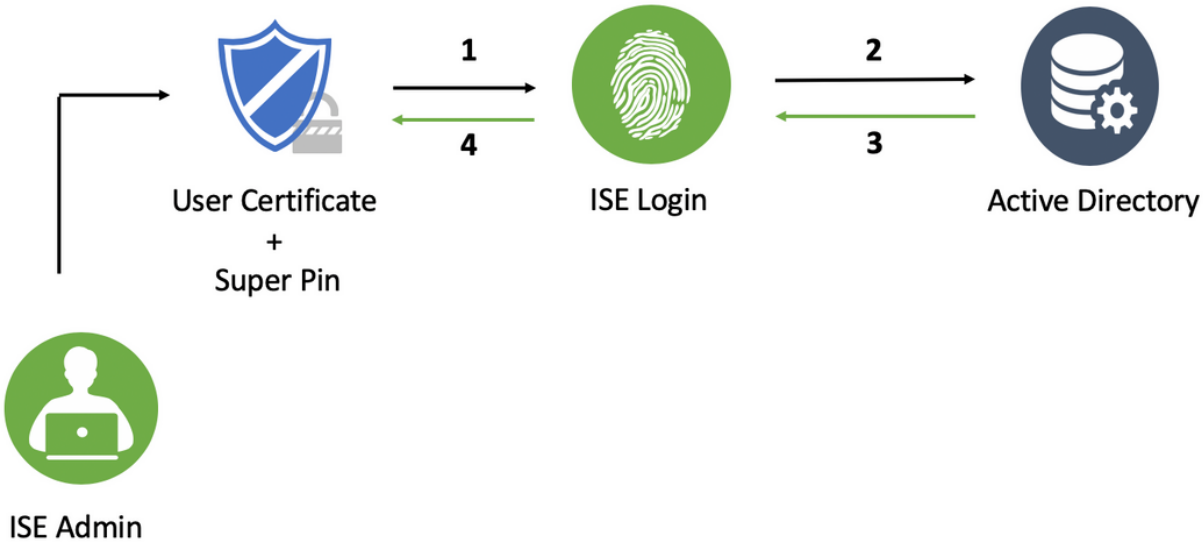
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、設定が及ぼす潜在的な影響を十分に理解しておいてください。

設定

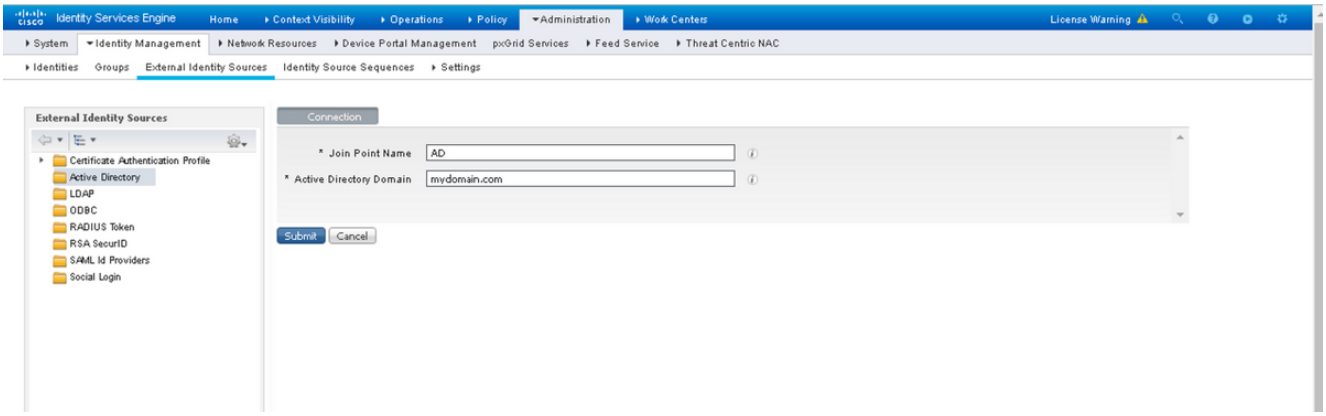
このセクションでは、Cisco ISE管理GUIへの管理アクセス用の外部IDとしてクライアント証明書またはスマートカードを設定します。

ネットワーク図

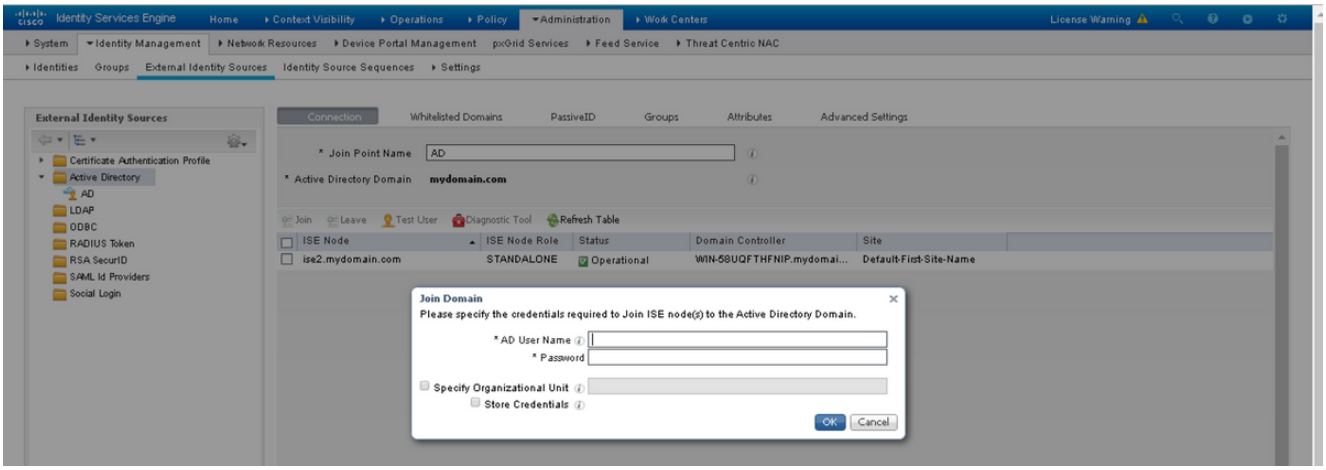


ISEのActive Directoryへの参加

1. **Administration > [Identity Management] > [External Identity Sources] > [Active Directory]。**
2. Cisco ISEで結合ポイント名とADドメイン**を持つActive Directory**イン**スタンスを**作成します。
3. [Submit] をクリックします。



4. プロンプトで、すべてのノードに適切なユーザ**名とパ**スワード**を追加**します。



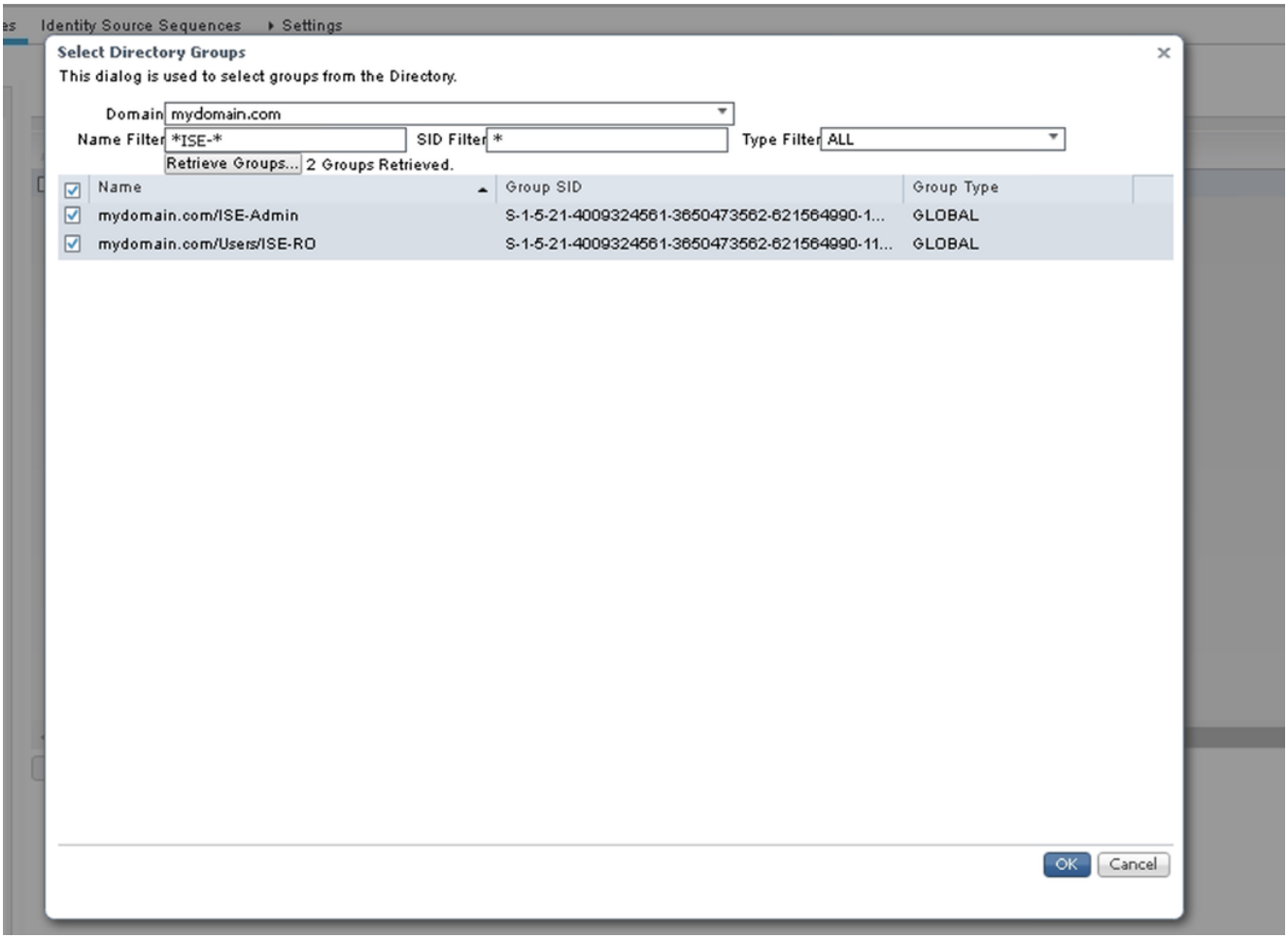
5. [Save] をクリックします。

ディレクトリ グループの選択

1. 外部の管理者グループを作成し、Active Directoryグループにマッピングします。

2. **Administration >[Identity Management] > [External Identity Sources] > [Active Directory] > [Groups] > [Select Groups from Directory]。**

3. 管理者が属する少なくとも1つのADグループを取得します。

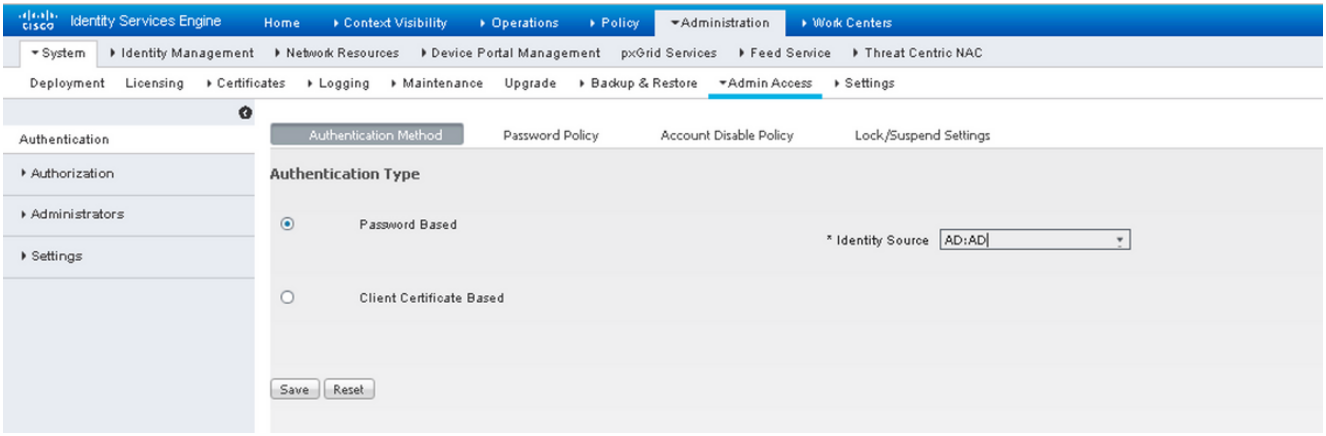


4. [Save] をクリックします。

管理アクセスのためのActive Directoryパスワードベース認証の有効化

1. Active Directoryインスタンスを、以前にISEに参加したパスワードベースの認証方式として有効にします。

2. 図に示すように、[Administration > [System] > [Admin access] > [Authentication]を選択します。



3. [Save] をクリックします。

注：証明書ベースの認証を有効にするには、パスワードベースの認証設定が必要です。証明

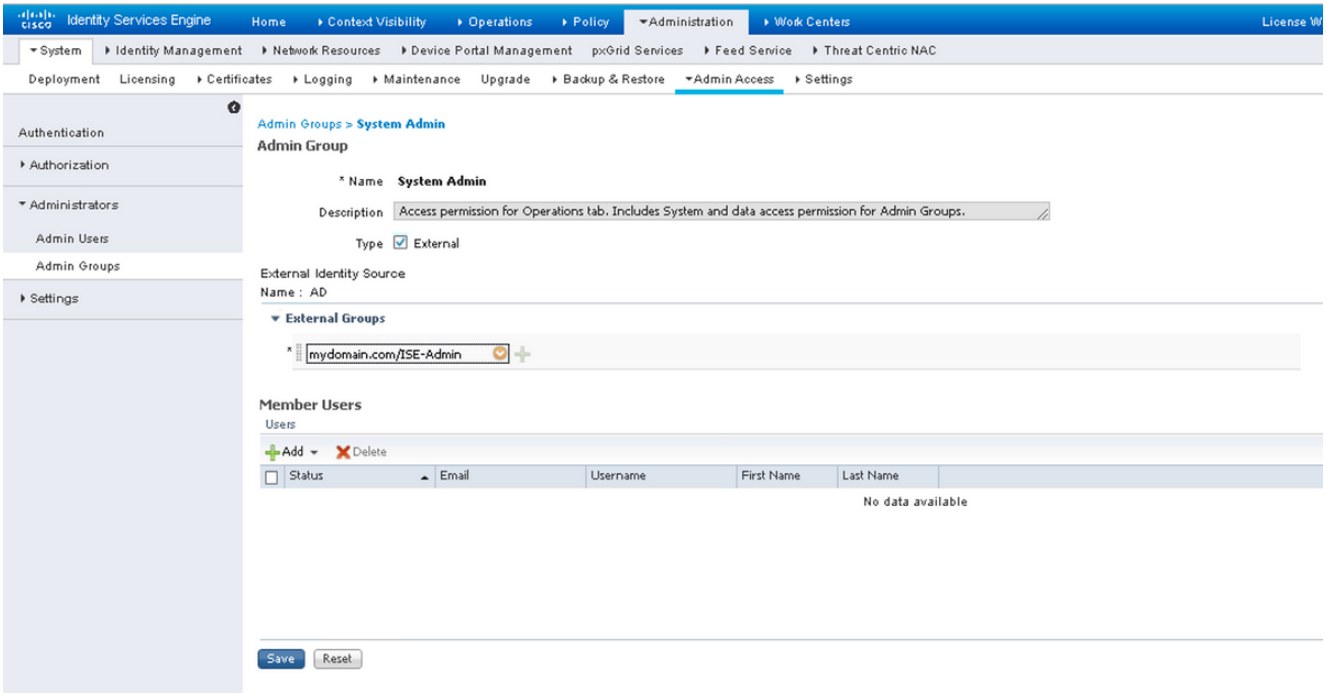
書ベースの認証を正常に設定した後、この設定を元に戻す必要があります。

外部IDグループの管理グループへのマッピング

この例では、外部ADグループがデフォルトのAdminグループにマッピングされています。

1. [Administration] > [System] > [Admin Access] > [Administrators]の順に選択します。[Admin Groups] > [Super admin]。

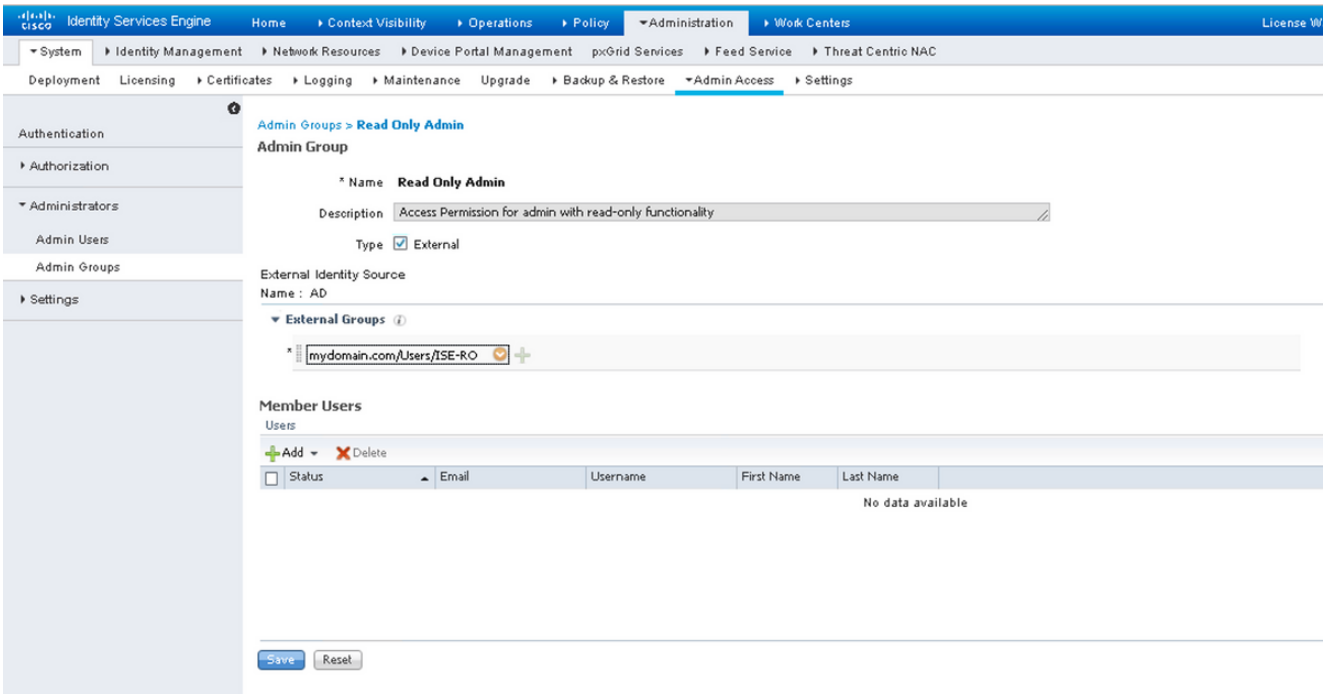
2. [Type]を[External]に選択し、[External groups]の下のADグループを選択します。



3. [Save] をクリックします。

4. Administration > System > Admin Access > Administrators > Admin Groups > Read Only Adminの順に選択します。

5. 図に示すように、[Type]に[External]を選択し、[External groups]の下のADグループを選択します。



6. [Save] をクリックします。

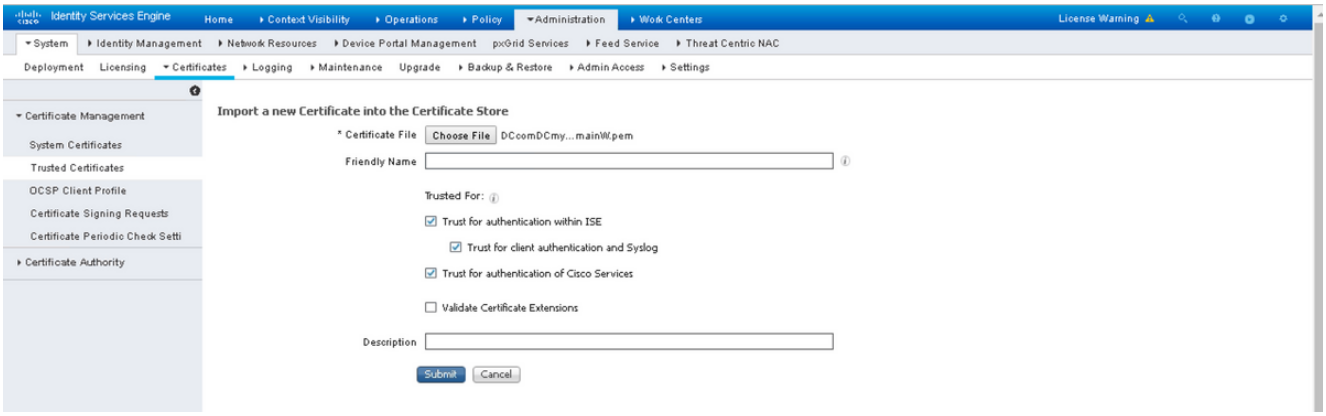
信頼できる証明書のインポート

1. クライアント証明書に署名する認証局(CA)証明書をインポートします。

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

3. [browse]をクリックし、CA証明書を選択します。

4. 図に示すように、**[Trust for client authentication and Syslog]チェックボックス**をオンにします。



5. [Submit] をクリックします。

証明書認証プロファイルの設定

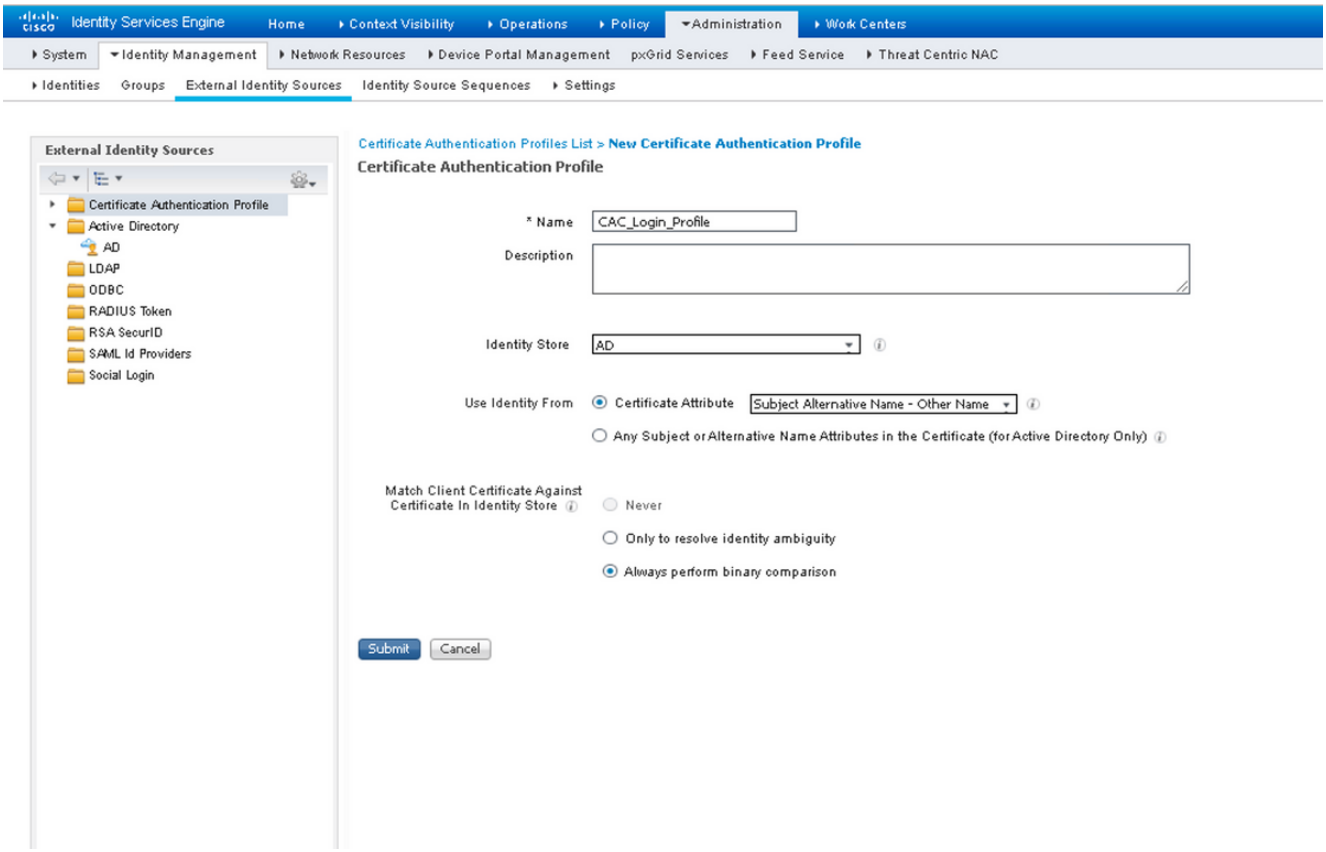
1. クライアント証明書ベース認証用の証明書認証プロファイルを作成するには、**[Administration] > [Select]を選択します[Identity Management] > [External Identity Sources] >**

[Certificate Authentication Profile] > [Add]を選択します。

2. プロファイル名を追加します。

3. 証明書属性の管理者ユーザ名を含む適切な属性を選択します。

4. ユーザのADレコードにユーザの証明書が含まれ、ブラウザから受信した証明書をADの証明書と比較する場合は、[Always perform binary comparison]チェックボックスをオンにして、先に指定したActive Directoryインスタンス名を選択します。

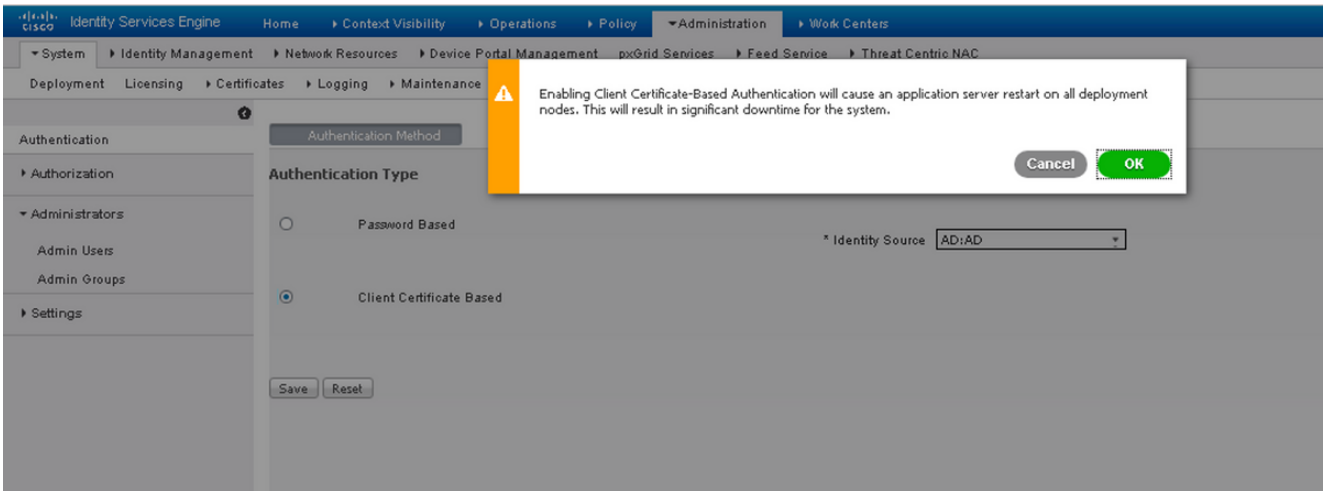


5. [Submit] をクリックします。

注：同じ証明書認証プロファイルをエンドポイントのIDベースの認証にも使用できます。

クライアント証明書ベース認証の有効化

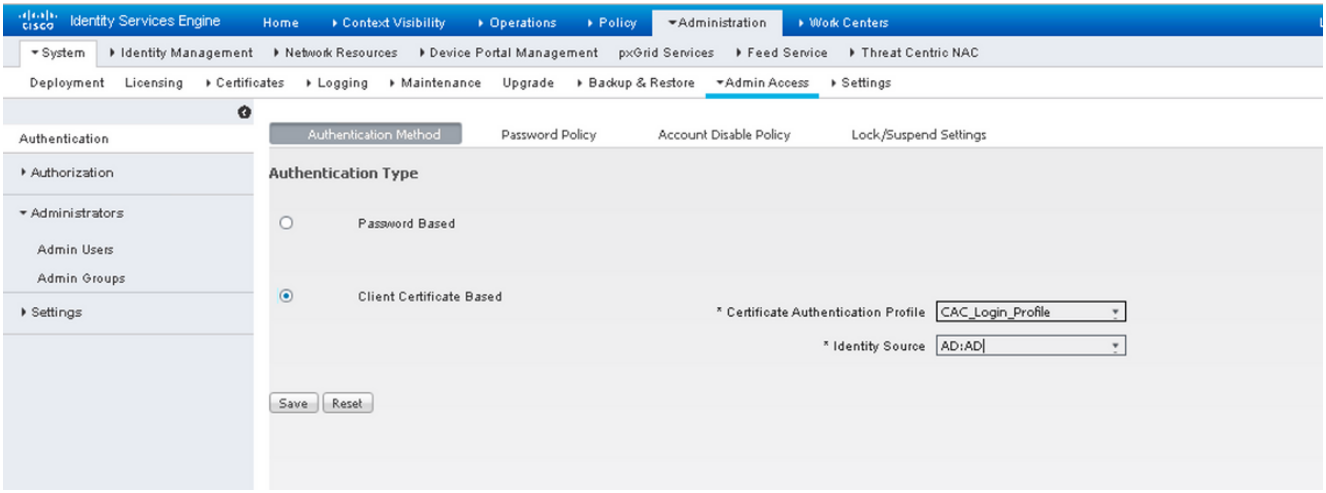
1. 選択 [Administration] > [System] > [Admin Access] > [Authentication] > [Authentication Method Client Certificate Based]。



2. [OK] をクリックします。

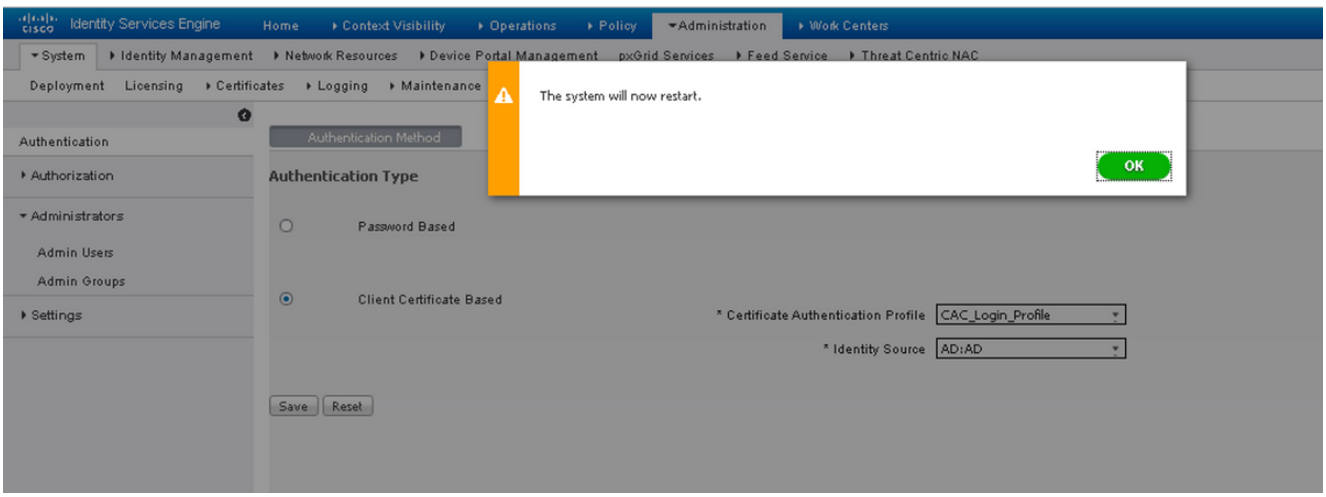
3. 先ほど設定した**証明書認証プロファイル**を選択します。

4. Active Directoryインスタンス名を選択します。



5. [Save] をクリックします。

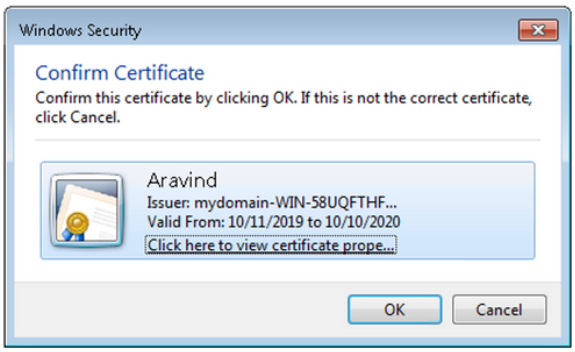
6. 展開内のすべてのノードのISEサービスが再起動します。

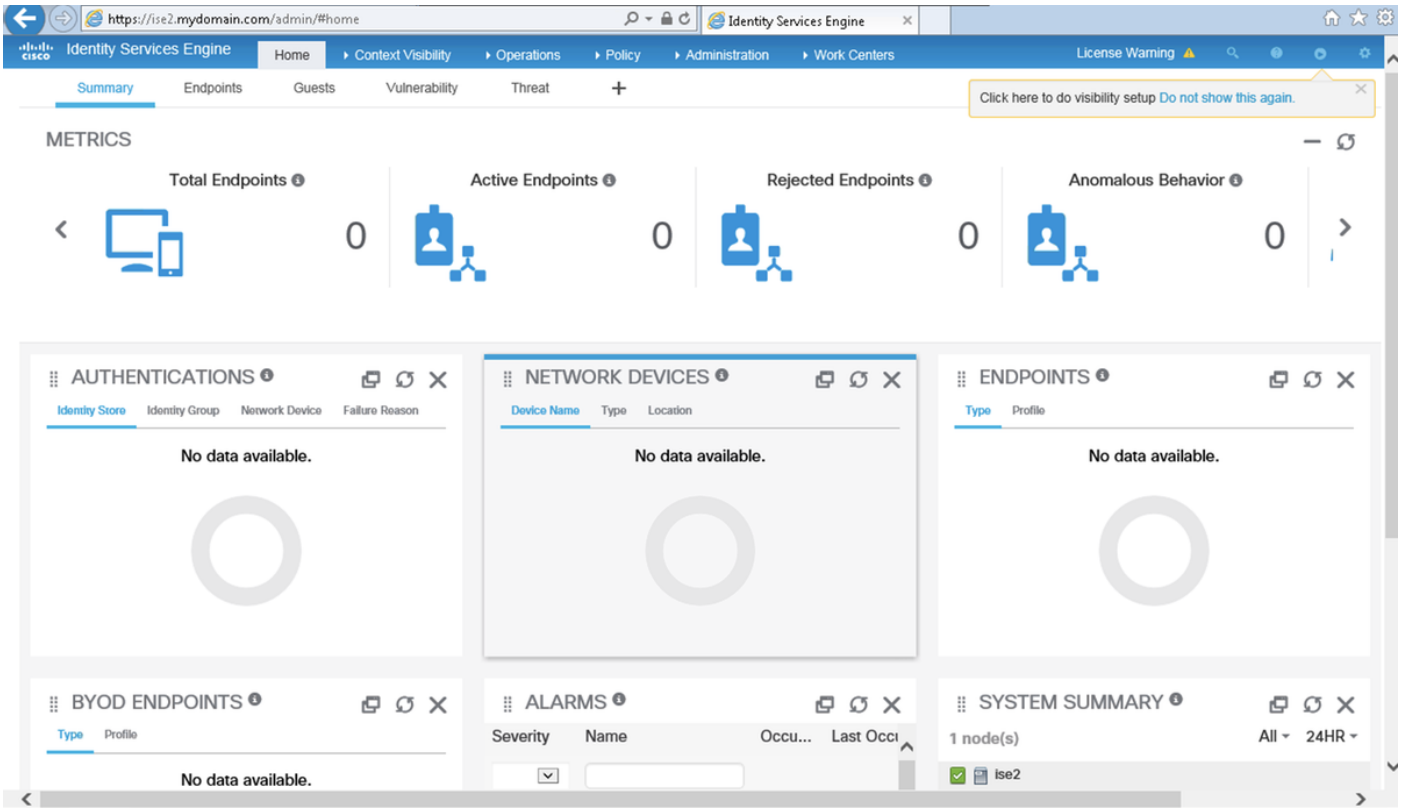


確認

Application Serverサービスのステータスが**Running**に変わった後**に**、ISE GUI**へのア**クセスを確認**します。**

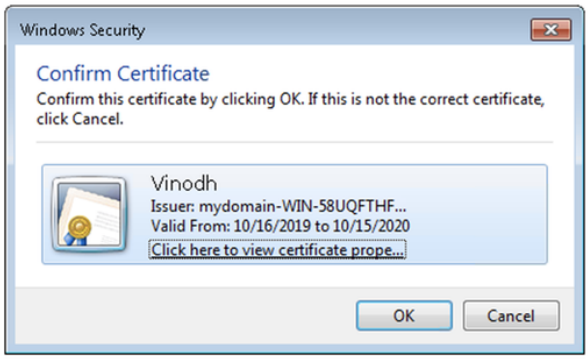
スーパー管理者ユーザ：ISE GUIにログインするための証明書の選択を求めるプロンプトが表示され、証明書がスーパー管理者外部IDグループのユーザ部分の場合はスーパー管理者権限が付与されることを確認します。

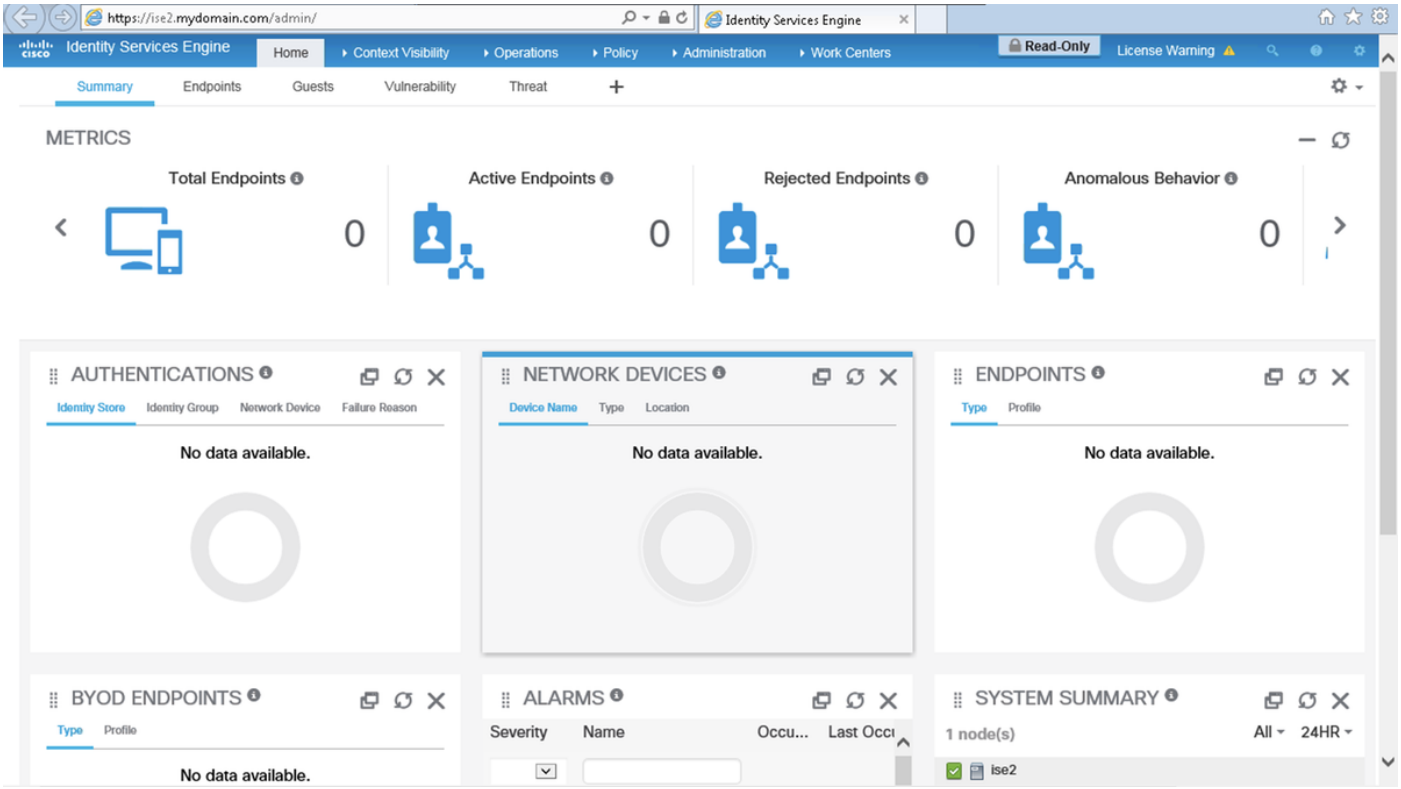




Read-only Admin User:ISE GUIにログインするための証明書の選択を求めるプロンプトが表示さ

れ、証明書がRead-only Admin External Identityグループのユーザ部分の場合は、Read-only Admin権限が付与されることを確認します。





注：Common Access Card(CAC)が使用中の場合、ユーザが有効なスーパーピンを入力すると、スマートカードはユーザ証明書をISEに提示します。

トラブルシュート

1. **application start ise safe**コマンドを使用して、Cisco ISEを安全モードで起動します。これに

より、管理ポータルへのアクセス制御を一時的に無効にし、設定を修正し、application stop iseコマンドを使用してISEのサービスを再起動できます.

2. [safe]オプションを使用すると、管理者が誤ってすべてのユーザのCisco ISE Adminポータルへのアクセスをロックアウトした場合の回復方法が提供されます。このイベントは、管理者が[Administration] > [Admin Access] > [Settings] > [Access]ページで誤ったIPアクセスリストを設定した場合に発生することがあります。safeオプションは証明書ベースの認証をバイパスし、Cisco ISE Adminポータルにログインするためのデフォルトのユーザ名とパスワード認証に戻ります。