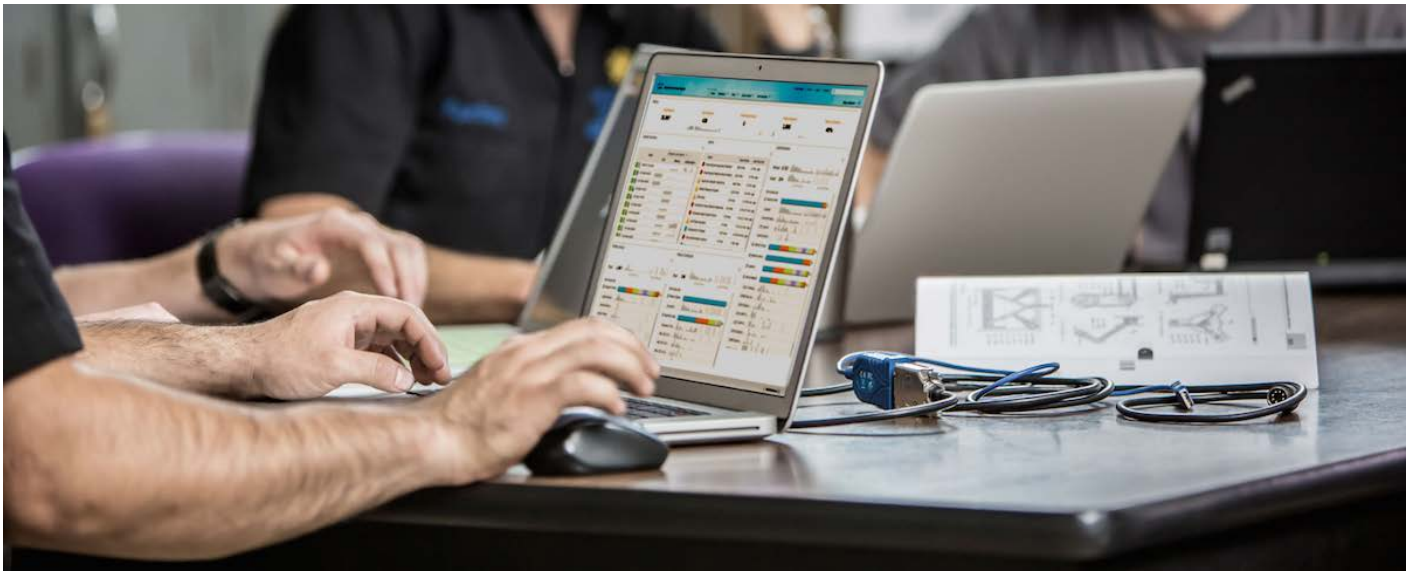

Cisco ISEのセットアップ基礎（原題：Boot Strapping）

セキュア アクセスを実現するハウツー ガイド シリーズ

作成者：シスコシステムズ合同会社

日付：2016 年 8 月

目次

最初のインストールと設定

概要

このガイドでは、Cisco Identity Services Engine（ISE）セットアップ プログラムを実行して Cisco ISE ハードウェア アプライアンスと仮想マシン環境を設定する方法について説明します。Cisco ISE をご注文いただくと物理アプライアンスにインストール済みで提供されますが、物理アプライアンスを再インストール（または再イメージ化）する必要が生じることがあります。このハウツー ガイドを参考資料として使用できます。後の項で、構成方法を段階を追って説明します。

セットアップ ダイアログの完了

ISE は仮想マシンにまったく新しくインストールする必要があります。インストールには 2 つの手順があります。

- 手順 1 - ISE ISO イメージからブートする
- 手順 2 - インストール プロセスを開始し、オペレーティング システムおよび ISE アプリケーションをインストールする

Vmware の設定方法の詳細については、『Cisco Identity Services Engine Hardware Installation Guide』の「Installing the Cisco ISE System Software on a VMware Virtual Machine」を参照してください。

手順 1 と 2 が完了すると、インストールが一時中断します。インストールを再開して完了する前に、セットアップ ダイアログを完了する必要があります。

手順 1

セットアップ を完了するには、次の手順を実行します。

ステップ 1　Ise-1 マシン コンソールにログインします。

```
*********************************************
Please type 'setup' to configure the appliance
localhost login:
*********************************************
```

ステップ 2　ログイン プロンプトで setup と入力し、セットアップ を開始します。

```
Enter hostname[]: ise
Enter IP address[]: 10.1.100.21
Enter IP default netmask[]: 255.255.255.0 Enter IP default gateway[]: 10.1.100.1 Enter default DNS
domain[]: demo.local Enter Primary nameserver[]: 10.1.100.10 Add/Edit another nameserver?Y/N : n
Enter Primary NTP server[time.nist.gov]: ntp.demo.local Add/Edit secondary NTP server?Y/N : n
Enter system timezone[UTC]: <return> Enter username[admin]: <return> Enter password: default1A
Enter password again: default1A Bringing up network interface...Pinging the gateway...
Pinging the primary nameserver ...
Do not use 'Ctrl-C' from this point on...Appliance is configured
Installing applications...Installing ise ...
Generating configuration...

=== Initial Setup for Application: ise ===
Welcome to the ISE initial setup.The purpose of this setup is to provision the internal ISE
database.This setup is non-interactive, and will take roughly 15 minutes to complete.Please be
patient.

Running database cloning script...
Running database network config assistant tool...Extracting ISE database content...
Starting ISE database processes...Restarting ISE database processes...Creating ISE M&T session
directory...Performing ISE database priming...
Generating configuration...Rebooting...
```

パスワード ポリシーが明示的に指定されていませんが、default1A のパスワードが機能します。セットアップ を完了した後、インストールが完了するまで約 45 分間かかります。ホスト名と DNS ドメイン名にはすべて小文字を使用することをお勧めします（しかし必須ではありません）。この ISE を Active Directory ドメインに参加させる予定であれば、ホスト名を 15 文字以下にしてください。

ステップ 3　セットアップ ダイアログを終了すると、インストールが続行し、最後に再起動します。次のログイン プロンプトが表示されると、インストールは完了です。

```
ise-1 login:
```

これで手順 1 は終わりです。

手順 2

セットアップ を完了するには、次の手順を実行します。

ステップ 4　セットアップ時に指定されたクレデンシャルを使用してログインします。

注：VM コンソール インターフェイスを使用して ISE CLI へのアクセスを続行することも、Secure Shell (SSH) プロトコルを使用することもできます。物理アプライアンスでは、シリアル ポートまたはキーボードおよびビデオを使用して ISE CLI にアクセスできます。

ステップ 5　show run と入力してセットアップ設定を確認します。
ステップ 6　リポジトリを設定します。

ISE リポジトリは、ISE にファイルをコピーしたり、ISE からファイルをコピーしたりするのに使用できるファイル ストレージ場所です。これらのリポジトリは、 パッチ適用や ISE アップグレードなどのさまざまな操作に使用できます。また、設定のバックアプや復元、サポート バンドルの作成なども可能です。

次の表にさまざまなリポジトリの種類を示します。

表 1. ISE リポジトリ タイプ

ISE リポジトリ	リポジトリ タイプ
CDROM	読み取りのみ
FTP	
HTTP	読み取りのみ
HTTPS	読み取りのみ
NFS	

ステップ 7 ISE で FTP リポジトリを設定する

```
ise-1/admin# config t
Enter configuration commands, one per line.End with CNTL/Z. ise-1/admin(config)# repository myFTP
ise-1/admin(config-Repository)# url ftp ftp.demo.local/
ise-1/admin(config-Repository)# user anonymous password plain admin@demo.local
ise-1/admin(config-Repository)# end
ise-1/admin# copy running-config startup-config
Generating configuration... ise-1/admin#
```

ステップ 8 show repository コマンドを使用して、ISE がリポジトリと通信できることを確認します。

ステップ 1 FTP サーバのディレクトリ リストが表示されます。

```
ise-1/admin# show repository myFTP
<file list>
ise-1/admin#
```

ステップ 2 注：このサンプル設定では、FTP サーバが管理者 PC 上にあり、FTP ホーム ディレクトリは <local directory>:\Configs です。

ステップ 9 時刻の同期が機能していることを確認します。

ステップ 10 Network Time Protocol（NTP）プライマリ サーバが設定された直後は、ISE が非同期状態のままです。

```
ise-pap-1/admin# sho ntp
Primary NTP : ntp.demo.local unsynchronized
time server re-starting polling server every 64 s
remote      refid   st t when poll reach   delay   offset jitter
==============================================================================
Warning: Output results may conflict during periods of changing synchronization.
```

ステップ 11 2、3 分後に、ISE は NTP プライマリ サーバと同期するはずです。アスタリスクは、どの時刻サーバと同期したかを示します。

```
ise-pap-1/admin# sho ntp
Primary NTP : ntp.demo.local
synchronised to NTP server (128.107.220.1) at stratum 5 time correct to within 459 ms
polling server every 64 s
remote              refid     st   t    when    poll   reach   delay    offset     jitter
==============================================================================
127.127.1.0     .LOCL.           10  1       5     64      377    0.000    0.000      0.001
127.107.220.1   .LOCL.      4  u     1026   1026   377    0.478  -866.81     60.476

Warning: Output results may conflict during periods of changing synchronization.
```

注：NTP サーバとの同期はすぐには行われないことがあります。ISE がローカル クロックを介して NTP サーバを選択するのに 10 分から 15 分間待たなければならないことがあります。

ステップ 12　ISE がローカル マシンに同期したと示される場合（下記参照）、NTP 時刻同期が機能していないことを意味します。

```
ise-pap-1/admin# show ntp
Primary NTP : ntp.demo.local synchronised to local net at stratum 11
time correct to within 10 ms polling server every 1024 s
remote            refid     st t     when    poll    reach    delay     offset     jitter
==============================================================================
127.127.1.0    .LOCL.    10 1       5      64     377    0.000      0.000       0.001
127.127.220.1 .LOCL.     4 u    1026    1024    377    0.478    -866.61      60.476

Warning: Output results may conflict during periods of changing synchronization.
```

注：NTP サーバとの同期はすぐには行われないことがあります。ISE がローカル クロックを介して NTP サーバを選択するのに 10 分から 15 分間待たなければならないことがあります。

ISE Web GUI アクセス

概要

初めて Cisco ISE Web ベースのインターフェイスにログインするときには、事前インストールされている評価ライセンスが使用されます。前の項で挙げた、HTTPS が有効なサポート対象ブラウザのみを使用する必要があります。本マニュアルで説明するとおりに Cisco ISE をインストールした後、Cisco ISE Web ベースインターフェイスにログインできます。

ISE との Web セッションを開始する

ログインして ISE との Web セッションを開始するには、次の手順を実行します。

ステップ 1　HTTP が有効なブラウザ ウィンドウを開き、http://ise.demo.local を参照します。

注：この URL は前の項のサンプル設定に基づいています。ブラウザにアクセスするには、http://<host name>.<domain name> を使用します。HTTPS が有効なブラウザは、Mozilla Firefox 2.6 と 9、および Microsoft Internet Explorer 8 と 9 です。

セッションは、セキュアな Cisco ISE ログイン ページ https://ise.demo.local/admin にリダイレクトされます。

ステップ 2　ログイン ページで、セットアップ時に定義したユーザ名とパスワードを入力します。
ステップ 3　[ログイン（Login）] をクリックすると、図 2 に示すように Cisco ISE のダッシュボードが表示されます。

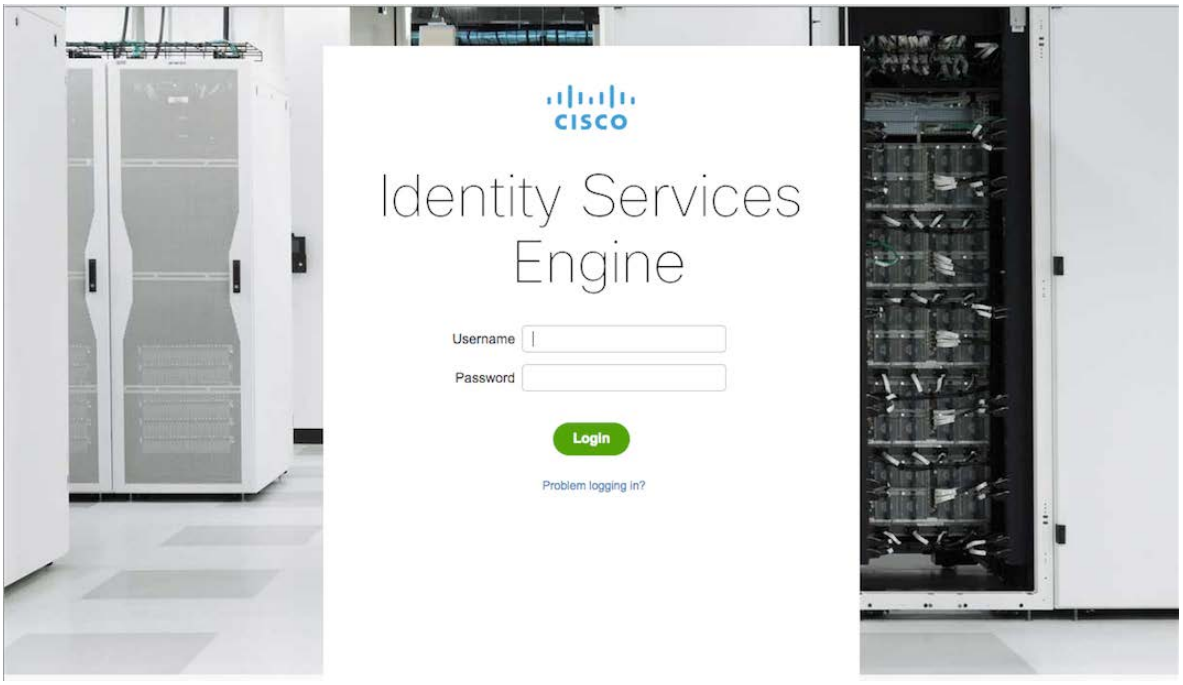

図1.　ISE Web ログイン

証明書と認証局

概要

このガイドでは ISE 証明書の生成方法、認証局（CA）が ISE に証明書を発行する方法、その証明書を ISE にインストールする方法について説明します。Cisco ISE のインストール時に、デフォルトの自己署名証明書が生成されます。自己署名証明書はサンプルやデモ用には十分ですが、Cisco ISE を実稼働環境で使用する場合にはあまりお勧めできません。ISE との通信を保護するには、その通信が認証関連のものであるか、ISE の管理（ISE の Web インターフェイスを使用した設定など）のためであるかに関わらず、X.509 証明書と証明書トラスト チェーンを設定して、非対称暗号化を有効にする必要があります。

注：時刻同期は証明書の操作に極めて重要です。NTP をすでに設定したこと、および正しい時間であることを確認してください。

Cisco ISE の構成 - 証明書と CA の信頼

注：特定のチェーンでは、証明書要求が作成される前に、チェーン全体を正常にインポートする必要があります。

ステップ 1　Cisco Identity Services Engine にログインして、[管理（Administration)] タブをクリックします。
ステップ 2　メニュー バーの [システム（System）] リンクをクリックして、[証明書（Certificates）] を選択します。

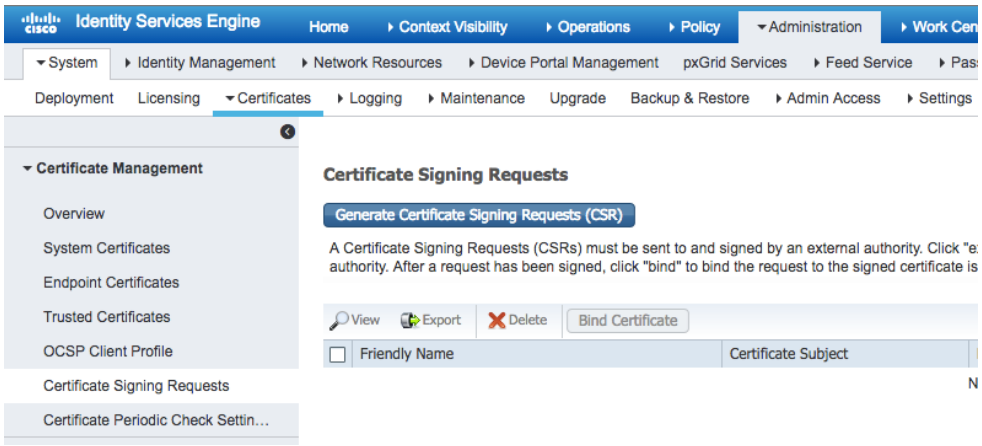

図2.　証明書（Certificates）

ステップ 3　左パネルから[証明書署名要求（**Certificate Signing Requests**）] を選択します。
ステップ 4　[証明書署名要求の生成（Generate Certificate Signing Request）]ボタンをクリック します。

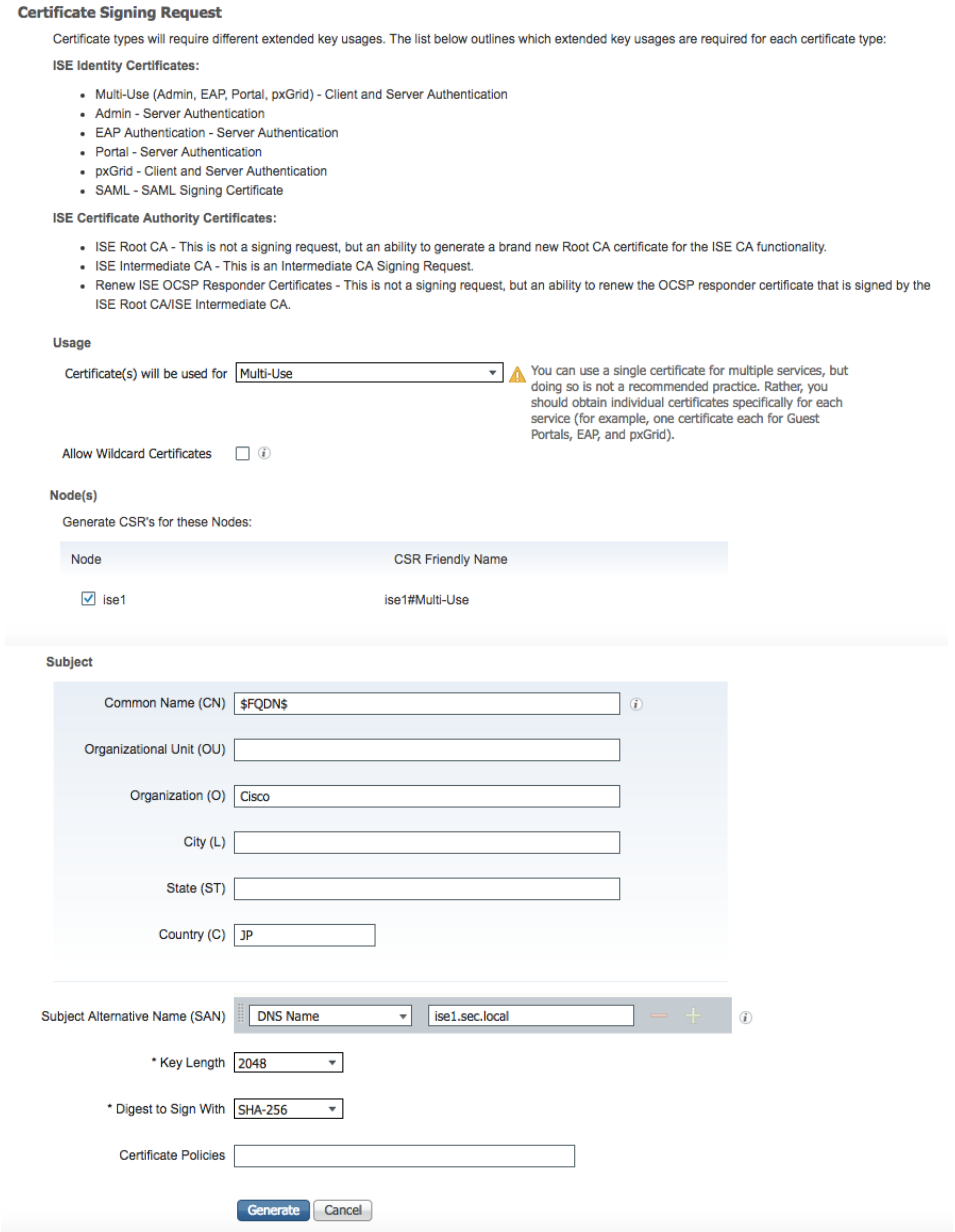

図3. 証明書署名要求の生成（Generate Certificate Signing Request Panel）

注： Subject Alternative Name（SAN）拡張フィールド内のDNS名、またはCommon Name(CN)のフィールド中に、ISEノードのFQDNを含んでいる必要があります。ワイルドカード証明書を使用することもできます。

注： **Cisco** ISEでは、管理（Admin）、認証（EAP Authentication）、ポータル（Portal）などの各種サービスが利用する証明書を個別に指定することができます。 複数のサービスで単一の共通証明書を使うことも可能ですが、個別指定が推奨です。

ステップ 5 Node(s) の項目で、対象のISEノードにチェックを入れます。

ステップ 6 SubjectおよびSubject Alternative Name(SAN) に適切な値を入力します。[証明書の件名（Certificate Subject）] フィールドは$FQDN$のままにしておきます。

ステップ 7 [送信（**Submit**）] ボタンをクリックします。

図4.

ステップ 8 [エクスポート（**Export**）] リンクをクリックします。

ステップ 9 pem ファイルを簡単にアクセスできる場所に保存します。

CA ルート証明書をダウンロードし、証明書を発行する

ステップ 1 CA を参照します。

ステップ 2 [CA 証明書、証明書チェーン、または CRL をダウンロード（Download a CA certificate, certificate chain, or CRF）] というリンクをクリックします。

注：ここでは Microsoft CA を使用します。したがって、http://ad.cts.local/certsrv/ を参照します。企業で使用される CA によって、証明書要求の手順は異なります。Microsoft CA を使用する場合は、Internet Explorer を使用するとよりスムーズに作業が進むことがわかっています。

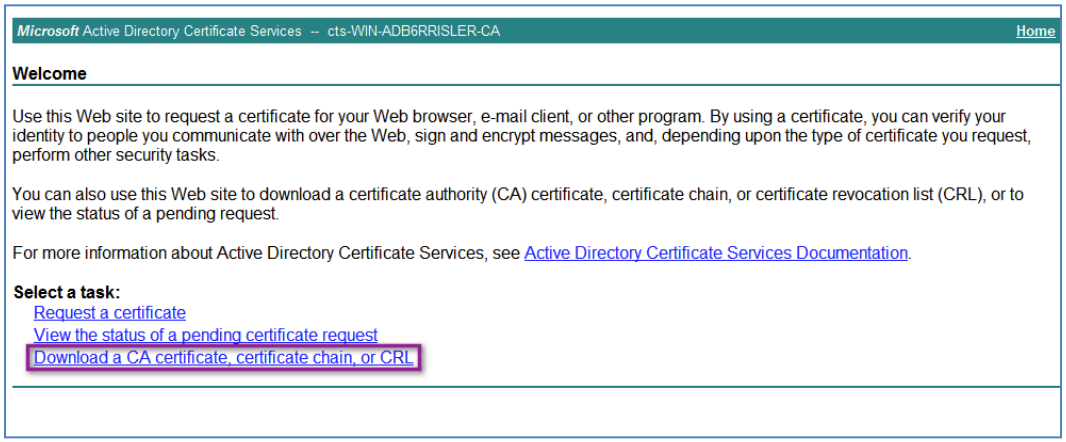

図5. CA 証明書のダウンロード

ステップ 3 [CA 証明書のダウンロード（Download CA certificate）] をクリックします。

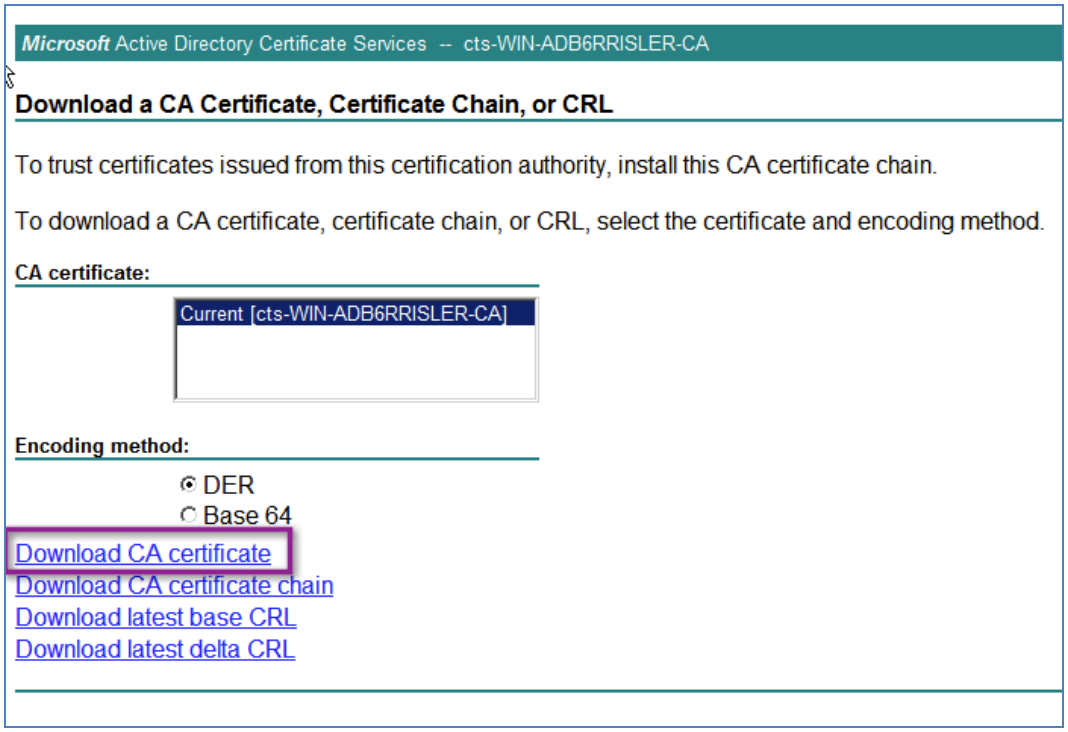

図6. [証明書（Certificate）] と [エンコード方式（Encoding Method）] を選択します。

ステップ 4 この結果生成された .cer ファイルを、アクセスしやすい場所に保存します。

Cisco ベスト プラクティス：ファイルには RootCert.cer など、固有の名前を付けます。

ステップ 5 右上隅の [ホーム（Home）] をクリックします。

ステップ 6 [証明書を要求する（Request a certificate）] をクリックします。

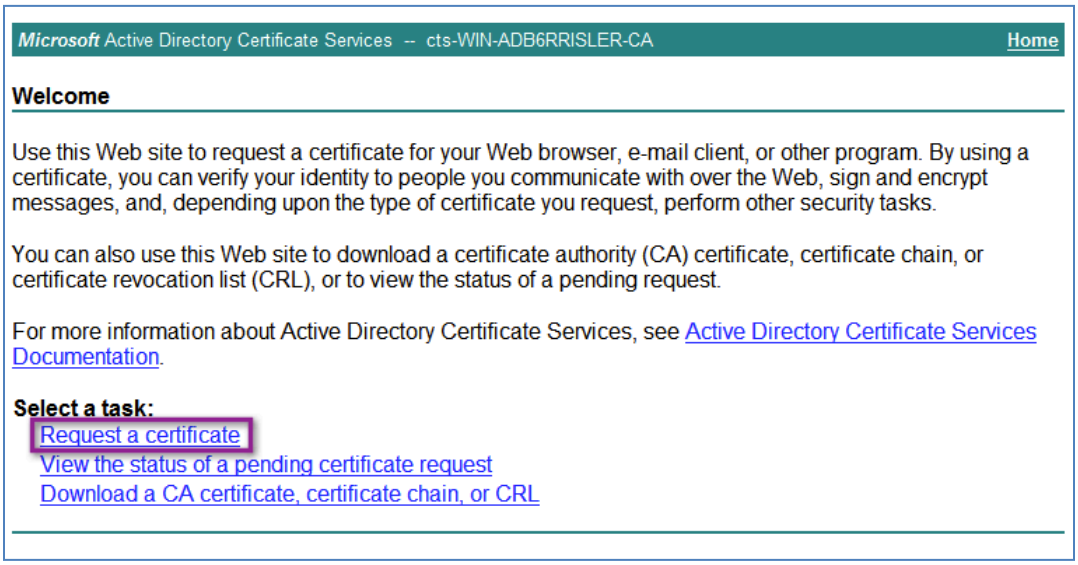

図7. 証明書を要求する

ステップ 7 [証明書の要求の詳細設定（Advanced certificate request）] をクリックします。

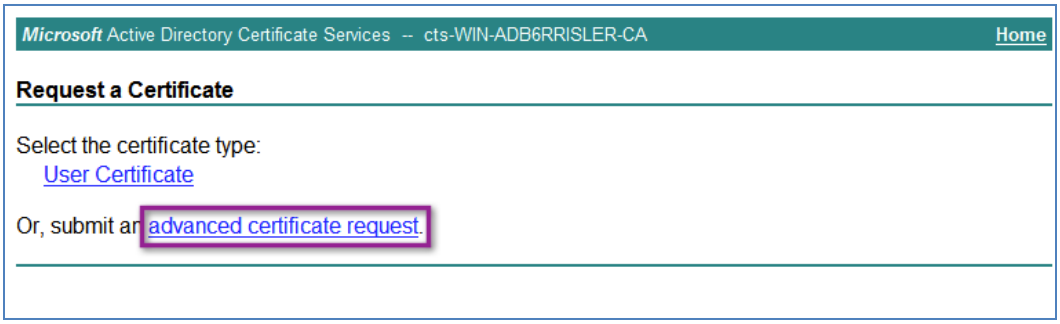

図8. 証明書の要求の詳細設定（Advanced certificate request）

ステップ 8 [ベース 64 エンコード CMC または PKCS #10 ファイルを使用して証明書要求を送信するか、ベース 64 エンコード PKCS #7 ファイルを使用して更新要求を送信する（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file）] というオプションを選択します。

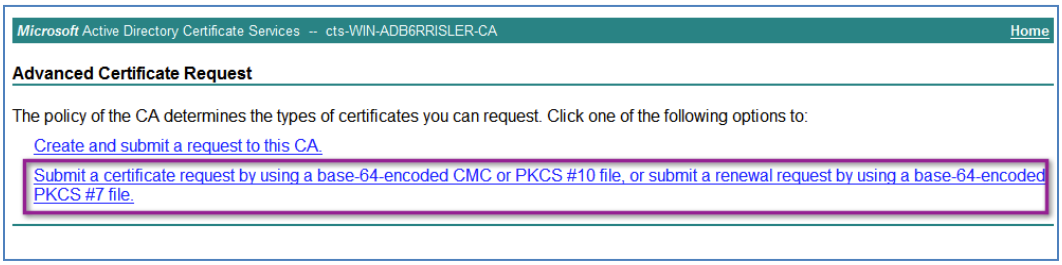

図9. 証明書の要求オプションの選択

ステップ 9 メモ帳または任意のテキスト エディタを使用して、手順 2 で保存した .pem ファイルを開きます。

ステップ 10 ファイルの内容全体を強調表示して、[編集（Edit）] → [コピー（Copy）] を選択します。

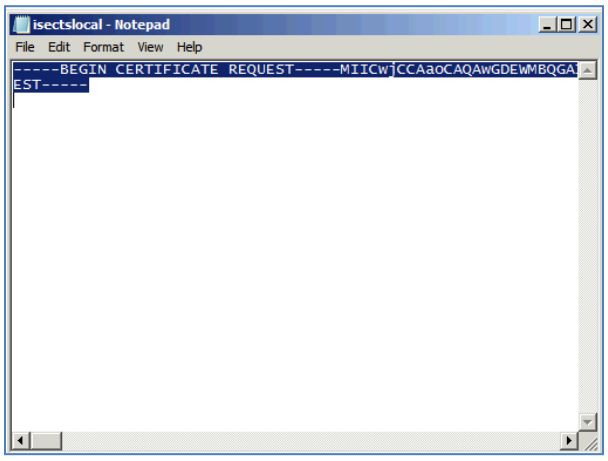

図10. 証明書のコピー

ステップ 11 証明書要求の .pem ファイルの内容を CA ウィンドウの [保存済み要求（Saved Request）] テキスト ボックスに貼り付けます。[証明書のテンプレート（Certificate Template）] は [Web サーバ（Web Server）] に設定する必要があります。

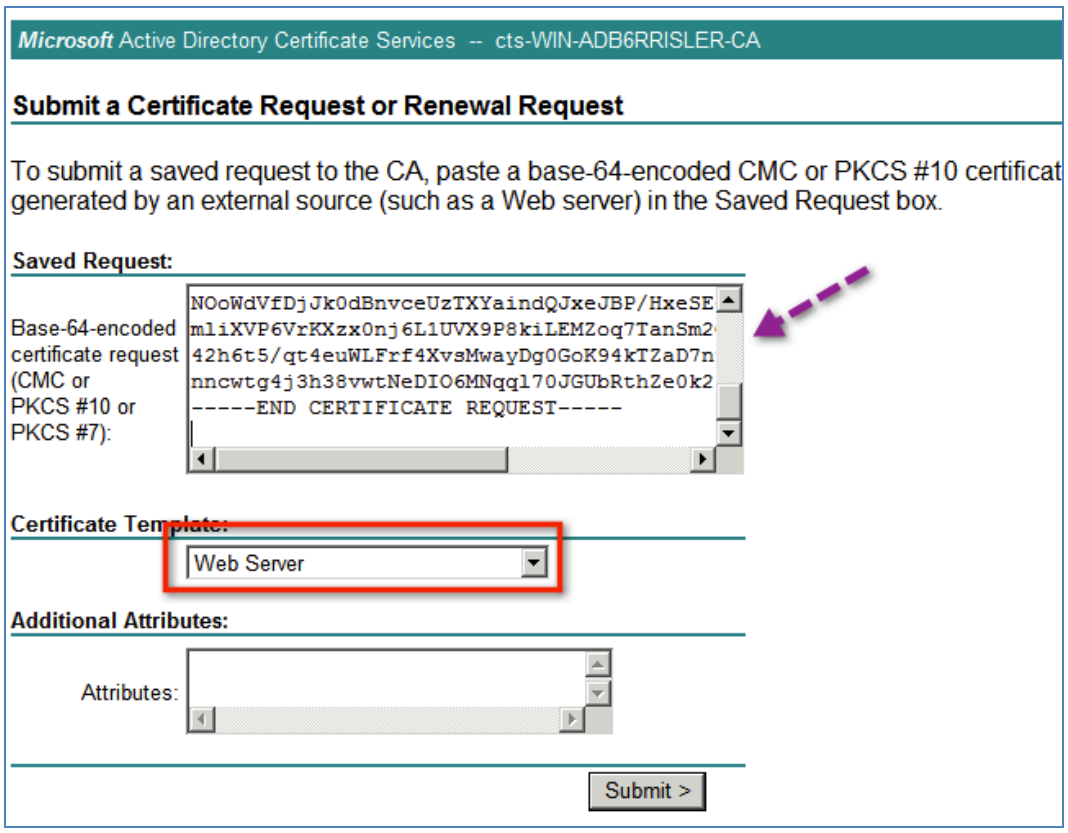

図11. 証明書要求の送信

ステップ 12 Cisco ISE 管理インターフェイスで、[管理（Administration）] → [システム（System）] → {証明書（Certificates）} → [信頼された証明書（Trusted Certificates）] と移動します。

ステップ 13 [インポート（Import）] をクリックします。

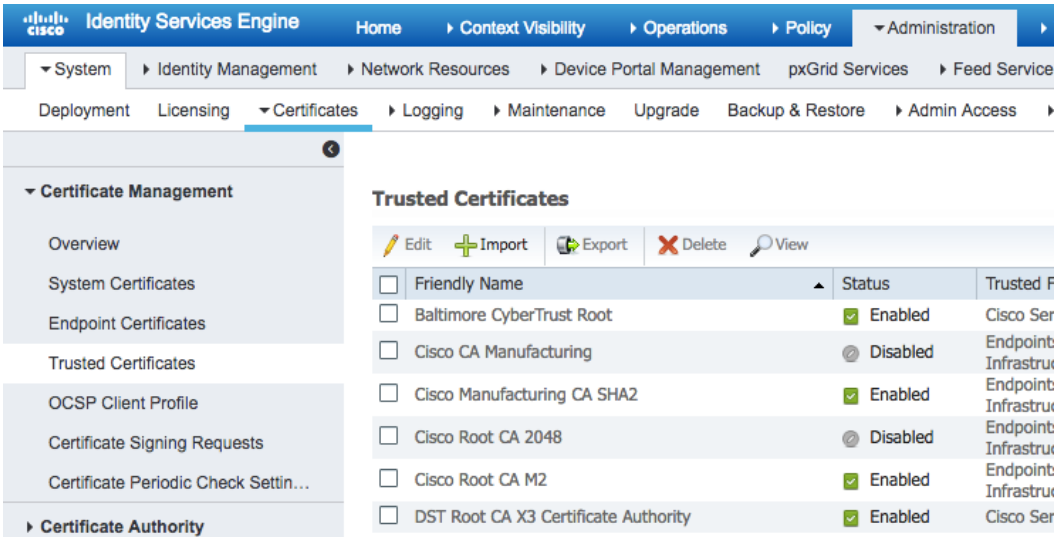

図12. 証明書のインポート

ステップ 14 手順 3 のステップ 3 で保存した CA ルート証明書を参照します。

ステップ 15　「クライアント認証とSyslogの信頼（Trust for client authentication and Syslog）」というチェックボックスを選択してから「証明書拡張子の検証する（Validate Certificate Extensions）] のチェックボックスを選択します。

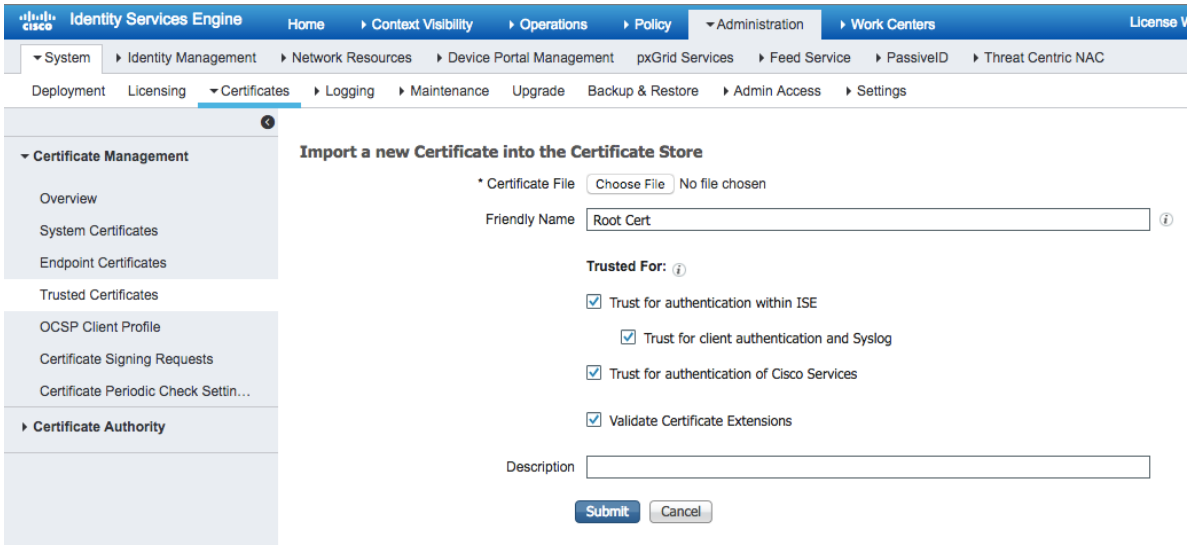

図13.　EAP-TLS による信頼

ステップ 16　[実行（Submit）] をクリックします。

新しいローカル証明書のインストール

CA ルート証明書を信頼できたので、次に自己署名証明書を CA 発行の証明書に取り替え、完了した証明書署名要求（CSR）を削除します。

ステップ 1　[管理（Administration）] → [システム（System）] → [証明書（Certificates）] → [証明書署名要求（Certificate Signing Requests）] に進み、発行したCSR にチェックを入れてから[証明書のバインド（Bind Certificate）] をクリックします。

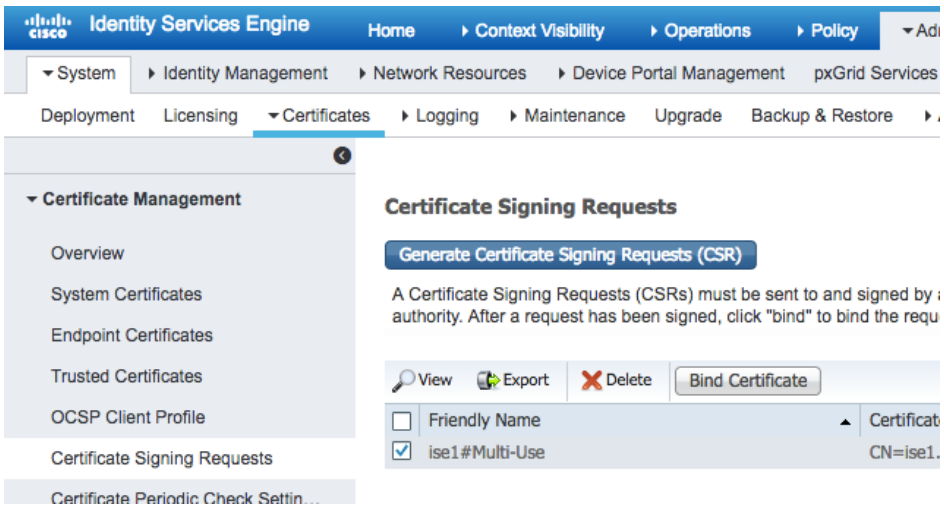

図14.　証明書のバインド

ステップ 2　Cisco ISE 用に CA により発行された証明書を参照します。[管理（Admin）] および [EAP認証（EAP Authentication）] のチェックボックスを選択します。

ステップ 3　[送信（Submit）] をクリックします。

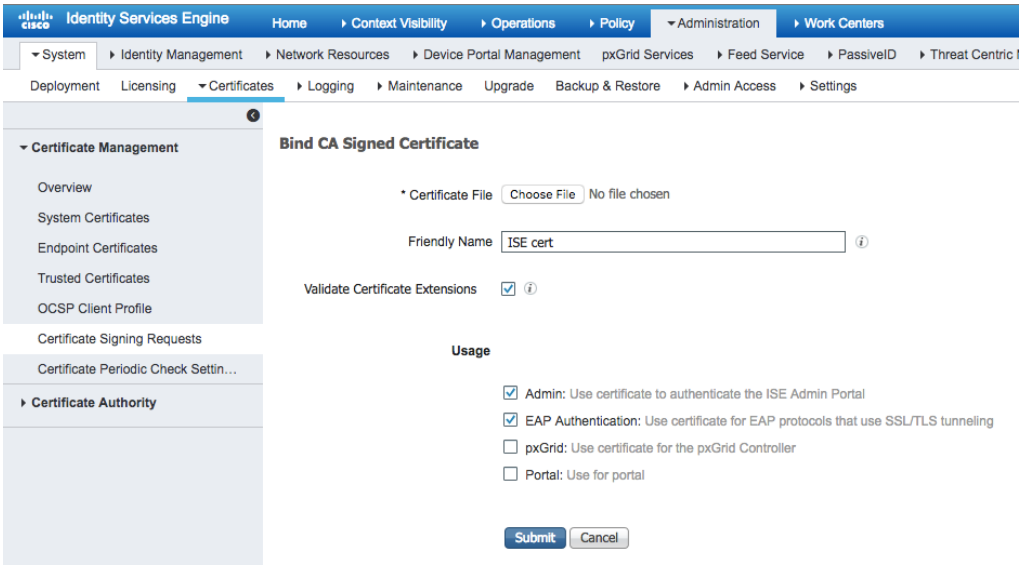

図15.　CA 署名付き証明書のバインドの選択画面

注：Cisco ISE サーバと同じホスト名の付いた証明書署名要求（CSR）を作成しなかった場合（または、同じドメイン名を使用しなかった場合）は、エラー メッセージが表示されます。古い CSR を削除するか、ホスト名だけを変更してもう一度起動します。

古い証明書と CSR のクリーンアップ

ステップ 1　作成したCSRを選択します。

ステップ 2　[削除（Delete）] をクリックします。

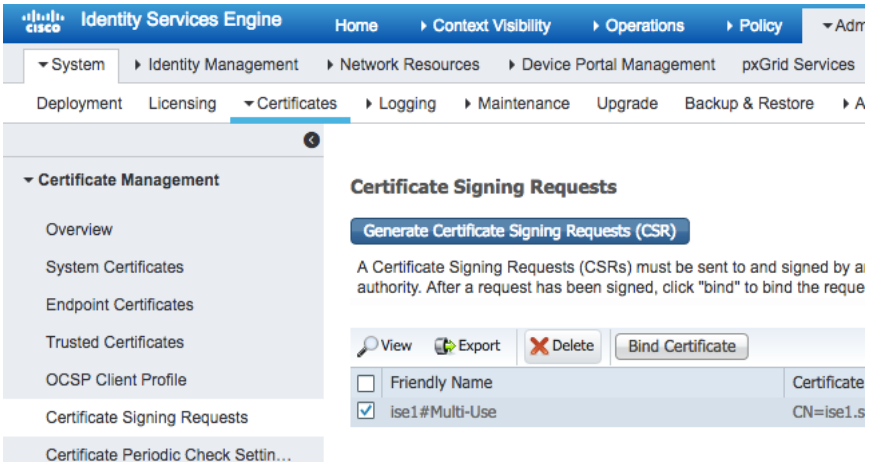

図16.　古い署名要求の削除

ステップ 3 [システム証明書（System Certificate）]をクリックし、「デフォルトの自己署名サーバ証明書（Default self-signed server certificate）」というチェックボックスを選択します。

ステップ 4 [削除（Delete）] をクリックします。

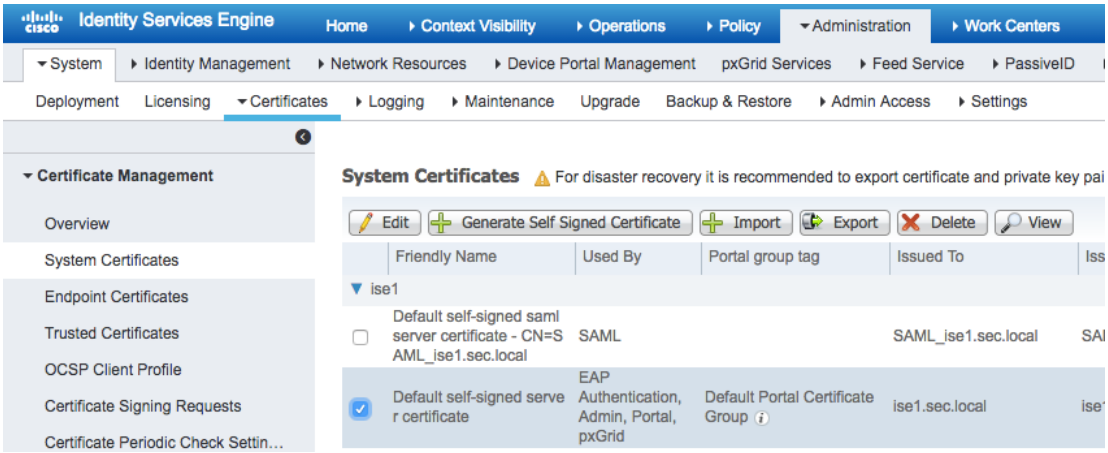

図17. 古い証明書の削除

ネットワーク デバイスの追加

概要

ネットワーク クライアントを認証/許可するために Cisco ISE に RADIUS 要求を送信する可能性のあるすべてのスイッチまたはワイヤレス LAN コントローラ（WLC）を、Cisco ISE に追加する必要があります。Cisco ISE にあるデフォルト デバイスを設定して、すべてのネットワーク デバイスが RADIUS 要求を送信できるようにすることができますが、セキュリティ上、この機能の使用はあまりお勧めできません。

完全なポリシー レベルの作成と、詳細レベルのレポート作成を可能にするには、すべてのデバイスを個別に Cisco ISE に追加し、ネットワーク デバイス グループ（NDG）を使用してそれらのネットワーク デバイスを編成することをお勧めします。

注：ネットワーク デバイスを一括インポートし、それらのデバイスを各 NDG に割り当てることができるよう、Cisco ISE にはインポート/エクスポート機構が用意されています。詳細については、『Cisco ISE User Guide』（http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_admin.html）を参照してください。

ネットワーク デバイス グループの設定

NDG は適切に使うと強力なツールになります。Cisco ISE には、ポリシー決定時に任意の数の属性を使用できる強みがあります。NDG メンバーシップは、ポリシー条件として使用できる、そうした属性の 1 つです。たとえば、スイッチ用の NDG を作成し、VPN デバイス用の NDG を別に作り、WLC 用に 3 つ目の NDG を作成するという例が考えられます。

Cisco ベスト プラクティス：少なくとも、デバイス タイプと場所に関して必ず NDG を使用してください。

ステップ 1　[管理（Administration）] → [ネットワーク リソース（Network Resources）] → [ネットワーク デバイス グループ（Network Device Groups）] に移動します。

デフォルトで、最上位の NDG タイプには、「すべてのデバイス タイプ（All Device Types）」と「すべてのロケーション（All Locations）」という 2 つのタイプがあります。これらのタイプは、ほとんどの導入環境で基礎として使用するのに適しています。導入環境によっては、複数の場所のサブグループを作成しなければならない場合もあります。可能性は事実上無限にあります（次のサンプル階層を参照）。

グループの構造は階層型です。グループ構造の例として「すべての場所」→「北米」 →「アメリカ合衆国」 →「サンノゼ」 →「M ビル」 →「1 階」がありますが、任意のレベルのグループ階層をポリシーで使用できます。つまり、ポリシーで「アメリカ合衆国」を選択し、すべてのグループのすべてのデバイスを「アメリカ合衆国」の下に入れることができます。

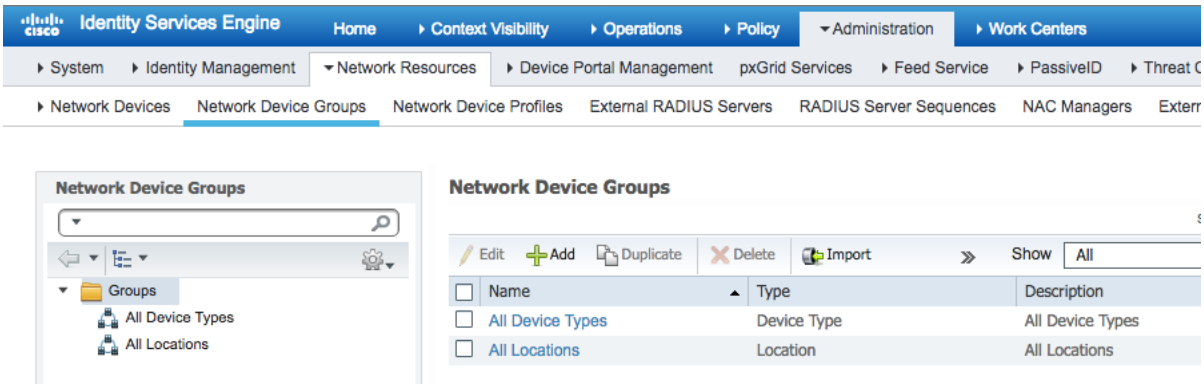

図18. ネットワーク デバイス グループ

ステップ 2 [全てのデバイスタイプ（All Device Types）] を選択します。[追加（Add）] をクリックします。

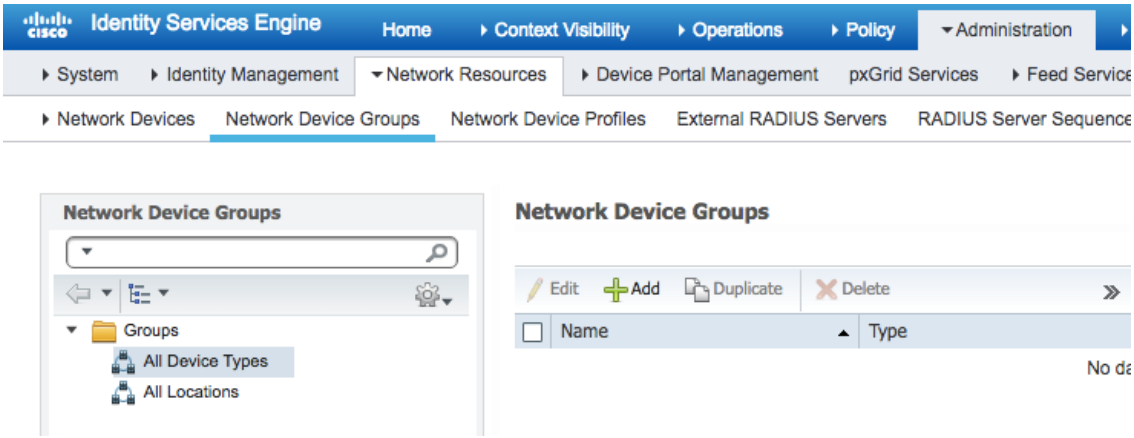

図19. ネットワーク デバイス タイプの追加

ステップ 3 [名前（Name）] フィールドに名前「**Switch**」を入力し、[実行（Submit）] をクリックします。

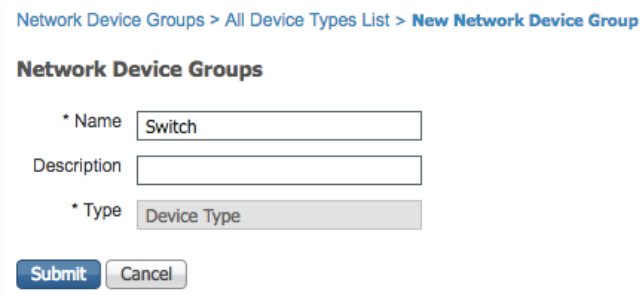

図20. スイッチの追加

ステップ 4　このプロセスを繰り返して、適切な NDG 階層を作成します。図 21 は階層の例を示しています。

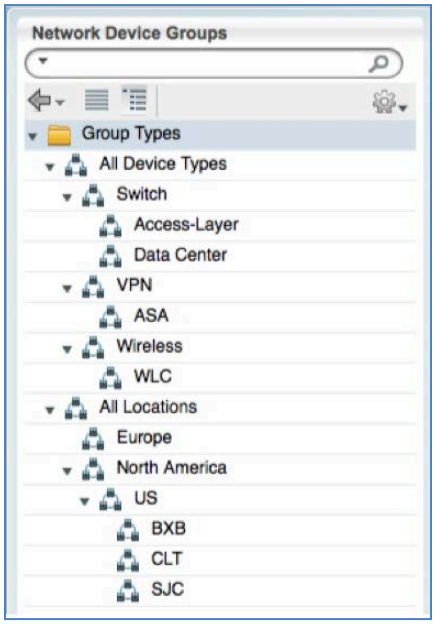

図21. グループ タイプ

ネットワーク デバイスの追加

ステップ 1　[管理（Administration）] → [ネットワーク リソース（Network Resources）] → [ネットワーク デバイス（Network Devices）] に移動して、[追加（Add）] をクリックします。

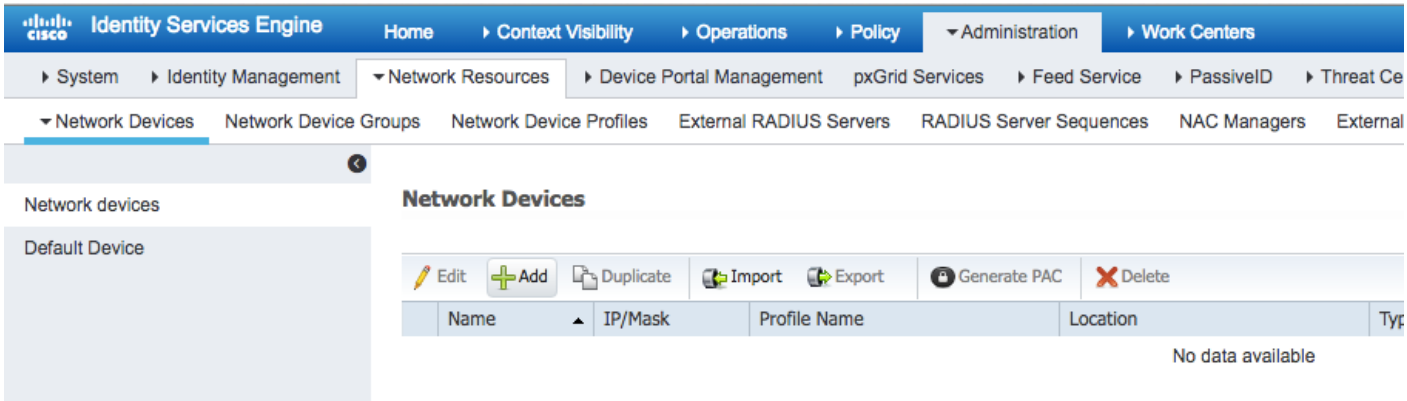

図22. ネットワーク デバイス

ステップ 2　[名前（Name）]、[IPアドレス（IP Address）]、[ネットワーク デバイス グループ（Network Device Group）] の各フィールドに入力します。

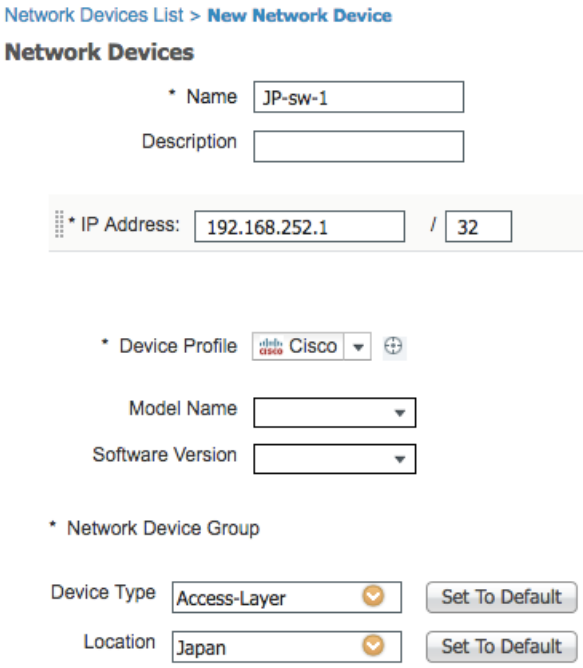

図23. ネットワーク デバイスの詳細

ステップ 3 すべてのネットワーク デバイス（「ポリシー適用ポイント」ともいう）について繰り返します。

注：一括管理のために、ネットワーク デバイスを CSV ファイルでインポートすることができます。詳細については、『Cisco ISE User Guide』（http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_admin.html）を参照してください。

表 2. ネットワーク デバイス

セクション	目的
全般設定	
名前（Name）	後で区別しやすい名前を使用してください。この名前はすべてのモニター、ダッシュボード、およびレポートに表示されます。
説明（Description）	オプション
IPアドレス（IP Address）	スイッチの設定設定セクションで RADIUS 通信用に選択したソース インターフェイスに一致する必要があります。ベスト プラクティスとしては、管理用にループバック インターフェイスを使用してください。
モデル名（Model Name）	オプション

セクション	目的
ソフトウェア バージョン（Software Version）	オプション
ネットワーク デバイス グループ（Network Device Group）	
参照先 (Location)	できるだけ具体的に入力します。
デバイスタイプ（Device Type）	できるだけ具体的に入力します。
認証設定	
プロトコル（Protocol）	「RADIUS」と自動的に入力されます。
共有秘密鍵（Shared Secret）	スイッチに設定した RADIUS キーに一致する必要があります。
SNMP 設定（デバイス プロファイルに使用）	
SNMP バージョン（SNMP Version）	組織で使用されているバージョンを選択します。
SNMP RO コミュニティ（SNMP RO Community）	SNMP はデバイス プロファイルの目的にのみ使用されます。Cisco ISE はスイッチを調べて、Cisco Discovery Protocol テーブルや Link Layer Discovery Protocol（LLDP）テーブルなどの内容を確認します。
SNMP ユーザ名（SNMP Username）	SNMPv3 での使用 - スイッチの設定と一致する必要があります。
セキュリティ レベル（Security Level）	SNMPv3 での使用 - スイッチの設定と一致する必要があります。
認証プロトコル（Auth Protocol）	SNMPv3 での使用 - スイッチの設定と一致する必要があります。

セクション	目的
プライバシー プロトコル（Privacy Protocol）	SNMPv3 での使用 - スイッチの設定と一致する必要があります。
ポーリング間隔（Polling Interval）	デフォルトのポーリング間隔（3,600 秒）の変更は推奨できません。
リンク トラップ クエリー（Link Trap Query）	スイッチからの linkup および linkdown SNMP トラップを受け入れるよう、Cisco ISE を設定します。このチェックボックスは選択したままにしてください。
MAC トラップ クエリー（MAC Trap Query）	スイッチからの mac アドレステーブル タイプのトラップを許容するように、Cisco ISE を設定します。このチェックボックスは選択したままにしてください。
セキュリティ グループ アクセス（SGA）（Security Group Access (SGA)）：本導入ガイドのこの段階では使用しません。SGA の項で説明します。	
デバイス設定導入（Device Configuration Deployment）：本導入ガイドのこの段階では使用しません。SGA の項で説明します。	

付録 A

シスコ セキュア アクセス システム

- http://www.cisco.com/en/US/products/ps11640/products_implementation_design_guides_list.html

デバイス設定ガイド

- Cisco Identity Services Engine User Guides
  http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、および Cisco NX-OS ソフトウェアの各リリースの詳細情報については、次の URL を参照してください。

- Cisco Catalyst 2900 シリーズのスイッチ：
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 3000 シリーズのスイッチ：
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 3000-X シリーズのスイッチ：
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 4500 シリーズのスイッチ：
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- Cisco Catalyst 6500 シリーズのスイッチ：
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- Cisco ASR 1000 シリーズのルータ：
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

Cisco ワイヤレス LAN コントローラ

- http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html