Cisco pxGrid と Cisco StealthWatch 6.7.1 の導入

目次

このマニュアルについて **3**
はじめに **4**
SMC および ISE pxGrid ノードでの CA 署名付き証明書の使用 **5**
CA 署名操作用にカスタマイズされた pxGrid テンプレート 5
ISE 2.0 の設定 9
SMC アイデンティティ証明書の作成および CA ルート証明書のダウンロード 16
SMC 信頼ストアへの CA ルート証明書のアップロード 17
SSL サーバ ID への SMC アイデンティティ証明書のアップロード 17
SSL クライアント ID への SMC アイデンティティ証明書のアップロード 18
ISE からの Syslog イベントの受信 18
SMC クライアント - ホスト Java ストアで CA 証明書を信頼するための設定 21
SMC クライアントの例 21
SMC および ISE pxGrid ノードでの自己署名証明書の使用 **24**
自己署名証明書用の ISE 1.3/1.4 の設定 24
pxGrid の有効化 25
自己署名証明書用の ISE 2.0 の設定 26
SMC への ISE アイデンティティ証明書のエクスポート 27
SMC 用の自己署名証明書の作成 28
SMC への自己署名証明書のアップロード 29
ISE 信頼システム証明書ストアへの SMC 自己署名証明書のアップロード 31
適応型ネットワーク制御（ANC）の有効化 **32**
CA 署名付き証明書を使用したテスト **34**
自己署名証明書を使用したテスト **37**
参考資料 **40**
付録 **41**
MAC での SSH の有効化 41
トラブルシューティング 42
pxGrid アクティブ スタンバイ設定の使用 42
SMC ANC ミティゲーション エラー メッセージ：ISE への検疫要求の送信に失敗しました（Quarantine request failed to be sent to ISE） 42
ISE pxGrid ノードに pxGrid への接続がない 42

このマニュアルについて

このマニュアルは、シスコのフィールド エンジニア、テクニカル マーケティング エンジニア、パートナー、お客様を対象に、Cisco Identity Service Engine（ISE）1.3 以降を使用した Cisco platform exchange Grid（pxGrid）と Cisco StealthWatch 6.7.1 の導入をガイドすることを目的としています。

このマニュアルでは、StealthWatch および ISE がすでにインストール済みであると想定して、以下について説明します。

- ISE pxGrid ノードと SMC（StealthWatch Management Center）の両方に対応するようにカスタマイズした pxGrid テンプレートの作成
- 認証局（CA）署名付き証明書または自己署名証明書を使用する pxGrid ノード操作用の ISE の設定
- 認証局（CA）署名付き証明書または自己署名証明書を使用する pxGrid クライアントとしての StealthWatch Management Console（SMC）の設定
- Cisco ANC（適応型ネットワーク制御）pxGrid ミティゲーション アクション用の StealthWatch Management Center（SMC）の設定

ここでは、pxGrid を有効化したスタンドアロン環境に ISE が導入されているものとします。

CA 署名付き証明書を使用する実稼働環境に pxGrid を導入する場合は、次のマニュアルの「Configuring pxGrid in an ISE Distributed Environment」を参照してください：http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html

はじめに

Cisco StealthWatch は、ネットワークトラフィックおよびユーザ トラフィックをリアルタイムに可視化して、異常動作、APT、インサイダー脅威、DDoS、その他のマルウェアを検出するネットワーク セキュリティ ソリューションです。また、Lancope は、ネットワーク全体の証跡の収集と分析を行い、これらの脅威の攻撃前、攻撃中、攻撃後に対応して、これらのエンドポイントでのリアルタイムのミティゲーション アクションの実行を要求します。

Cisco Platform Exchange Grid（pxGrid）は、エコシステム パートナーが Cisco Identity Service Engine（ISE）からユーザおよびデバイスのコンテキスト情報を取得できる統合フレームワークです。ISE から情報のトピックが発行され、エコシステム パートナーは、その発行されたトピックにサブスクライブして ISE セッション情報を取得し、エンドポイントで適応型ネットワーク制御（ANC）ミティゲーション アクションを実行します。

Cisco StealthWatch は、ISE pxGrid ノードにクライアントとして登録し、エンドポイント保護サービス機能にサブスクライブして、エンドポイントで ANC ミティゲーション アクションを実行します。これらのミティゲーション アクションには、検疫/検疫解除、ISE による IEEE 802.1X エンドポイント認証などがあります。

このマニュアルでは、StealthWatch 6.7.1 以降および ISE 1.3 以降がインストール済みであることを前提としています。

pxGrid クライアントとしての StealthWatch は、認証局（CA）署名付き証明書または自己署名証明書を pxGrid 操作に使用する必要があります。両方の証明書の使用例について説明します。

- 署名付き証明書の使用例としては、CA 信頼ルート証明書のインポート、SMC での公開キー ペアの生成、ISE pxGrid ノード証明書に署名した同じ CA による署名などが含まれます。ここでは、CA ルート証明書が ISE 信頼システム証明書ストアにインストール済みであり、pxGrid ISE ノード証明書が ISE システム証明書ストアにインストール済みであることを前提としています。

- 自己署名証明書の使用例では、ISE pxGrid ノードの設定手順と自己署名公開キーまたは秘密キーを SMC で作成する手順を詳細に説明します。

- StealthWatch 6.7.1 では、pxGrid 操作用に、クライアント ID SSL ストアにアイデンティティ証明書がアップロードされている必要があります。

両方の使用例には、SMC ミティゲーション アクションの設定と例が含まれています。

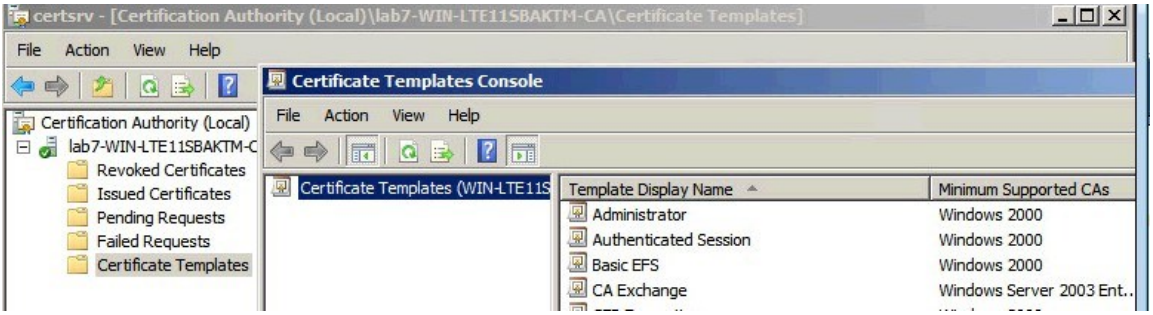
SMC および ISE pxGrid ノードでの CA 署名付き証明書の使用

この項では、SMC に CA 署名付き証明書を導入し、Java クライアントを使用する手順について説明します。

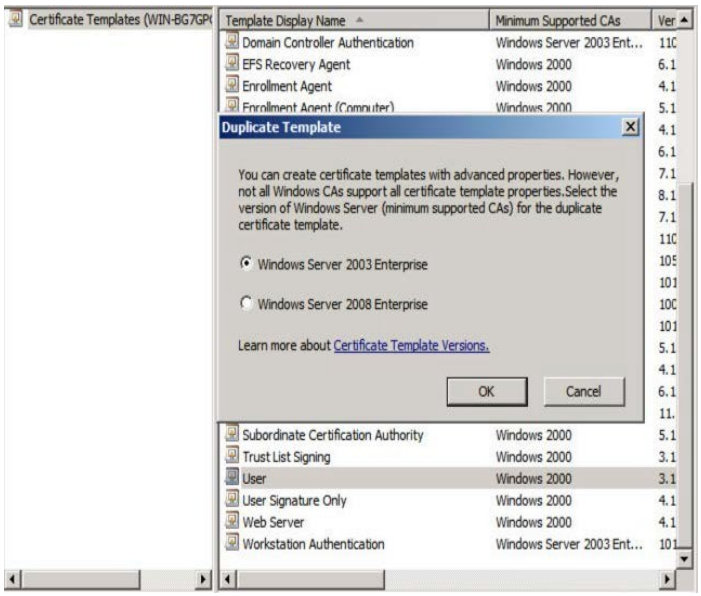
CA 署名操作用にカスタマイズされた pxGrid テンプレート

pxGrid クライアント、SMC、ISE pxGrid ノード間での pxGrid 操作では、クライアント認証とサーバ認証の両方の Enhanced Key Usage（EKU）を持つように pxGrid テンプレートをカスタマイズする必要があります。これは、SMC と ISE pxGrid ノードの両方が同じ認証局（CA）によって署名される CA 署名環境に必須です。

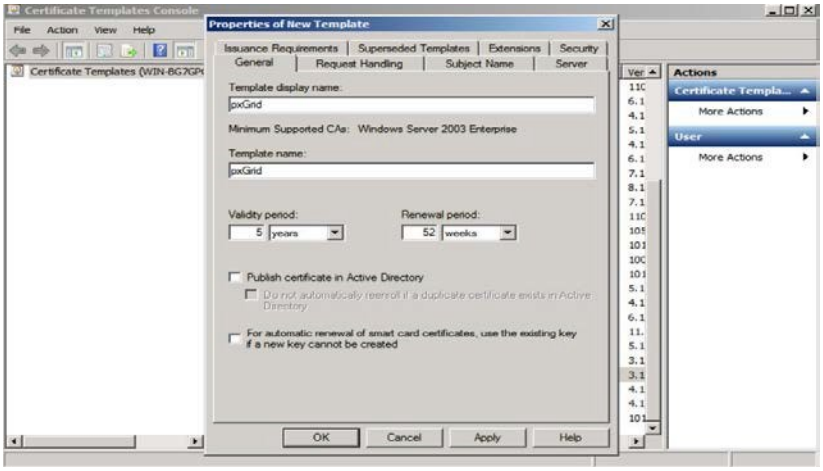
ステップ 1 [管理ツール（Administrative Tools）] -> [認証局（Certificate Authority）] を選択し、CA サーバの横の [+] をクリックした後、ドロップダウン リストから [証明書テンプレート（Certificate Templates）] を右クリックして、[管理（Manage）] を選択します。



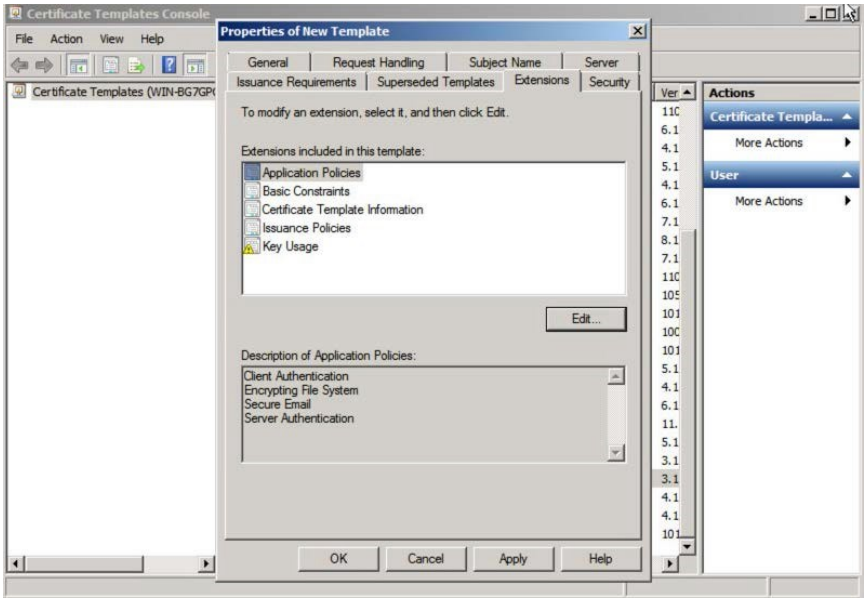
ステップ 2 右クリックして [ユーザテンプレートの複製（Duplicate User template）] を選択し、[Windows 2003 Enterprise] を選択して、[OK] をクリックします。



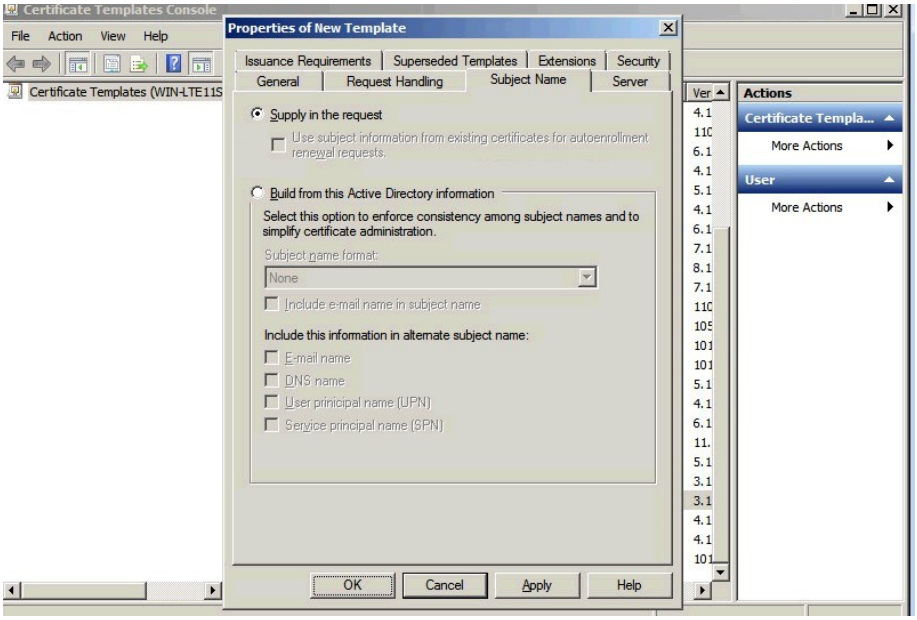
ステップ 3 証明書テンプレートの名前を入力し、[Active Directory で証明書を発行する（Publish certificate in Active Directory）] をオフにして、[有効期間（Validity period）] および [更新期間（Renewal period）] を指定します。



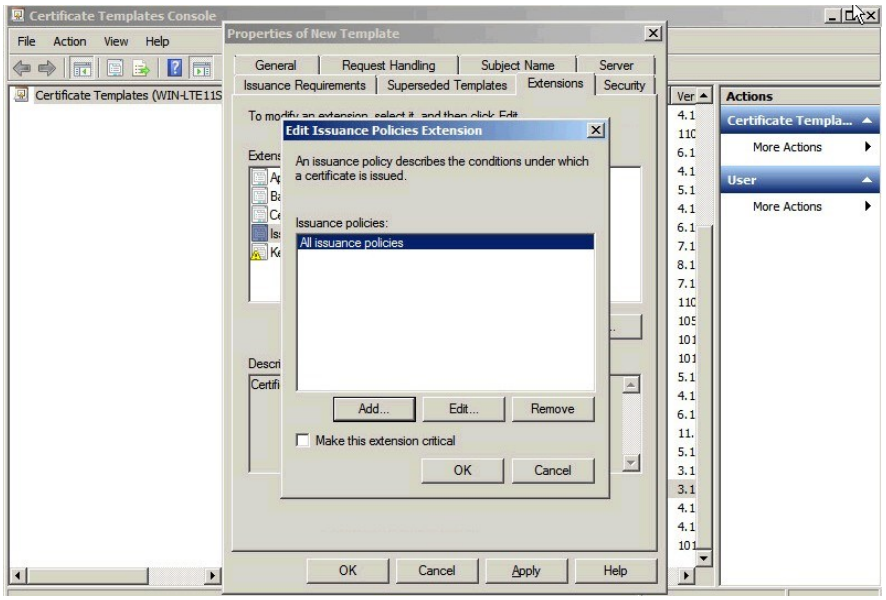
ステップ 4 [拡張（Extensions）] -> [追加（Add）] -> [サーバ認証（Server Authentication）] -> [OK] -> [適用（Apply）] の順にクリックします。



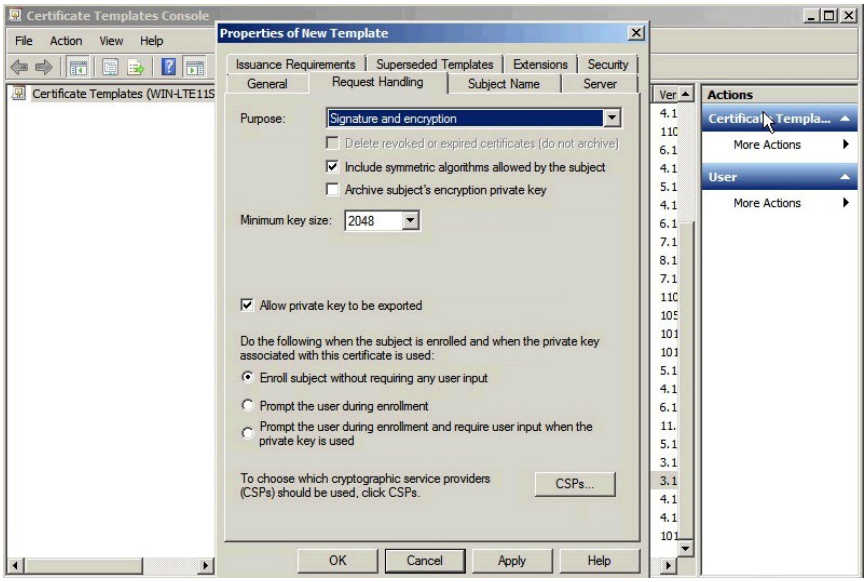
ステップ 5 [サブジェクト名（Subject Name）] をクリックして、[要求に含まれる（Supply in request）] をオンにします。



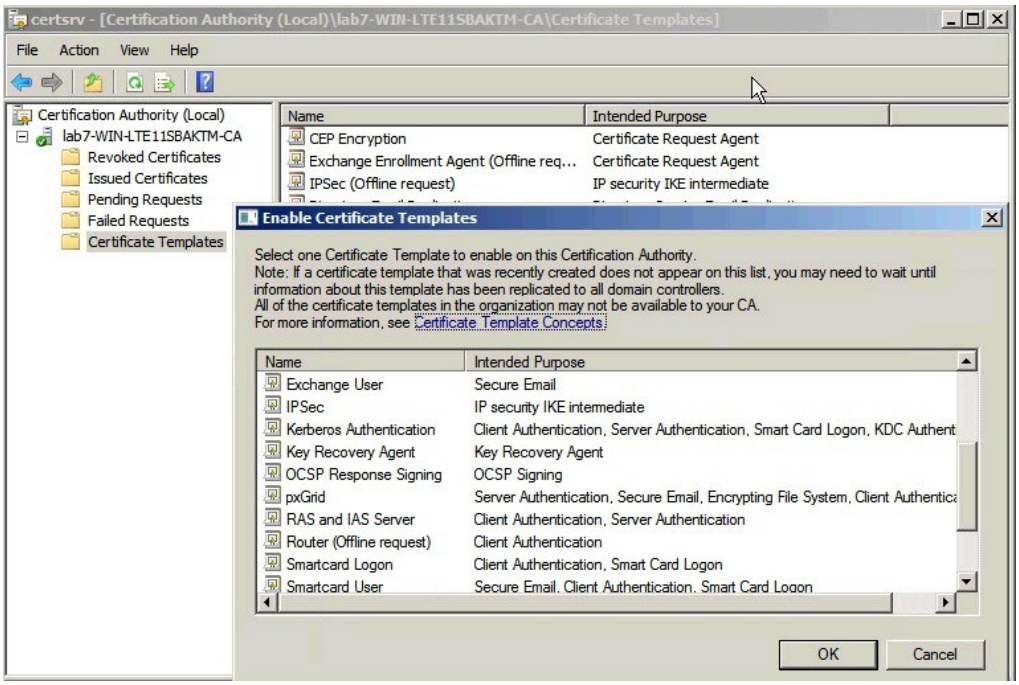
ステップ 6 [拡張（Extensions）] -> [発行ポリシー（Issuance Policies）] -> [編集（Edit）] -> [すべての発行ポリシー（All Issuance Policies）] の順にクリックします。



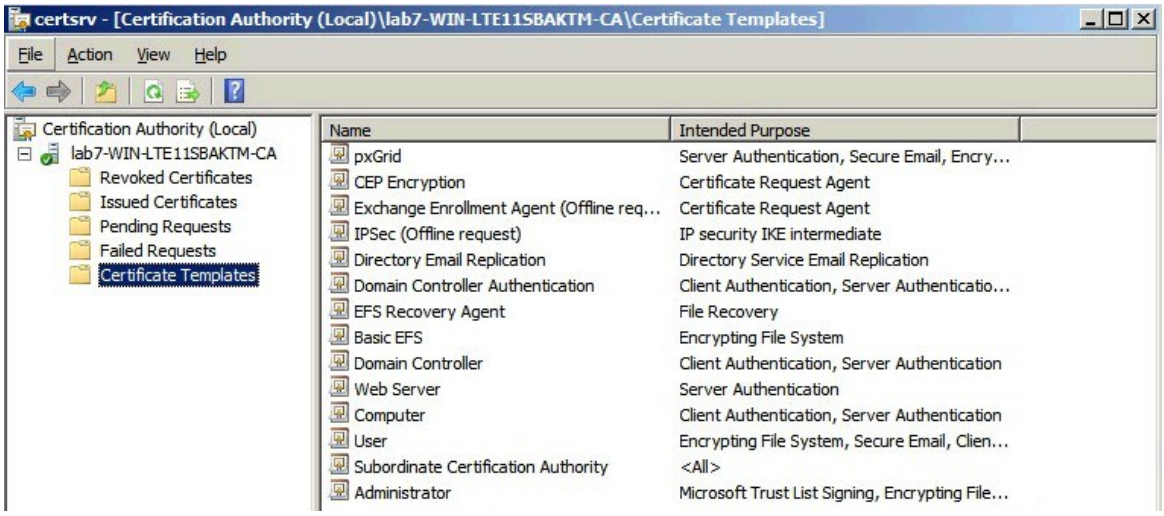
ステップ 7 [要求の処理（Request Handling）] はデフォルトのままにします。



ステップ 8 [証明書テンプレート（Certificate Templates）] を右クリックします。
ステップ 9 発行する [新規テンプレート（New Template）] を選択後、[pxGrid] を選択します。



ステップ 10 pxGrid のテンプレートが表示されます。



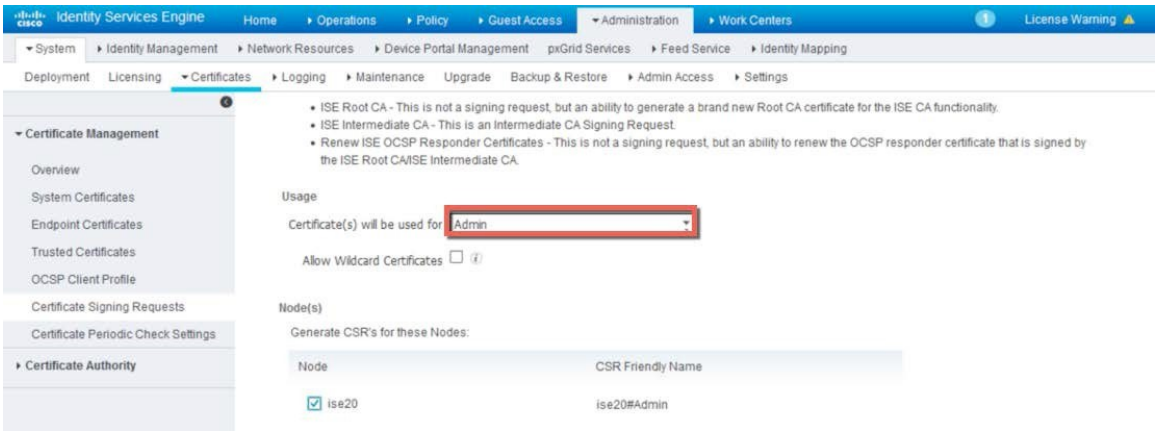
ISE 2.0 の設定

スタンドアロン構成の認証局（CA）署名環境用に ISE pxGrid ノードを設定します。最初に、「pxGrid」CSR 要求が ISE ノードから生成され、pxGrid のカスタマイズされたテンプレートを使用して、CA サーバによって署名されます。証明書は最初の ISE CSR 要求にバインドされます。

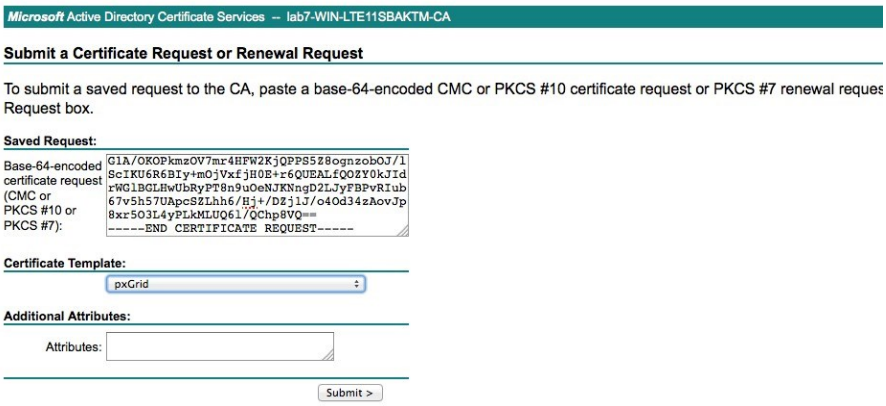
CA ルート証明書は ISE 証明書信頼ストアにインポートされます。ISE ID 識別証明書は ISE 証明書システム ストアにエクスポートされます。ISE ノードは pxGrid 操作用に有効化されます。

ステップ 1 ISE pxGrid ノードになる ISE ノードの CSR 要求を生成します。
[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [証明書署名要求（Certificate Signing Requests）] -> [生成（Generate）] を選択します。

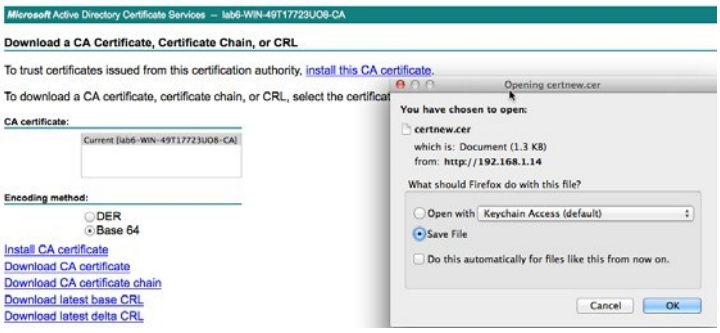
注：証明書の用途は管理用であることが必要です。これは、FMC 6.0 でのアクティブー括ダウンロード セッションで必須です。



ステップ 2 [証明書の要求（Request a certificate）] -> [証明書の要求の詳細設定（Advanced Certificate request）] に CSR 情報をコピーして貼り付け、カスタマイズした pxGrid テンプレートを選択して、[送信（Submit）] をクリックします。

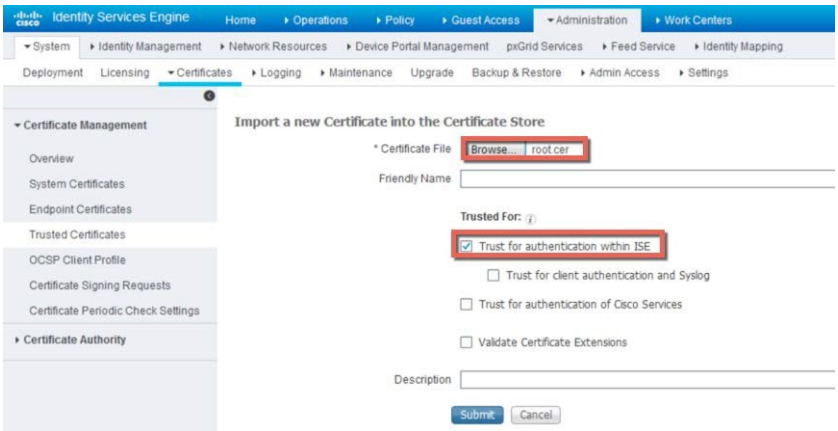


ステップ 3 Base 64 符号化形式の CA ルートをダウンロードします。

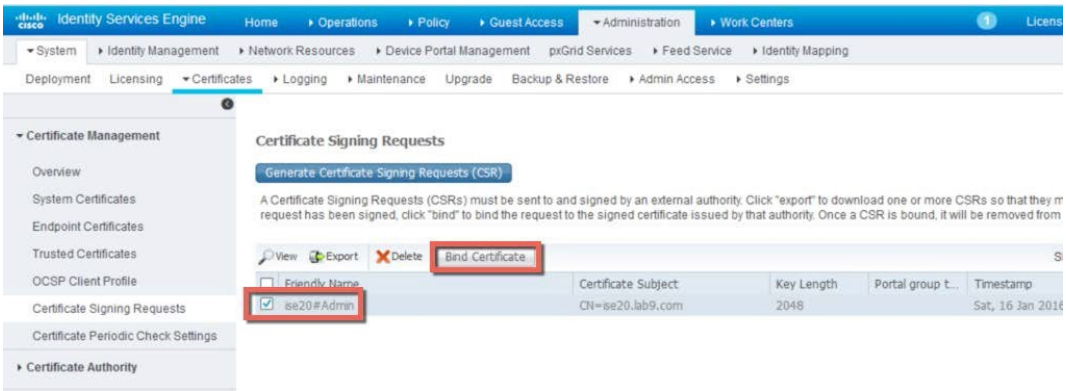


ステップ 4 CA ルートを ISE 証明書信頼システム ストアにアップロードします。
[管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [信頼できる証明書（Trusted Certificates）] を選択し、CA ルート証明書をアップロードします。

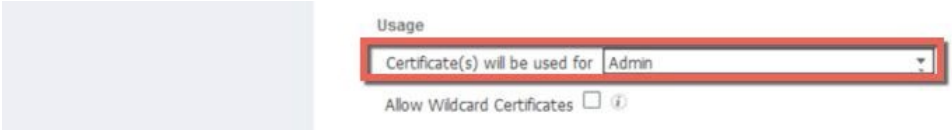
ステップ 5 [ISE 内認証の信頼（Trust for authentication within ISE）] を有効化し、[送信（Submit）] をクリックします。



ステップ 6 ISE pxGrid ノード証明書を ISE 証明書システム ストアにアップロードします。
[管理(Administration)] -> [システム(System)] -> [証明書署名の要求(Certificate Signing Requests)] を選択し、証明書を CSR 要求にバインドします。

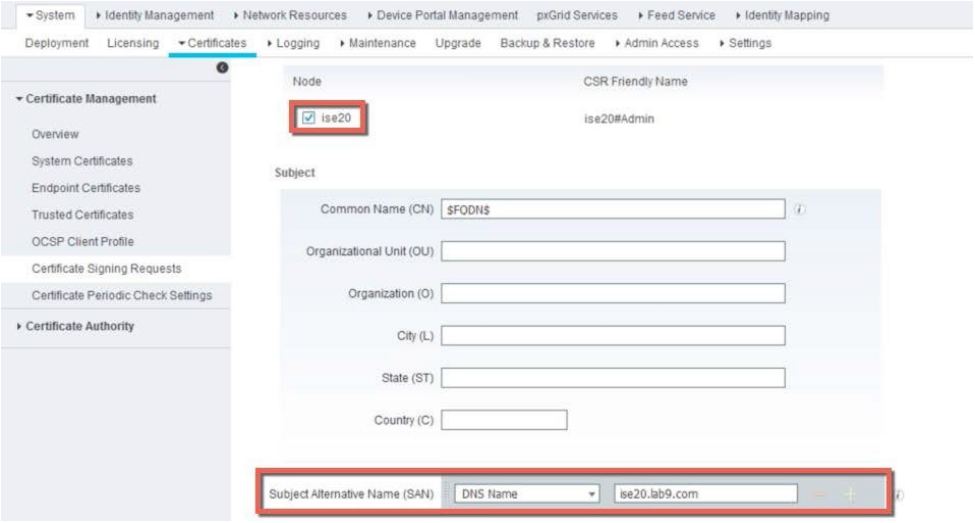


ステップ 7 [管理(Administration)] -> [システム(System)] -> [証明書(Certificates)] -> [証明書の管理(Certificate Management)] -> [証明書署名要求(Certificate Signing Request)] -> [証明書署名要求(CSR)の生成(Generate Certificate Signing Requests (CSR))] を選択し、証明書の用途として [管理(Admin)] を選択します。



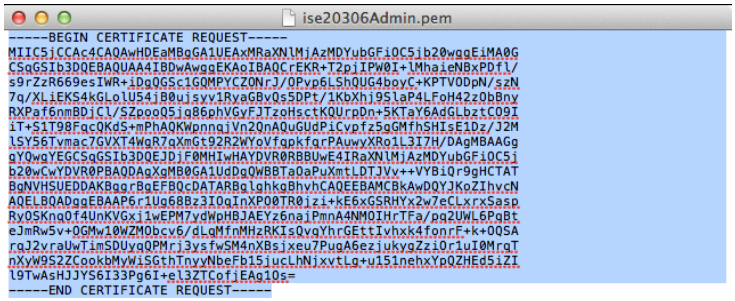
ステップ 8 [ノード(Node)] を選択します。

ステップ 9 [サブジェクトの別名(SAN)(Subject Alternative Name (SAN))] で [DNS 名(DNS name)] を選択し、DNS 名を追加します。

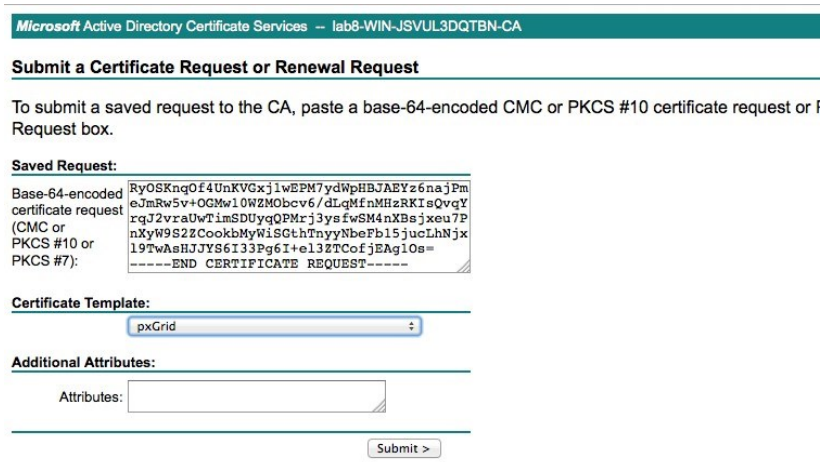


ステップ 10 [生成(Generate)] を選択します。
ステップ 11 [エクスポート(Export)] を選択します。

ステップ 12 pem ファイルを開き、csr 要求をコピーしてカスタマイズした pxGrid テンプレートに貼り付けます。

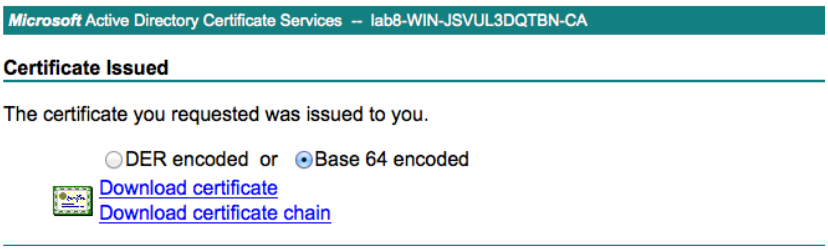


ステップ 13 [証明書の要求（Request a certificate）] -> [証明書要求の詳細設定（Advanced Certificate request）] に貼り付けた後、カスタマイズした pxGrid テンプレートを選択し、[送信（Submit）] をクリックします。

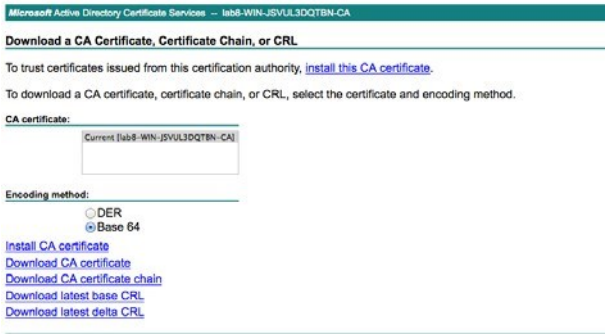


ステップ 14 [送信（Submit）] を選択します。

ステップ 15 Base 64 符号化形式の証明書をダウンロードします。

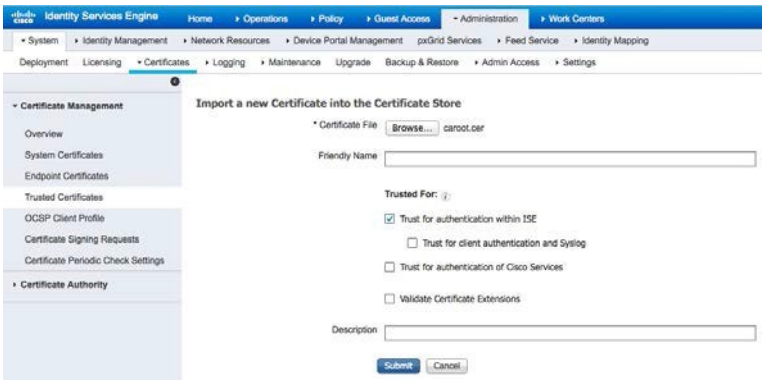


ステップ 16 Base 64 形式の CA ルート証明書をダウンロードします。



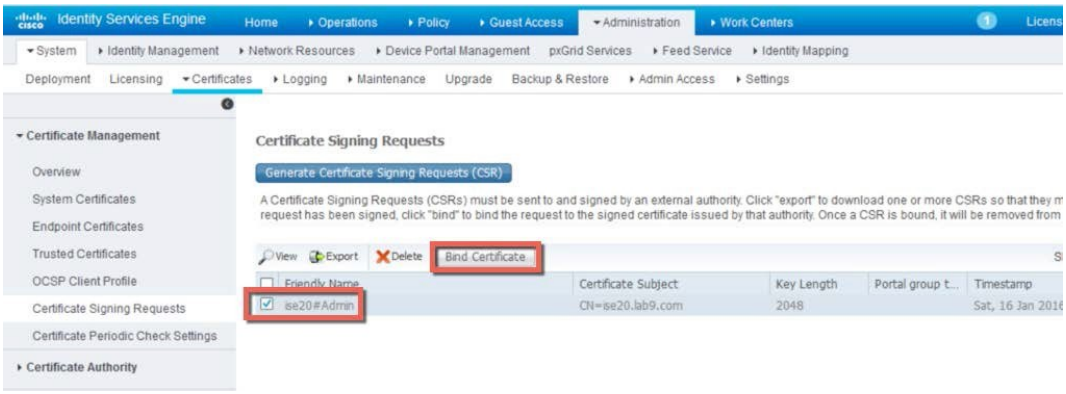
ステップ 17 [管理（Administration）] -> [システム（System）] -> [証明書（Certificate）] -> [証明書の管理（Certificate Management）] -> [信頼できる証明書（Trusted Certificates）] の順に選択し、ルート証明書をインポートします。

ステップ 18 [ISE 内認証の信頼（Trust for authentication within ISE）] を有効化します。

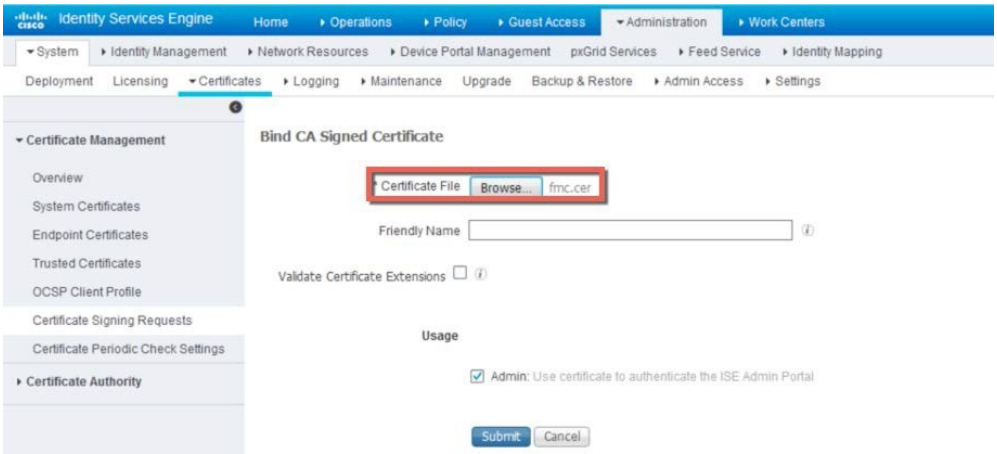


ステップ 19 [送信（Submit）] を選択します。

ステップ 20 [管理（Administration）] -> [証明書（Certificate）] -> [証明書の管理（Certificate Management）] -> [システム証明書（System Certificates）] -> [証明書署名要求（Certificate Signing Requests）] の順に選択し、CSR 要求を選択して、[証明書をバインド（Bind Certificate）] をクリックします。

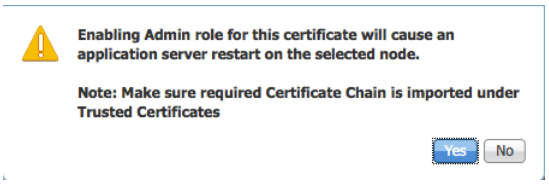


ステップ 21 ISE CA 署名付きアイデンティティ証明書をアップロードします。

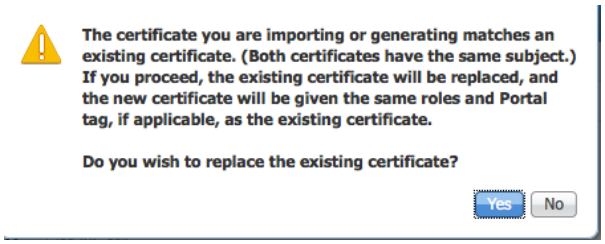


ステップ 22 [送信(Submit)] を選択します。

ステップ 23 次のメッセージが表示されたら、[はい(Yes)] を選択します。

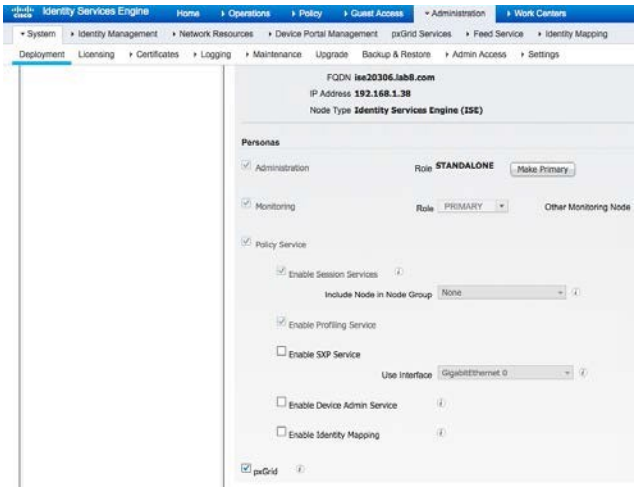


ステップ 24 次のメッセージが表示されたら、[はい(Yes)] を選択します。



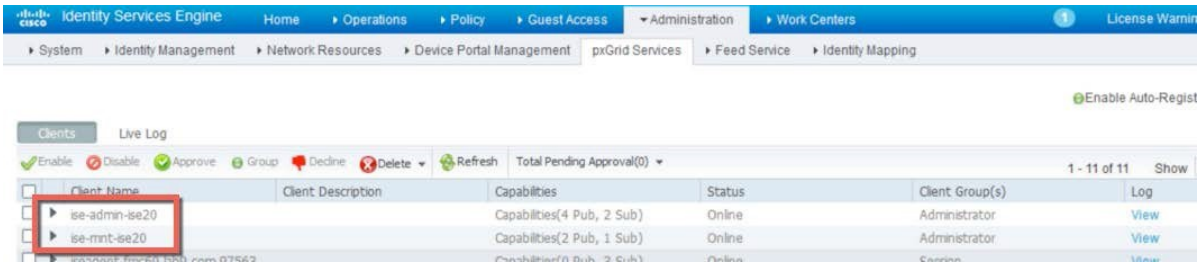
ステップ 25 システムが再起動され、GUI に戻ります。

ステップ 26 [管理(Administration)] -> [システム(System)] -> [導入(Deployment)] を選択し、ホスト名を編集した後、[pxGrid] をオンにします。



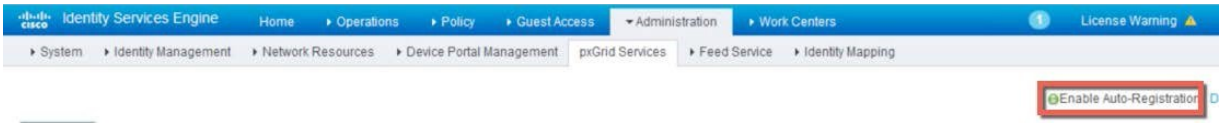
ステップ 27 [保存(Save)] を選択します。

ステップ 28 [管理(Administration)] -> [pxGrid サービス(pxGrid Services)] を選択し、公開されたサービスが表示されていることを確認します。



注:表示されるまでに数秒かかることがあります。ISE VM で「sh application status ise」を実行し、pxGrid サービスが初期化中であることを確認してください。

ステップ 29 [自動登録の有効化(Enable Auto Registration)] を有効にします。



ステップ 30 pxGrid に接続されていることを確認します。

SMC アイデンティティ証明書の作成および CA ルート証明書のダウンロード

ここでは、SMC 秘密キーおよび CA 局によって署名される証明書署名要求（CSR）を生成します。pxGrid 用の CA テンプレートには、pxGrid 操作に有効なクライアント認証とサーバ認証の両方の EKU が含まれている必要があります。

ステップ 1 SMC で秘密キーを作成します。

```
openssl genrsa -out smc.key 4096
Generating RSA private key, 4096 bit long modulus
.....................................................................................................
.....................................................................++
..........++
e is 65537 (0x10001)
```

ステップ 2 CA サーバによって署名される SMC CSR 要求を作成します。

```
openssl req -new -key smc.key -out smc.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

ステップ 3 SMC へのルート アクセスを取得し、SCP を使用して SMC.CSR および SMC.key ファイルをセキュアな PC にコピーします。この PC は、pxGrid カスタマイズ テンプレートの詳細ユーザ要求に SMC.CSR をコピーして貼り付けるために使用されます。

注：Win ラップトップを使用している場合は、SSH サービスをインストールする freeSSHd またはユーティリティをダウンロードして、これらのファイルを SMC から Win ラップトップにコピーするときに SCP コピーを使用できるようにしてください。

ステップ 4 Base 64 符号化形式の証明書をダウンロードします。

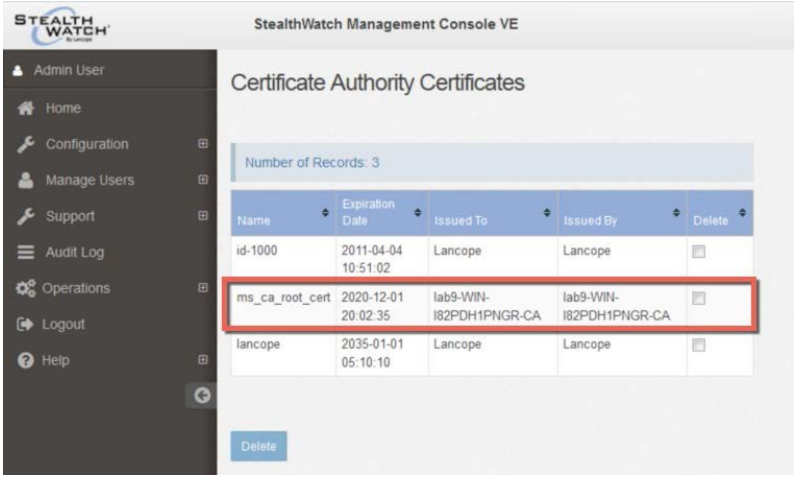
ステップ 5 この X509 証明書は Base 64 符号化形式でダウンロードされているため、ファイルの名前を .cer から .crt に変更します。この名前変更後の .crt ファイルは、SSL クライアント アイデンティティ証明書をアップロードするために使用されます。この証明書は、pxGrid クライアント認証に使用されます。これは、StealthWatch 6.7.1 の新機能です。

ステップ 6 CA ルート証明書をダウンロードします。

SMC 信頼ストアへの CA ルート証明書のアップロード

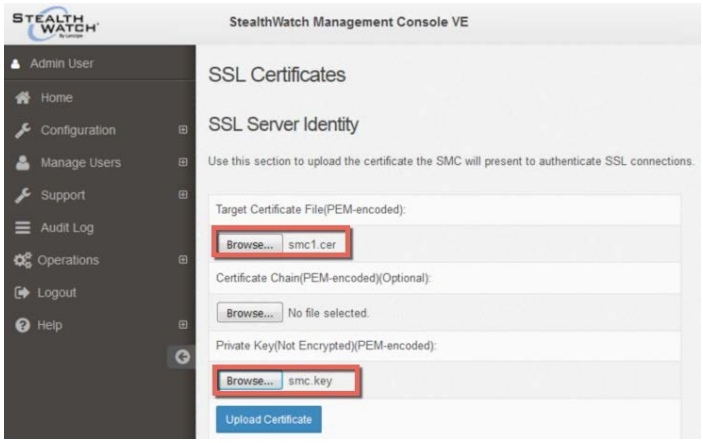
ステップ 1 [管理者ユーザ（Admin User）] -> [アプライアンスの管理（Administer Appliance）] -> [設定（Configuration）] -> [認証局証明書（Certificate Authority Certificates）] -> [参照（Browse）] を選択し、root.cert ファイルをアップロードします。

ステップ 2 **説明を入力します。**アンダースコアを使用し、スペースは使用しないでください。証明書を追加すると以下のように表示されます。



SSL サーバ ID への SMC アイデンティティ証明書のアップロード

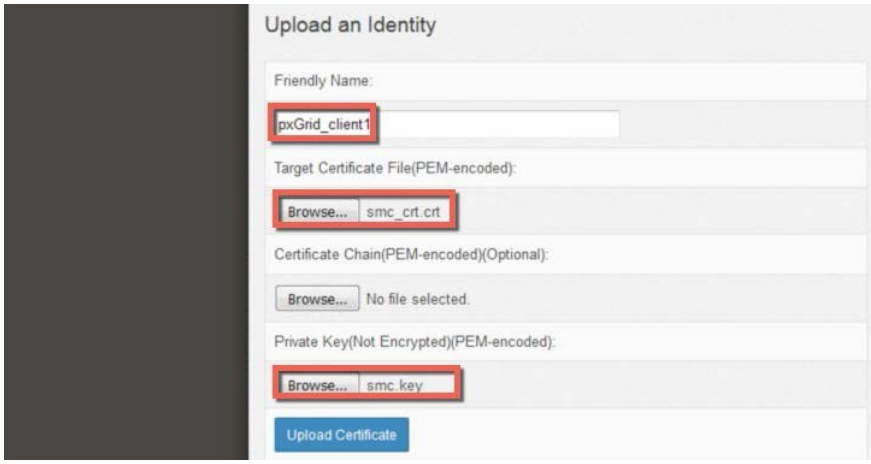
ステップ 3 [管理者ユーザ（Admin User）] -> [アプライアンスの管理（Administer Appliance）] -> [設定（Configuration）] -> [SSL 証明書（SSL Certificate）] -> [SSL サーバ ID（SSL Server Identity）] を選択し、SMC 公開証明書と秘密キーのペアをアップロードします。



ステップ 4 [証明書のアップロード（Upload Certificate）] をクリックします。

SSL クライアント ID への SMC アイデンティティ証明書のアップロード

ステップ 1 [管理者ユーザ（Admin User）] -> [アプライアンスの管理（Administer Appliance）] -> [設定（Configuration）] -> [SSL 証明書（SSL Certificate）] -> [SSL クライアント ID（SSL Client Identities）] を選択し、SMC 公開証明書 .crt ファイルと秘密キーのペアをアップロードします。



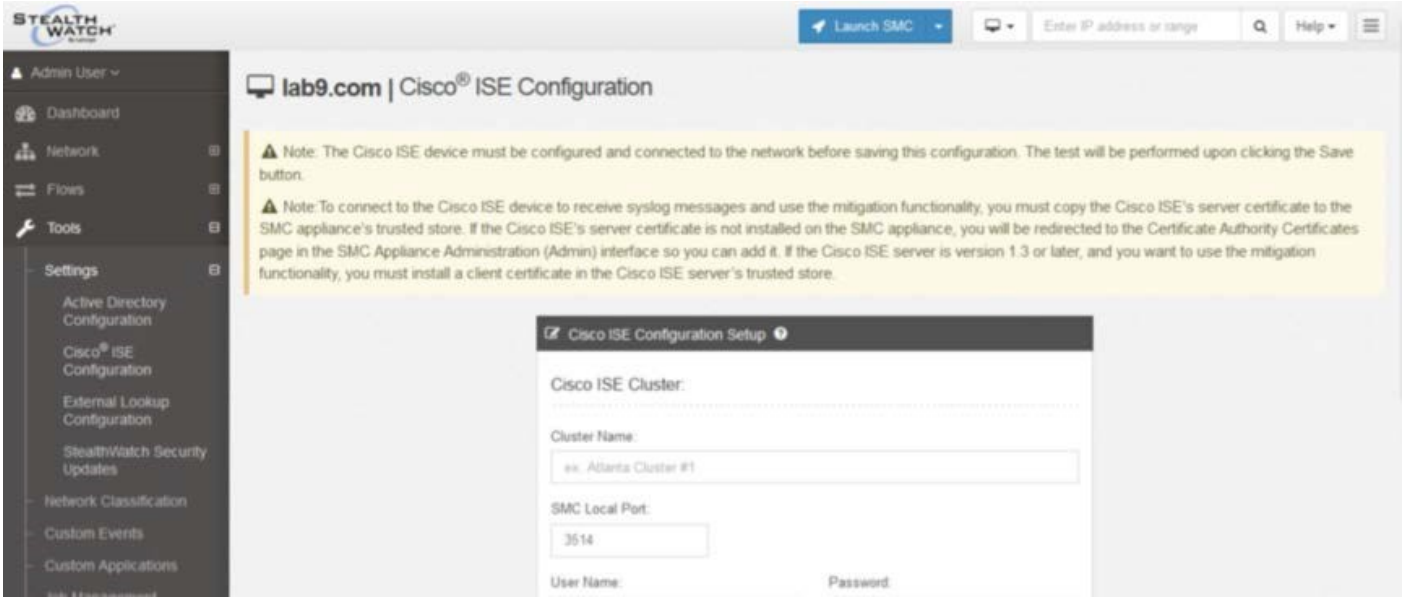
ステップ 2 [フレンドリ名（Friendly Name）] を入力します。アンダースコアを使用し、スペースは使用しないでください。

ステップ 3 [証明書のアップロード（Upload Certificate）] をクリックします。

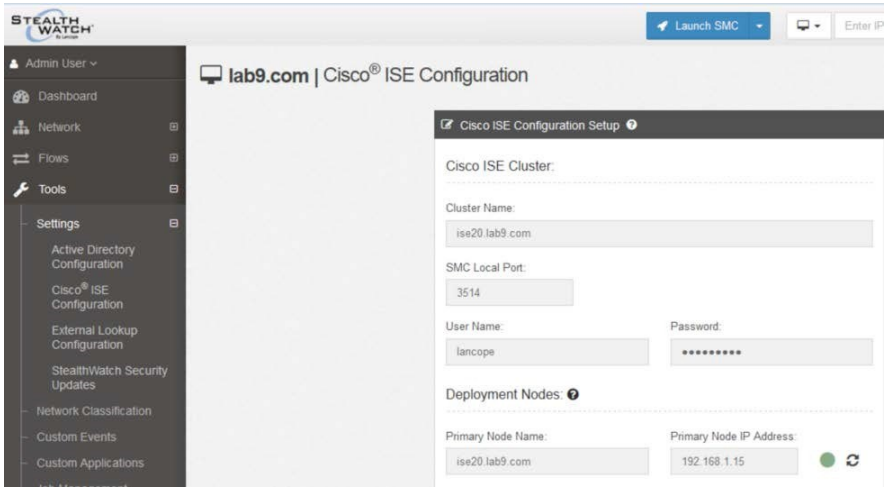
ISE からの Syslog イベントの受信

ステップ 1 SMC にログインし、[ツール（Tools）] -> [設定（Settings）] -> [Cisco ISE の設定（Cisco ISE Configuration）] を選択します。次のような設定が表示されます。以下のメッセージが表示されたら、CA ルート証明書が SMC CA ストアにアップロード済みであることを確認してください。

注：ここでは、成功した認証、RADIUS アカウンティング、プロファイラ、操作、管理などの監査 syslog メッセージが UDP 3514 で SMC に送信されるように、ISE がすでに設定済みであることを前提としています。

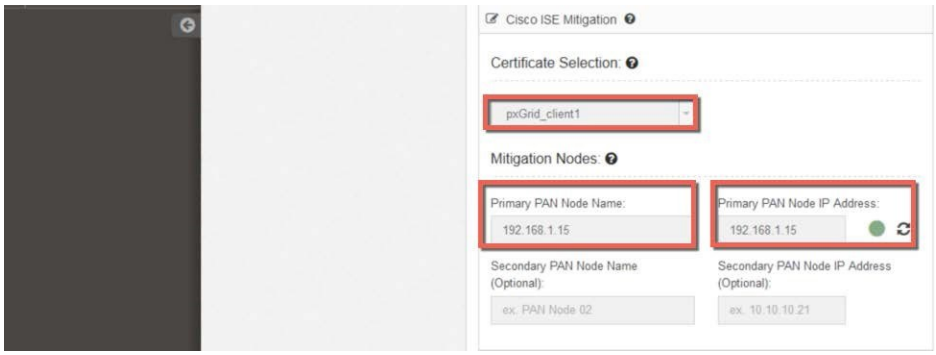


ステップ 2 CA ルート証明書を SMC にアップロードします。
ステップ 3 [ツール（Tools）] -> [設定（Settings）] を選択し、ISE MnT ノード情報を入力します。以下のように表示されます。

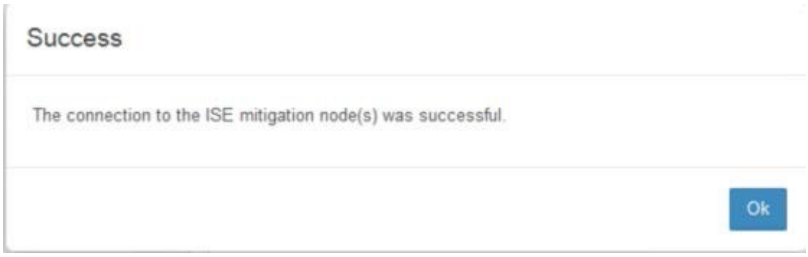


ステップ 4 Cisco ISE ミティゲーションを追加し、pxGrid_client1 または以前作成したフレンドリ名を選択します。

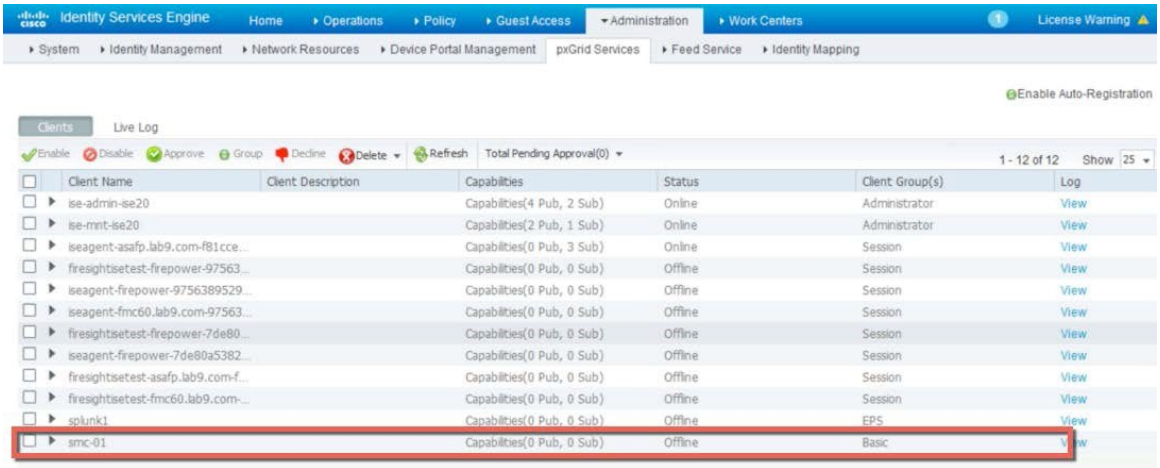
注：[プライマリ PAN ノード名（Primary PAN Node Name）] はプライマリ ISE pxGrid ノードのことです。



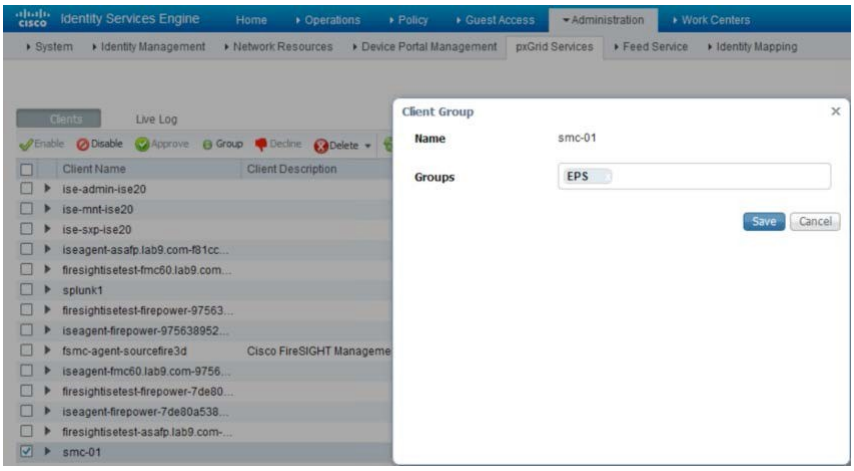
ステップ 5 [保存（Save）] をクリックします。
ステップ 6 以下のように表示されます。



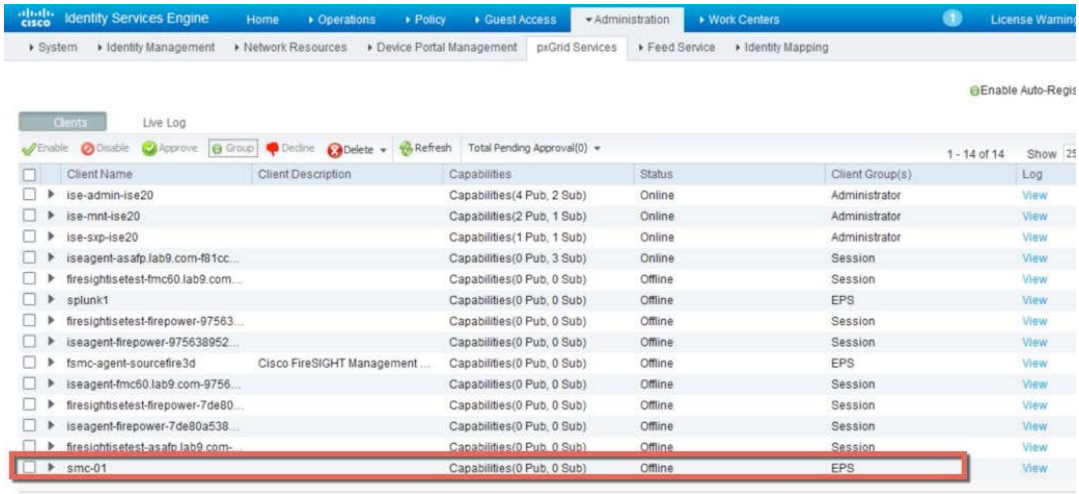
ステップ 7 [OK] をクリックします。
ステップ 8 SMC が pxGrid クライアントとして登録されます。



ステップ 9 登録済みの Lancope smc-01 クライアントを EPS クライアント グループに移動します。
[smc-01] -> [グループ（Group）] を選択して [Basic] を削除した後、[EPS] -> [保存（Save）] を選択します。



ステップ 10 smc-01 クライアントが EPS グループに移動されます。



SMC クライアント - ホスト Java ストアで CA 証明書を信頼するための設定

注：CA がそのルートとして標準の公開 CA を持たない場合、Java クライアントを開くには、ホスト Java ストアが CA ルート証明書を信頼するように設定する必要があります。

ステップ 1 SMC Java クライアントを開き、Java コンソールを有効化します。
ステップ 2 Java コンソールで、TrustStoreHelper のパスを特定します。

```
6 INFO  [SimpleSMCClient] https://172.25.73.134/smc-client/app
8 INFO  [XMLBindings] jar:https://172.25.73.134/smc-client/app/lc-core.jar!/xml/bindings.xml
5 INFO  [XMLBindings] jar:https://172.25.73.134/smc-client/app/sw-manager-client.jar!/com/lancope/sws/smcClient/bindings.xml
7 INFO  [TrustStoreHelper] System CA trust store not found, or could not be opened with given password at:/Library/Internet Plug-Ins/JavaAppletPlugin.
3 INFO  [TrustStoreHelper] System CA trust store loaded from:/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security/cacerts
6 INFO  [JRMProxyInvocationHandler] /smc/public/openlrmService/getBannerMessage
1 WARN  [LaunchWorkItem] Attempted login with session id failed: prompting for username and password
```

ステップ 3 ホスト上で、前のステップで特定した cacerts ファイルに CA ルート証明書をインポートします。ほとんどの cacerts ファイルのデフォルト パスワードは「changeit」です。

```
keytool -keystore cacerts -importcert -alias myca -file myfile
```

```
where: myfile represents the CA root certificate (i.e. root.cer)
```

ステップ 4 SMC Java クライアントを起動します。

SMC クライアントの例

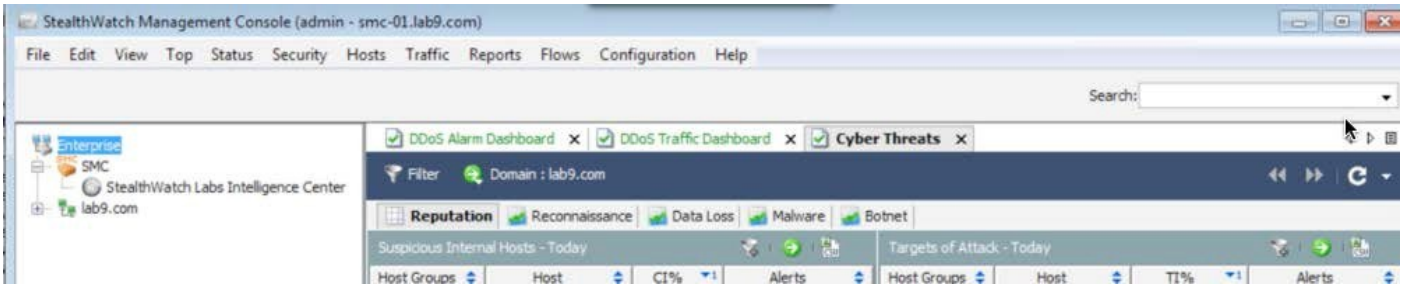
SMC Java クライアントを正常に起動するには、CA ルート証明書を cacerts ファイルにインポートし、使用する PC に Java 開発キット（JDK）をインストールします。

ステップ 1 Oracle Java 開発キットをダウンロードしてインストールします。
ステップ 2 JDK をパスに含めます。
ステップ 3 Java コンソールを有効化して表示します。
[すべてのプログラム（All Programs）] -> [Java] -> [Java の設定（Configure Java）] -> [詳細（Advanced）] -> [Java コンソール（Java Console）] -> [コンソールを表示する（Show Console）] -> [適用（Apply）] -> [OK] の順に選択します。
ステップ 4 以下のように入力して、caroot.cer（CA root.cert）を cacerts ファイルにインポートします。

```
C:\Program Files\Java\jre1.8.0_66\lib\security>path=c:\program files\java\jdk1.8
.0_66\bin

C:\Program Files\Java\jre1.8.0_66\lib\security>keytool.exe -keystore cacerts -im
portcert -alias myca -file caroot.cer
Enter keystore password:changeit
Owner: CN=lab9-WIN-I82PDH1PNGR-CA, DC=lab9, DC=com
Issuer: CN=lab9-WIN-I82PDH1PNGR-CA, DC=lab9, DC=com
Serial number: 913b274e6a35ea34efcdf6dadfe4f0e
Valid from: Tue Dec 01 19:52:35 GMT-05:00 2015 until: Tue Dec 01 20:02:35 GMT-05
:00 2020
Certificate fingerprints:
         MD5: FD:26:D1:E0:FA:C5:31:79:DC:5A:1E:BA:DD:91:03:D7
         SHA1: 22:2A:22:11:3A:00:50:67:AD:83:85:80:A9:41:25:4A:DE:C0:91:2A
         SHA256: 98:8E:A1:63:AB:C6:22:2B:50:A7:4A:25:77:03:84:E9:9E:95:B7:E8:45:
86:5F:58:77:04:42:D2:A3:82:BB:71
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00                                           ...
```

```
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: AB D9 CE DB CD 58 19 4A   42 A6 BF 68 7A 96 FF 91  .....X.JB..hz...
0010: 1F 73 BC 67                                        .s.g
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore

C:\Program Files\Java\jre1.8.0_66\lib\security>
```

ステップ 5 [SMC クライアントの起動（Launch SMC client）] をクリックします。
次が表示されます。



ステップ 6 コンソールに次のように表示されます。

```
Java Web Start 11.66.2.17
Using JRE version 1.8.0_66-b17 Java HotSpot(TM) 64-Bit Server VM
User home directory = C:\Users\jsmith
----------------------------------------------------
c:   clear console window
f:   finalize objects on finalization queue
g:   garbage collect
h:   display this help message
m:   print memory usage
o:   trigger logging
p:   reload proxy configuration
q:   hide console
r:   reload policy configuration
s:   dump system and deployment properties
t:   dump thread list
v:   dump thread stack
0-5: set trace level to <n>
----------------------------------------------------
Missing Application-Name manifest attribute for: https://smc-01.lab9.com/smc-client/app/guava.jar
StealthWatch detected JRE version 1.8.0_66
```

```
2016-01-31 00:34:39,306 INFO [LogManager] resource=jar:https://smc-01.lab9.com/smc-client/app/sw-manager-
client.jar!/com/lancope/sws/smcClient/log4j.xml
2016-01-31 00:34:39,306       [LogManager] level=default
INFO                          [SimpleSMCClient] https://smc-01.lab9.com/smc-client/app
2016-01-31 00:34:39,306       [XMLBindings] jar:https://smc-01.lab9.com/smc-client/app/lc-
INFO
2016-01-31 00:34:39,311       [XMLBindings] jar:https://smc-01.lab9.com/smc-client/app/sw-manager-
client.jar!/com/lancope/sws/smcClient/bindings.xml
2016-01-31 00:34:40,230 INFO [TrustStoreHelper] System CA trust store not found, or could not be opened with
given password at:C:\Program Files\Java\jre1.8.0_66\lib\security\jssecacerts
2016-01-31 00:34:40,240 INFO [TrustStoreHelper] System CA trust store loaded from:C:\Program
Files\Java\jre1.8.0_66\lib\security\cacerts
Jan 31, 2016 12:34:40 AM java.util.prefs.WindowsPreferences <init>
WARNING: Could not open/create prefs root node Software\JavaSoft\Prefs at root 0x80000002.Windows
RegCreateKeyEx(...) returned error code 5.
2016-01-31 00:34:40,343 INFO [JRMProxyInvocationHandler] /smc/public/openJrmService/getBannerMessage
2016-01-31 00:34:41,195 INFO [JRMProxyInvocationHandler] /smc/jrmService/userService/getUserProfile
2016-01-31 00:34:41,352 INFO [JRMProxyInvocationHandler] /smc/jrmService/objectService/get
2016-01-31 00:34:41,459 INFO [SMCClientObjectModel] added LObjectKey:{Domain:{143}}
2016-01-31 00:34:41,460 INFO [SMCClientObjectModel] added LObjectKey:{SMC:{0}}
2016-01-31 00:34:41,460 INFO [SMCClientObjectModel] added LObjectKey:{Domain:{143},CiscoISE:{162}}
.
.
.
```

SMC および ISE pxGrid ノードでの自己署名証明書の使用

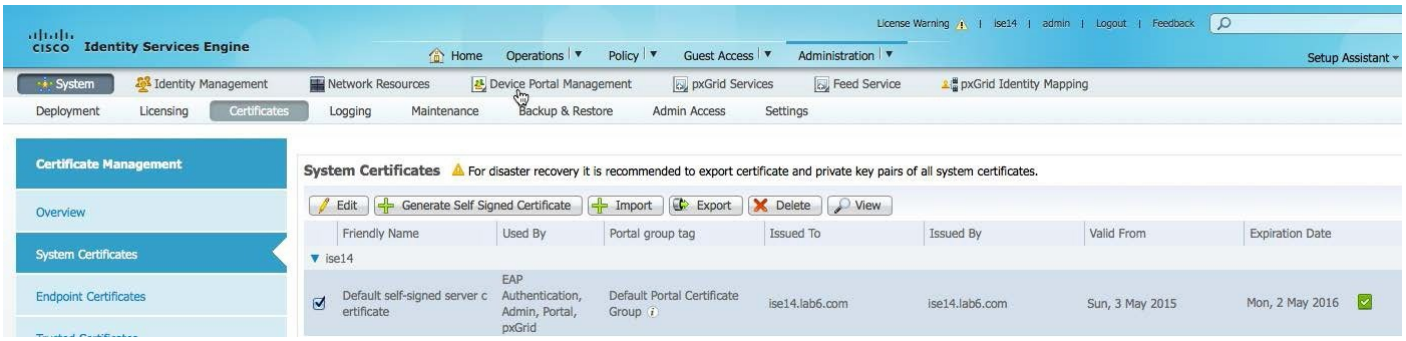
この項では、StealthWatch SMC および ISE pxGrid ノードでの自己署名証明書を使用について説明します。自己署名証明書は、主に PoC（コンセプト実証）のテストに使用されます。ISE pxGrid ノードは、スタンドアロン環境に導入されます。ISE の実稼働導入では、pxGrid は専用ノードになる点に注意してください。

自己署名証明書用の ISE 1.3/1.4 の設定

ISE アイデンティティ証明書は信頼される必要があり、公開証明書は ISE 信頼システム証明書ストアにエクスポートされる必要があります。これは、ISE 2.0 では不要です。

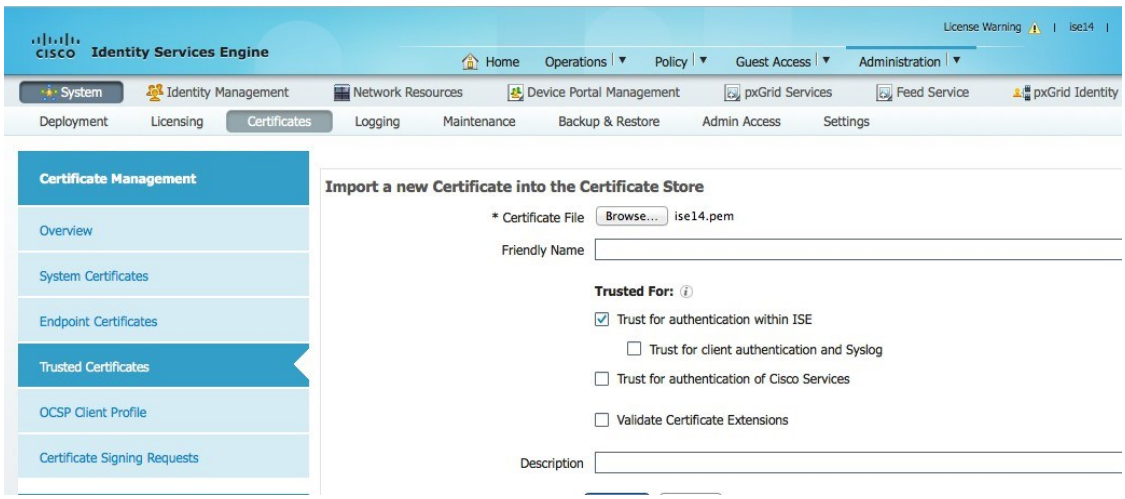
注：ISE 1.4 ではこのステップの実行が不要な場合があります。ISE アイデンティティ証明書がすでに信頼されていることがあります。

ステップ 1 [管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [システム証明書（System Certificates）] を選択し、ISE アイデンティティ証明書を選択してエクスポートします。



注：公開証明書のみをエクスポートします。デフォルトの証明書名は変更できます。この例では、証明書名が ise14.pem に変更されています。

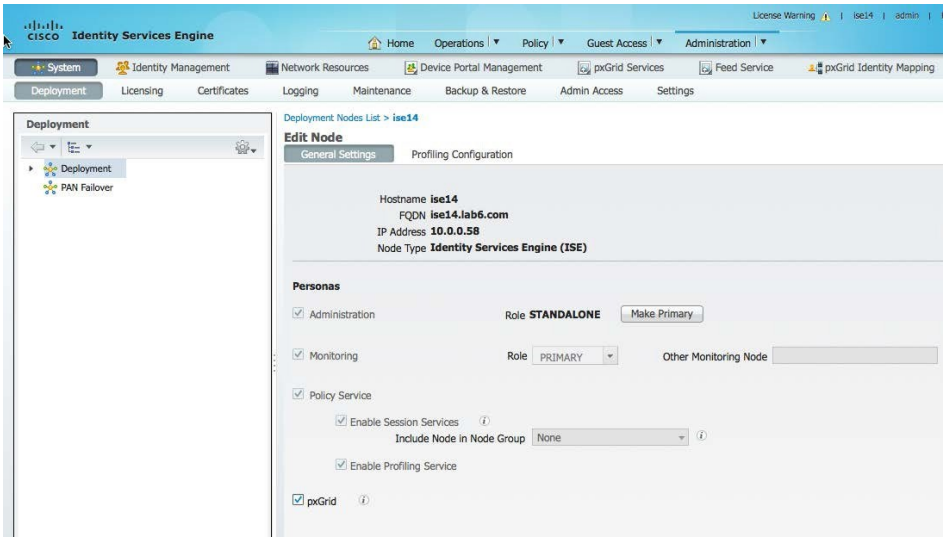
ステップ 2 [管理（Administration）] -> [システム（System）] -> [証明書（Certificates）] -> [信頼できる証明書（Trusted Certificates）] -> [インポート（Import）] -> [証明書ファイル（certificate file）] を選択し、[ISE 内認証の信頼（Trust for authentication within ISE）] をオンにして、[送信（Submit）] を選択します。



pxGrid の有効化

pxGrid およびペルソナを有効化します。pxGrid サービスは ISE 内で開始する必要があります。

ステップ 1 [管理(Administration)] -> [システム(System)] -> [導入(Deployment)] を選択し、[ペルソナ(Personas)] の [pxGrid] をオンにして、[保存(Save)] を選択します。



ステップ 2 pxGrid サービスが有効化されていることを確認します。[管理(Administration)] -> [pxGrid サービス(pxGrid Services)] を選択します。

注:これには 1 分ほど時間がかかることがあります。ISE pxGrid ノードで「application status ise」を実行して、pxGrid サービスが初期化中であることを確認してください。サービスが開始されない場合は、ISE アイデンティティ証明書を ISE 信頼システム証明書ストアにエクスポートしてください。

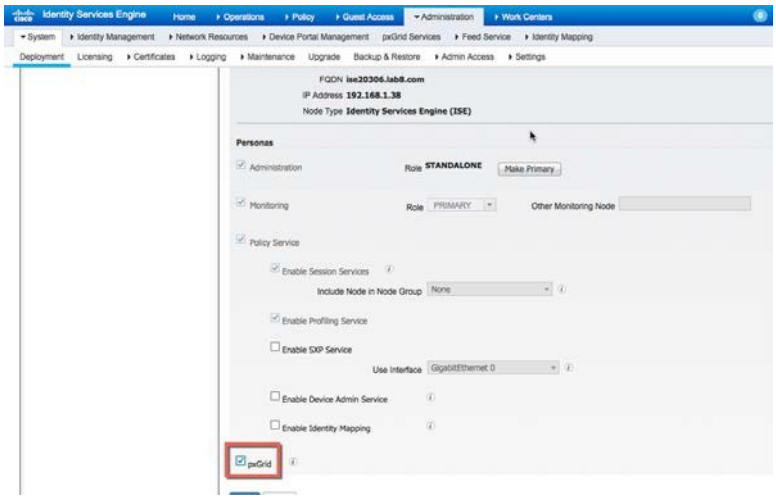
ステップ 3 [自動登録の有効化(Enable Auto Registration)] を有効にします。

注:「自動登録」が有効化されていない場合は、pxGrid クライアント要求が保留中の状態で表示されます。

自己署名証明書用の ISE 2.0 の設定

注：ISE 自己署名アイデンティティ証明書を、ISE 1.3 および ISE 1.4 のように ISE 証明書信頼ストアにエクスポートする必要がなくなりました。

ステップ 1 [管理（Administration）] -> [システム（System）] -> [導入（Deployment）] を選択し、ノードを選択後、[編集（Edit）] 画面で [pxGrid] をオンにします。

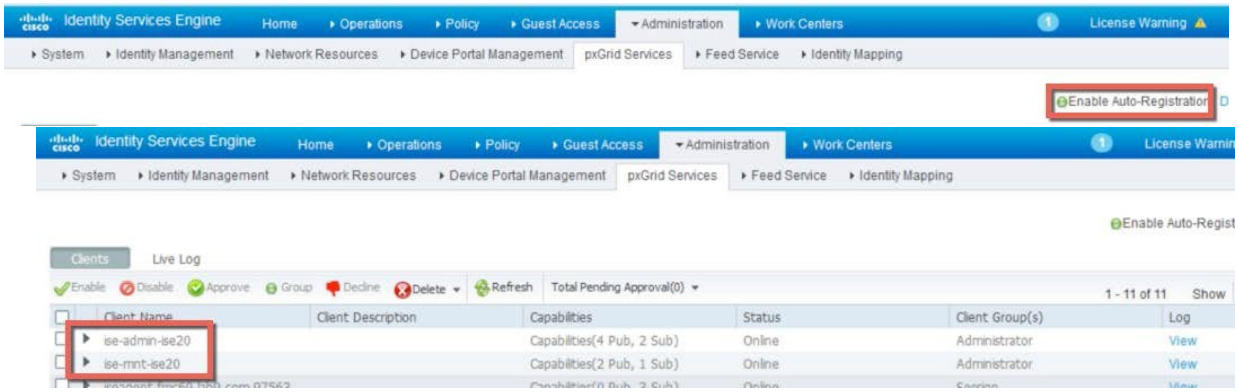


ステップ 2 [保存（Save）] を選択します。

ステップ 3 公開されたノードが [pxGrid サービス（pxGrid Services）] に表示され、接続されていることを確認します。[管理（Administration）] -> [pxGrid サービス（pxGrid Services）] を選択します。

注：公開されたノードが表示されるまでに時間がかかることがあります。ISE VM ノードで **sh application status ise** を実行することにより、pxGrid サービスが開始済みであることを確認してください。

ステップ 4 [自動登録の有効化（Enable Auto Registration）] を有効にします。

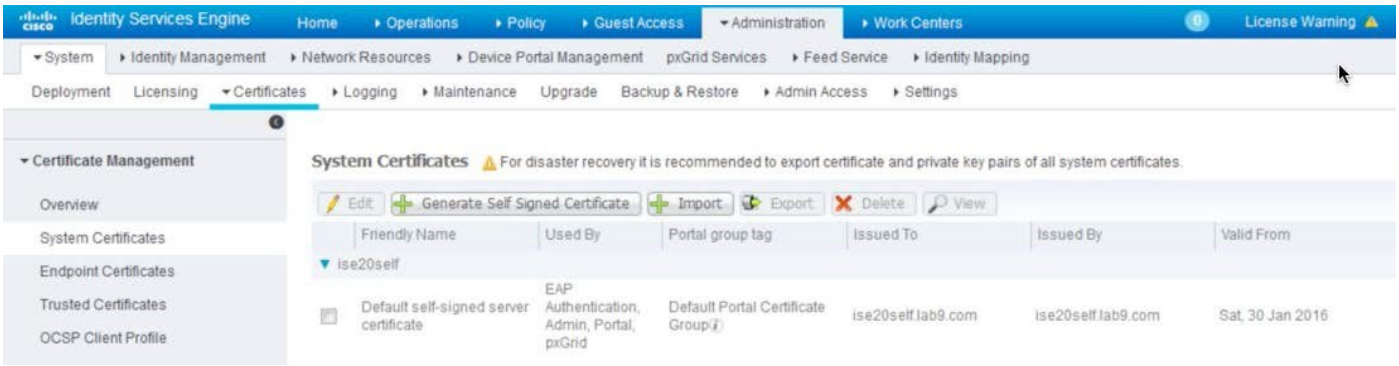


ステップ 5 [pxGrid に接続（connected to pxGrid）] と表示されていることを確認します。

SMC への ISE アイデンティティ証明書のエクスポート

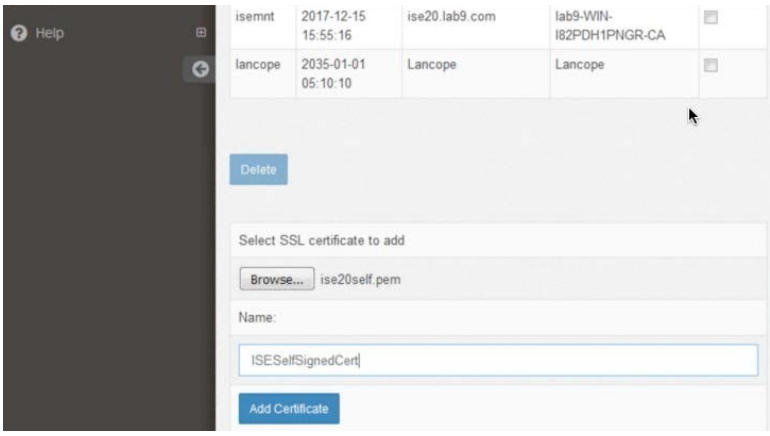
ステップ 1 ISE アイデンティティ証明書を SMC 認証局ストアにインポートします。

ステップ 2 [管理（Administration）] > [システム（System）] > [証明書（Certificate）] > [システム証明書（System Certificates）] の順に選択します。
次が表示されます。



ステップ 3 [Default self-signed server certificate] を選択し、**公開証明書のみをエクスポートします**。PEM ファイル名をわかりやすい名前に変更することもできます。

ステップ 4 SMC を開き、[管理者ユーザ（Admin User）] -> [アプライアンスの管理（Administer Appliance）] -> [設定（Configuration）] -> [認証局証明書（Certificate Authority Certificates）] -> [参照（Browse）] を選択し、ステップ 3 の ISE アイデンティティ証明書をアップロードします。



ステップ 5 証明書に名前を付けます。この例では、ISESelfSignedCert という名前です。値を追加する必要があります。アンダースコアは使用できますが、スペースは使用できません。

ステップ 6 [証明書を追加（Add Certificate）] を選択します。証明書が正常に追加されると、確認メッセージが表示されます。

SMC 用の自己署名証明書の作成

ここでは、pxGrid クライアントとしての SMC 用の自己署名証明書を作成します。SMC でのルート アクセスが必要です。

注:これらのステップは、SMC の自己署名証明書のヘルプに記載されています。

ステップ 1 SMC の秘密キーを生成します。後の手順で使用するパスフレーズの入力も求められます。

```
openssl genrsa -des3 -out selfsmc.key 2048
```

次が表示されます。

```
Generating RSA private key, 2048 bit long modulus
.....................................................................................................
...............................................+++
.+++
e is 65537 (0x10001)
Enter pass phrase for smc1.key:
Verifying - Enter pass phrase for smc1.key:
smc:~#
```

ステップ 2 自己署名証明書要求(CSR)を生成します。

```
openssl req -new -key selfsmc.key -out selfsmc.csr
```

注:[チャレンジ パスワード[](challenge password [])] と [会社名[](company name [])] を除き、すべてのフィールドが必須です。

次が表示されます。

```
Enter pass phrase for selfsmc.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Maryland
Locality Name (eg, city) []:Germantown
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lancope
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:smc.lab6.com
Email Address []:jdoe@lancope.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
smc:~#
```

ステップ 3 自己署名証明書を生成します。

```
openssl x509 -req -days 365 -in selfsmc.csr -signkey selfsmc.key -out selfsmc.crt
```

次が表示されます。

```
Signature ok
subject=/C=US/ST=Maryland/L=Germantown/O=Lancope/OU=Engineering/CN=smc.lab6.com/emailAddress=jdoe@lancope.com
Getting Private key
Enter pass phrase for selfsmc.key:
smc:~#
```

ステップ 4 先に入力したパスフレーズを復号します。

```
cp selfsmc.key selfsmc.key.org
openssl rsa -in selfsmc.key.org -out selfsmc.key
```

次が表示されます。

```
Enter pass phrase for selfsmc.key.org:
writing RSA key
smc:~#
```

ステップ 5 /root/smc ディレクトリに以下があることを確認します。

```
smc:~# ls
selfsmc.crt selfsmc.csr selfsmc.key selfsmc.key.org
smc:~#
```

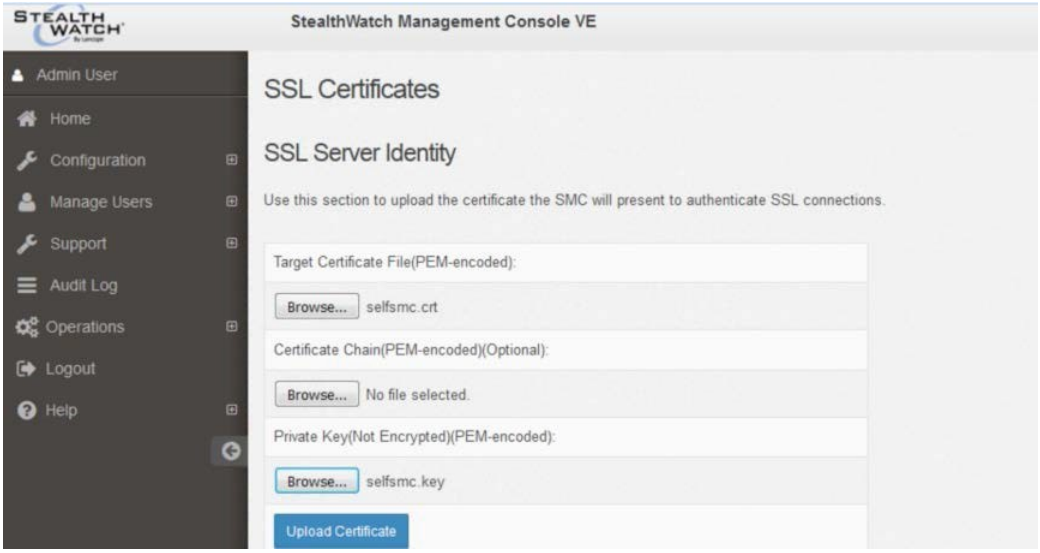
selfsmc.cert および selfsmc.key は、SMC の SSL 証明書の下に Admin User としてアップロードされます。

ステップ 6 SCP を使用して、selfsmc.crt ファイルおよび selfsmc.key ファイルをローカルにコピーします。ローカル PC へのコピー中に接続が拒否される場合は、「付録」の「MAC での SSH の有効化」を参照してください。

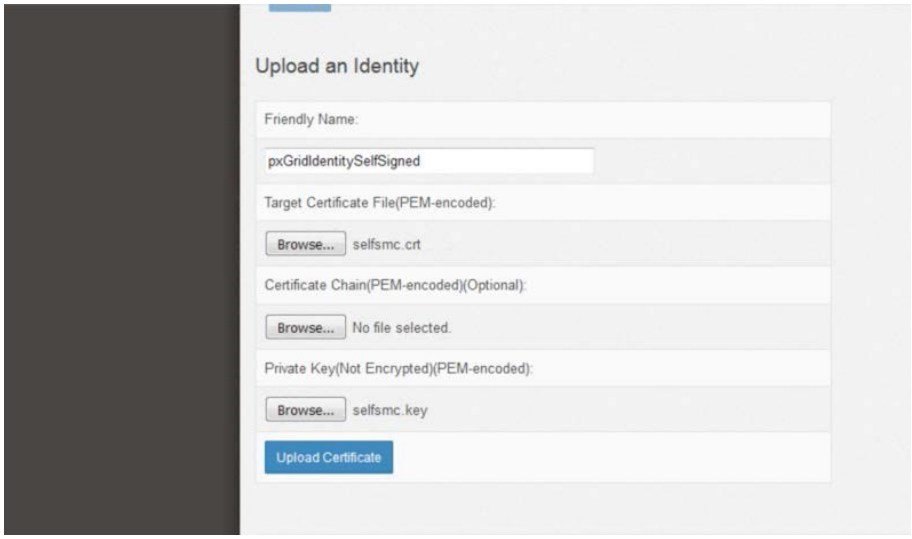
SMC への自己署名証明書のアップロード

ここでは、自己署名証明書の公開証明書と秘密キーのペアを SMC にアップロードします。

ステップ 1 [管理者ユーザ（Admin User）] -> [設定（Configuration）] -> [SSL 証明書（SSL Certificate）] -> [SSL サーバ ID（SSL Server Identity）] を選択し、selfsmc.crt および selfsmc.key を指定して [証明書のアップロード（Upload Certificate）] を選択します。



ステップ 2 [証明書のアップロード（Upload Certificate）] を選択します。
ステップ 3 証明書が正常にアップロードされ、再起動が必要であることを示すメッセージが表示されます。
ステップ 4 SMC サービスが開始されたら、再度ログインしてクライアント アイデンティティ証明書を追加します
ステップ 5 [管理者ユーザ（Admin User）] -> [設定（Configuration）] -> [SSL 証明書（SSL Certificate）] -> [SSL クライアント ID（SSL Client Identities）] を選択し、selfsmc.crt および selfsmc.key を指定して [証明書のアップロード（Upload Certificate）] を選択します。

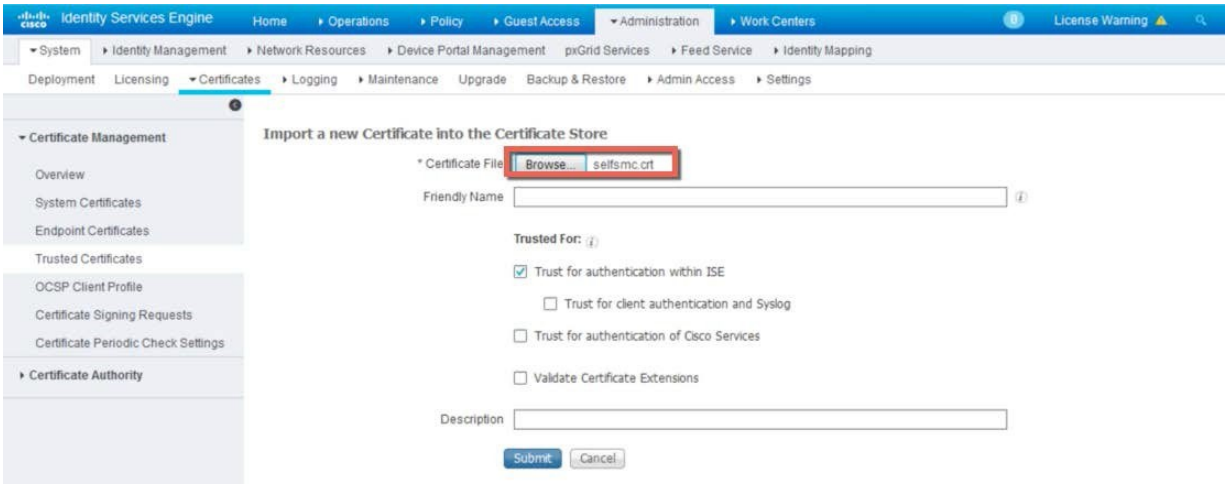


ステップ 6 フレンドリ名を追加し、[証明書のアップロード（Upload Certificate）] を選択します。
ステップ 7 アップロードした証明書が SSL クライアント ID の下に表示されます。

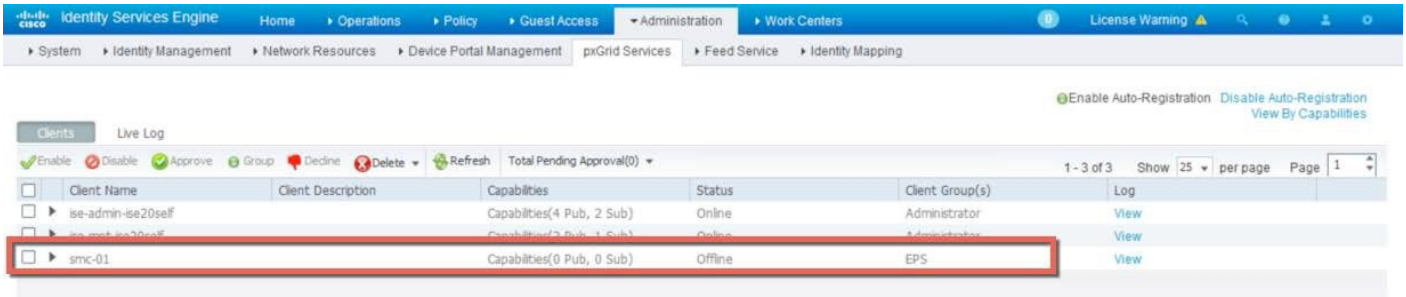
ISE 信頼システム証明書ストアへの SMC 自己署名証明書のアップロード

ここでは、SMC 自己署名証明書を ISE 信頼システム署名証明書ストアにアップロードします。

ステップ 1 [管理（Administration）] -> [システム（System）]-> [証明書（Certificate）] -> [信頼できる証明書（Trusted Certificates）] の順に選択し、SMC 自己署名証明書をインポートします。[ISE 内認証の信頼（Trust for authentication within ISE）] をオンにし、[送信（Submit）] をクリックします。



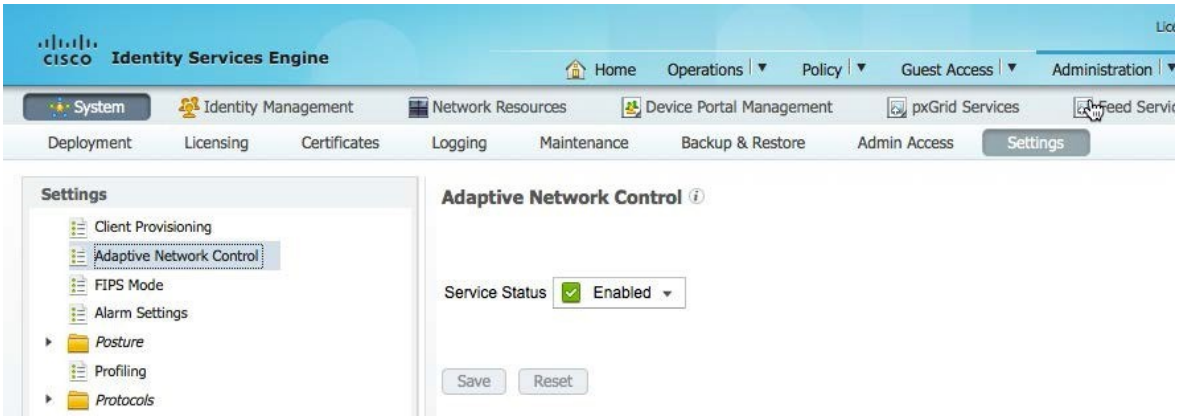
ステップ 2 SMC が ISE pxGrid ノードに登録されます。



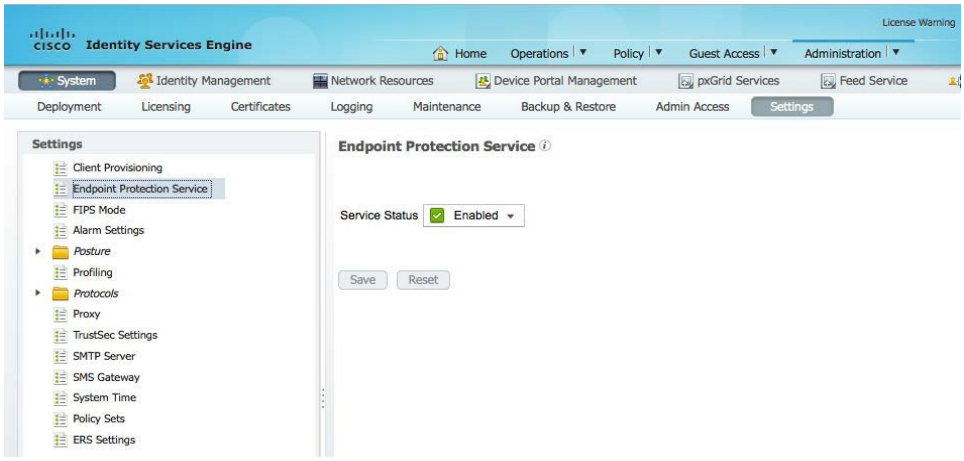
適応型ネットワーク制御（ANC）の有効化

この項では、ISE 1.4 での適応型ネットワーク制御（ANC）の有効化と、認可ポリシーの設定について説明します。ANC は、ISE 1.3 ではエンドポイント保護サービス（EPS）と呼ばれていました。ISE 2.0 以降では不要になり、自動的に有効化されます。ただし、ISE 検疫認可ポリシーを設定する必要があります。

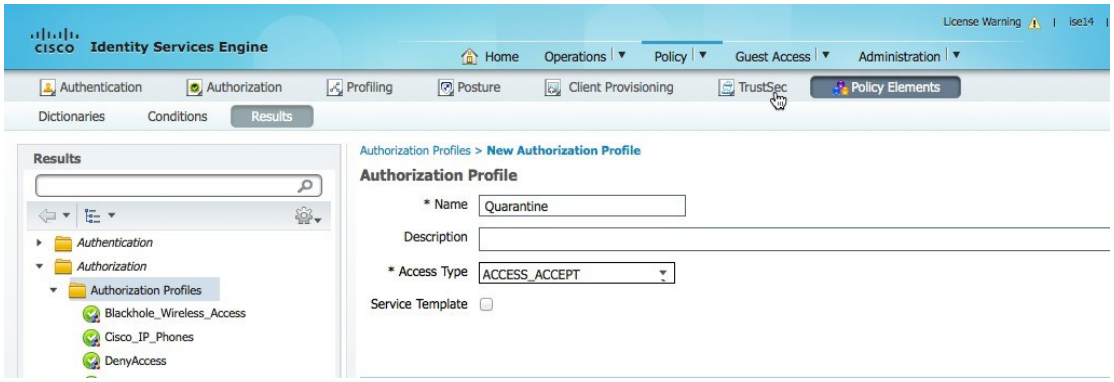
ステップ 1 ISE 1.4 で ANC を有効化するには、[管理（Administration）] -> [システム（System）]-> [設定（Settings）] -> [適応型ネットワーク制御（Adaptive Network Control）] -> [有効化（Enable）] -> [保存（Save）] の順に選択します。



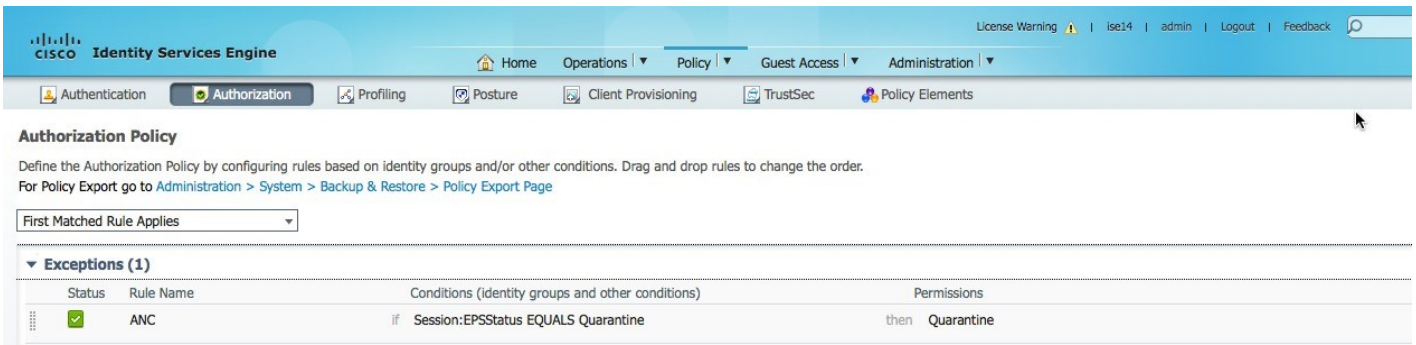
ステップ 2 ISE 1.3 で EPS を有効化するには、[管理（Administration）] -> [システム（System）]-> [設定（Settings）] -> [エンドポイント保護サービス（Endpoint Protection Service）] を選択し、[サービス ステータス（Service Status）] を有効化した後 [保存（Save）] を選択します。



ステップ 3 [ポリシー（Policy）] -> [ポリシー要素（Policy Elements）] -> [結果（Results）] -> [認可（Authorization）] -> [認可プロファイル（Authorization Profiles）] -> [追加（Add）] の順に選択し、[名前（Name）] に Quarantine と入力して、[送信（Submit）] をクリックします。

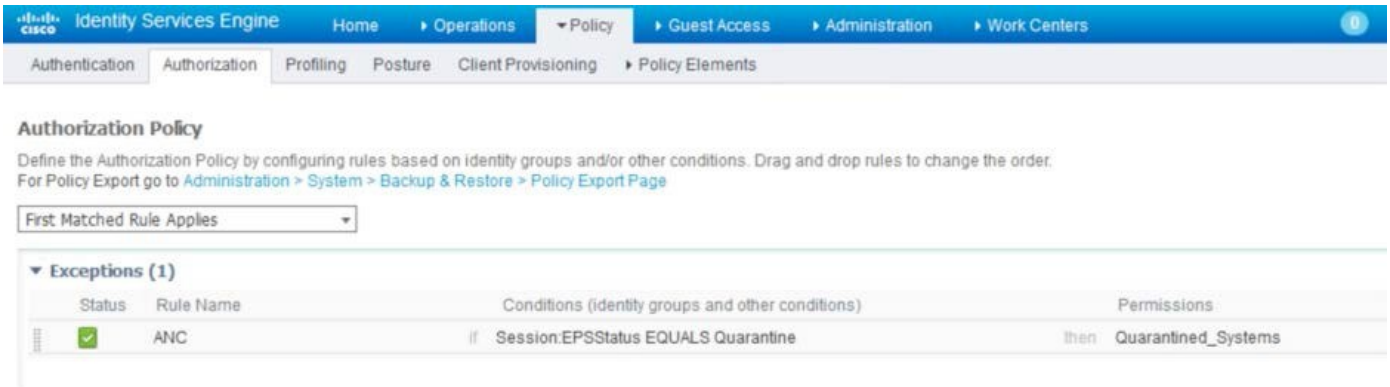


ステップ 4 [ポリシー(Policy)] -> [認可(Authorization)] -> [例外(Exceptions)] を選択し、次のように追加します。



ステップ 5 [ルール名(Rule Name)]:**ANC**
ステップ 6 新しい条件ルールの新しい属性値:**Session:EPStatus:Equals:Quarantine**
ステップ 7 [権限(Permissions)]:[プロファイル(Profiles)]:[標準(Standard)]:[検疫(Quarantine)]
ステップ 8 [完了(Done)] -> [保存(Save)] の順にクリックします。

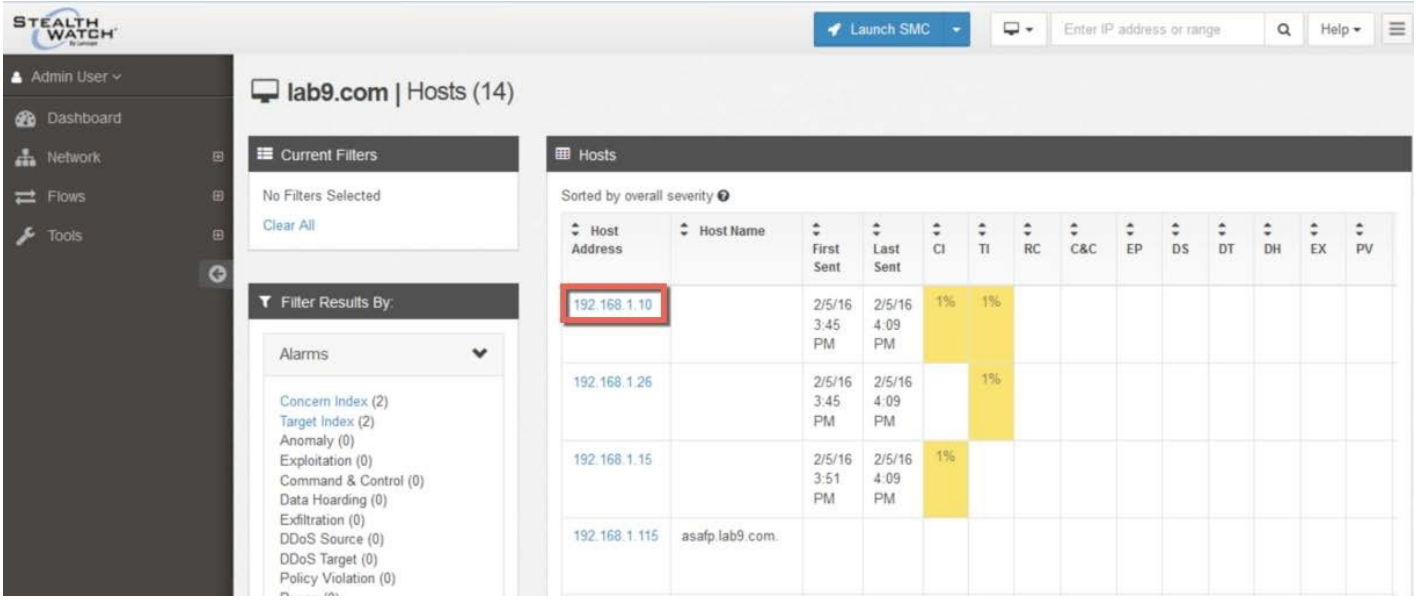
ISE 2.0 では、デフォルトの検疫システム SGT を使用して次のように定義されたポリシーを作成できます。



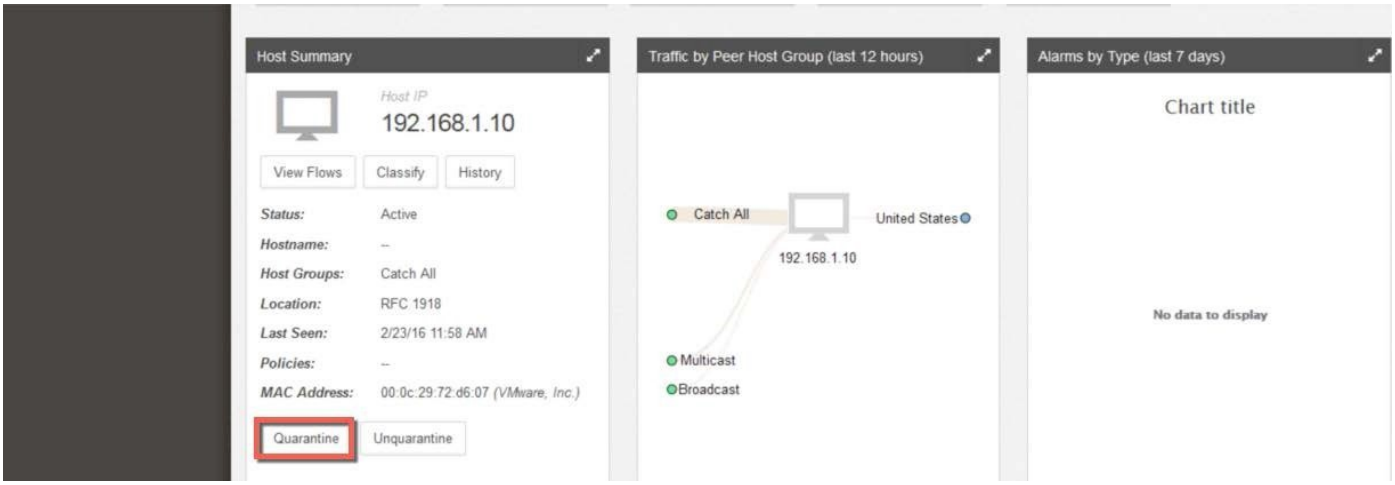
CA 署名付き証明書を使用したテスト

次の使用例では、エンドポイントの検疫/検疫解除を行います。

ステップ 1 SMC から、[ネットワーク(Network)] -> [ホスト(Hosts)] を選択し、検疫するエンドポイントを選択します。



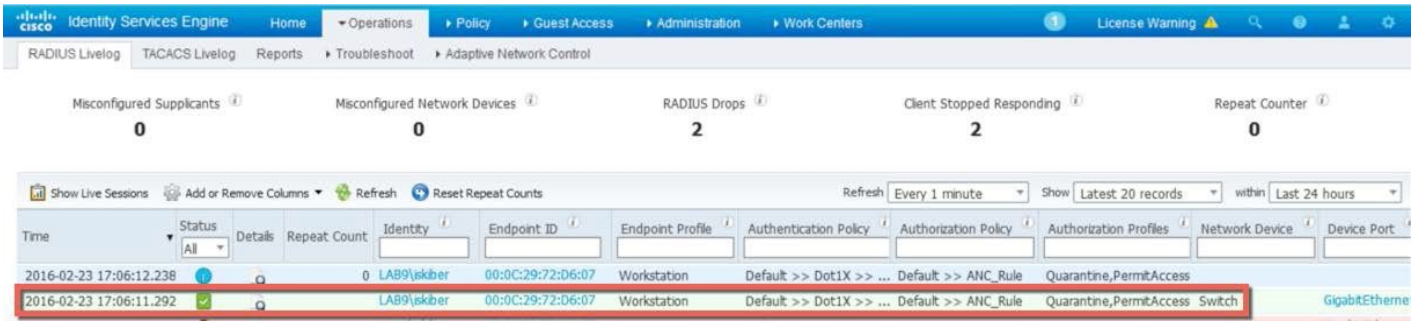
ステップ 2 エンドポイントを選択後、[検疫(Quarantine)] を選択します。



ステップ 3 検疫要求が正常に送信されたことを示すメッセージが表示されます。

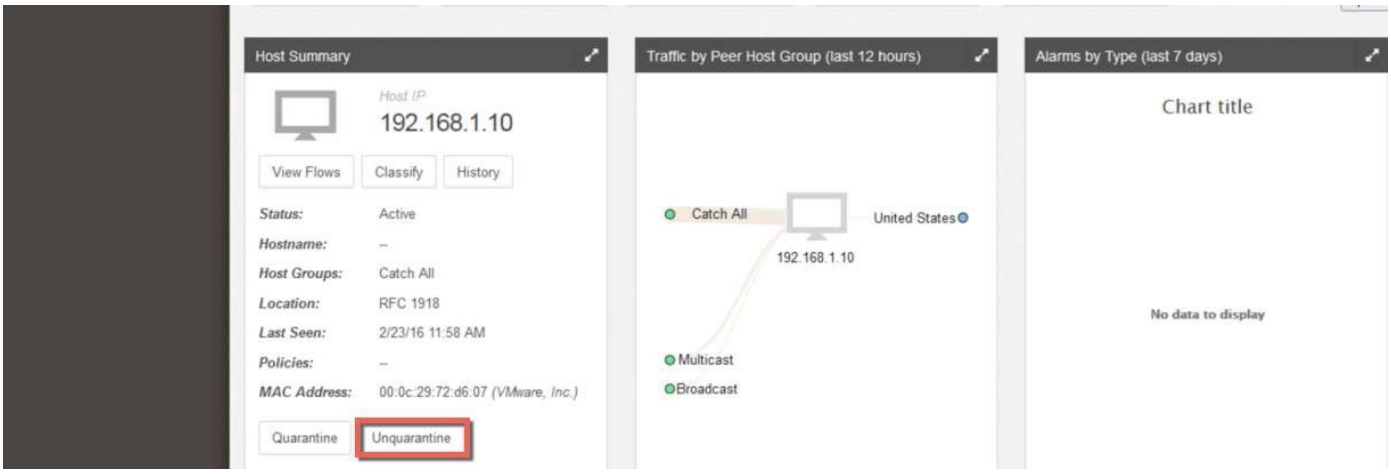
ステップ 4 [OK] を選択します。

ステップ 5 ISE の [操作(Operations)] から [RADIUS Livelog] ビューを選択すると、エンドポイントが検疫されたことを確認できます。

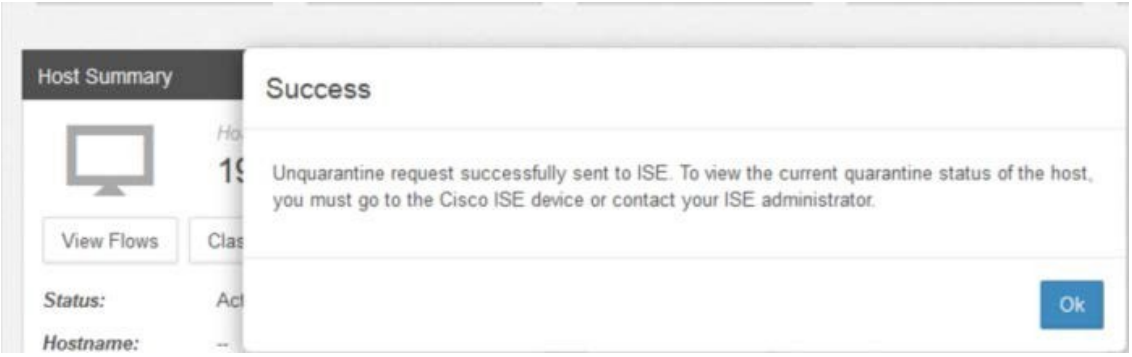


ステップ 6 次に、エンドポイントの検疫を解除します。エンドポイントを選択し、「検疫解除(Unquarantine)] を選択します。

注:ISE 2.0 では、エンドポイントを手動で検疫解除する方法はありません。検疫解除は SMC から実行する必要があります。または、EPS 検疫解除 RESTFUL API を使用する方法もあります。今後この問題に対応するパッチが発行される予定です。

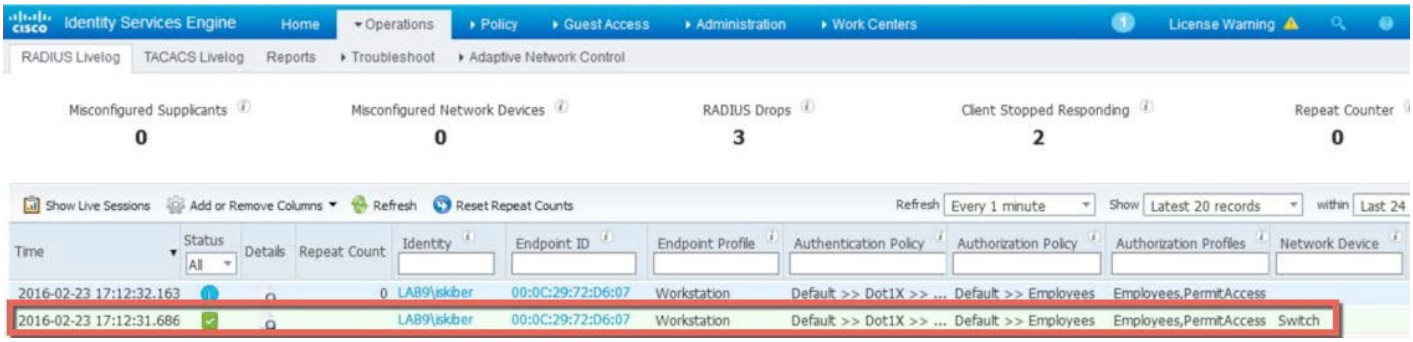


ステップ 7 検疫解除要求が正常に送信されたことを示すメッセージが表示されます。

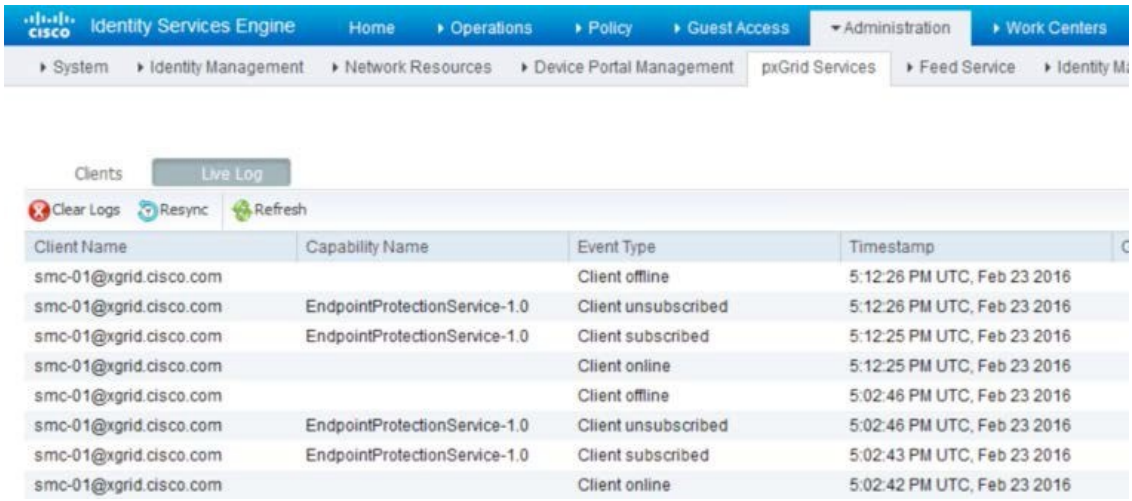


ステップ 8 [OK] を選択します。

ステップ 9 ISE の [操作（Operations）] から [RADIUS Livelog] ビューを選択し、エンドポイントの検疫が解除されたことを確認します。



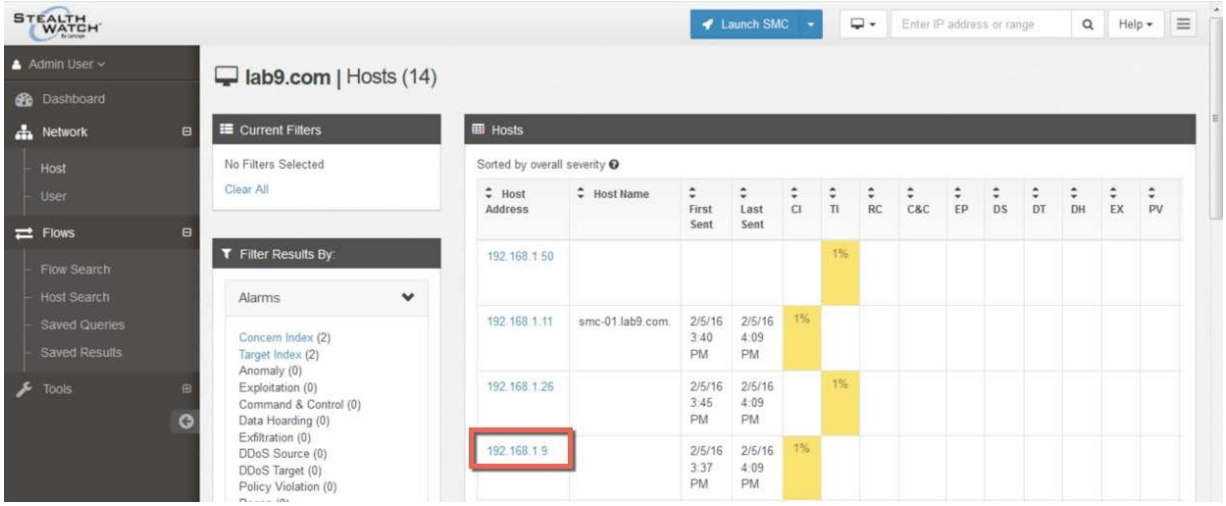
ステップ 10 SMC の pxGrid クライアント Live Log を確認します。これは、SMC がエンドポイント保護サービス機能にサブスクライブし、適応型ネットワーク制御（ANC）のミティゲーション アクションである、検疫/検疫解除を開始した時刻を示しています。



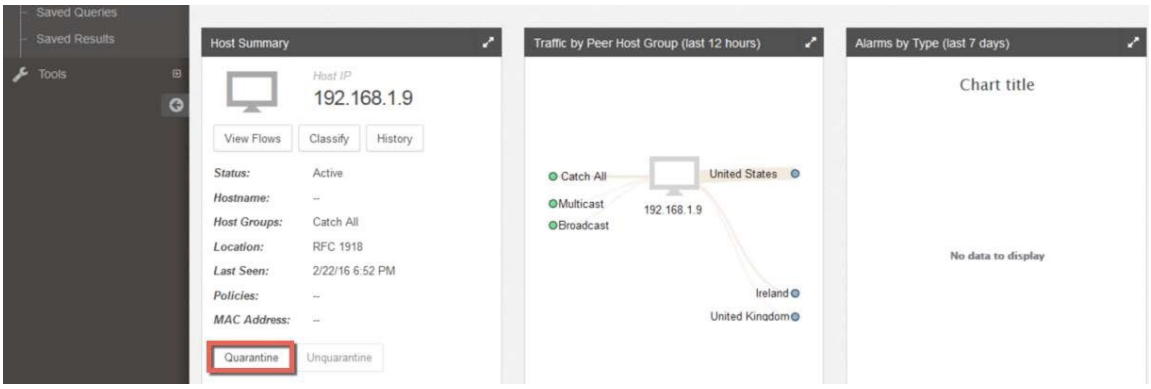
自己署名証明書を使用したテスト

次の使用例では、エンドポイントの検疫/検疫解除を行います。

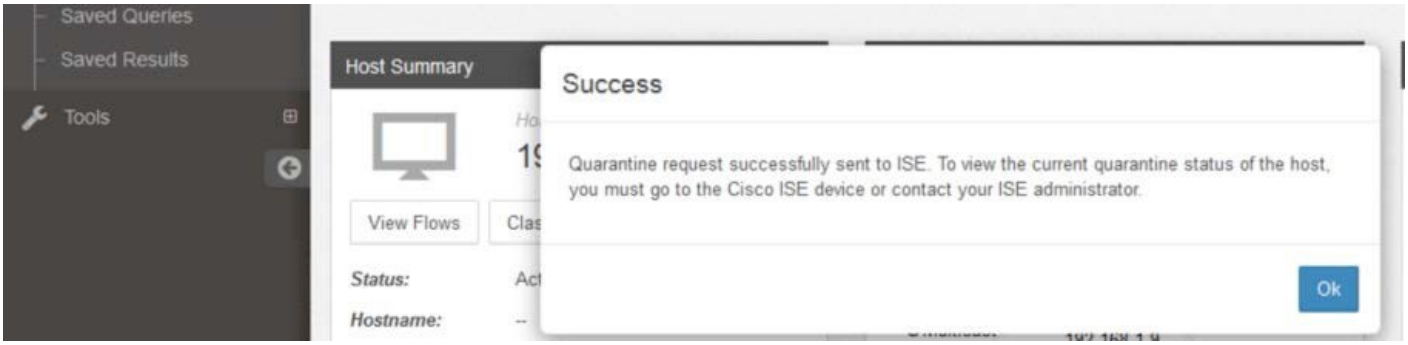
ステップ 1 SMC の [ネットワーク(Network)] -> [ホスト(Host)] メニューから 192.168.1.9 ホストを選択します。



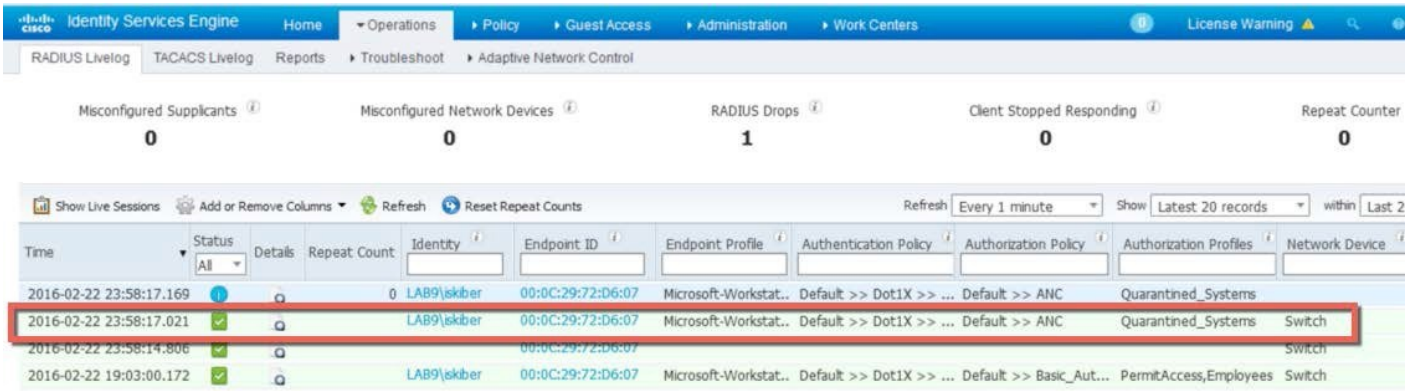
ステップ 2 次のように表示されます。



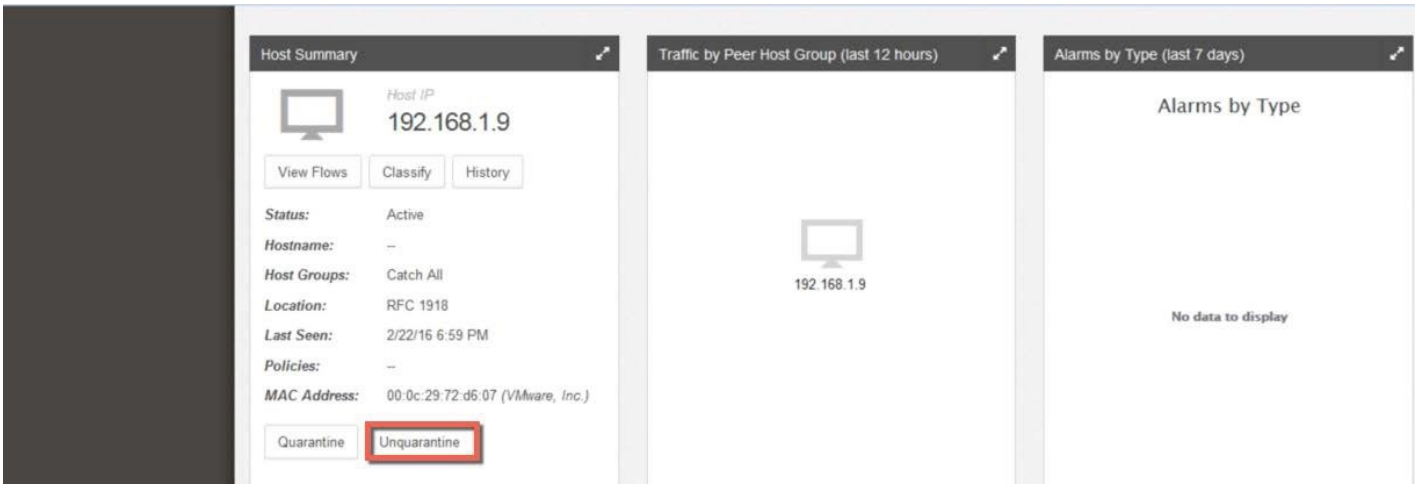
ステップ 3 [検疫（Quarantine）] を選択します。エンドポイントが正常に検疫されたことを示すメッセージが表示されます。



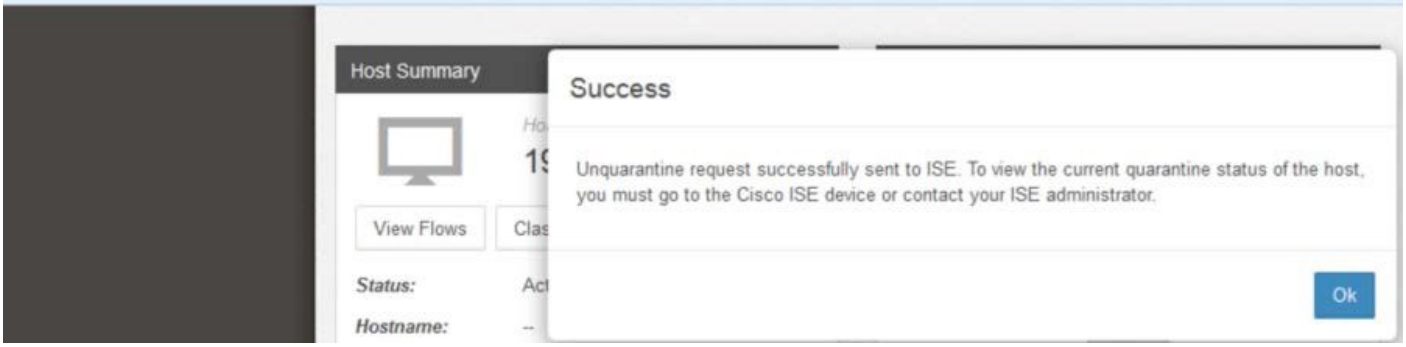
ステップ 4 [OK] を選択します。
ステップ 5 検疫されたエンドポイントを確認します。



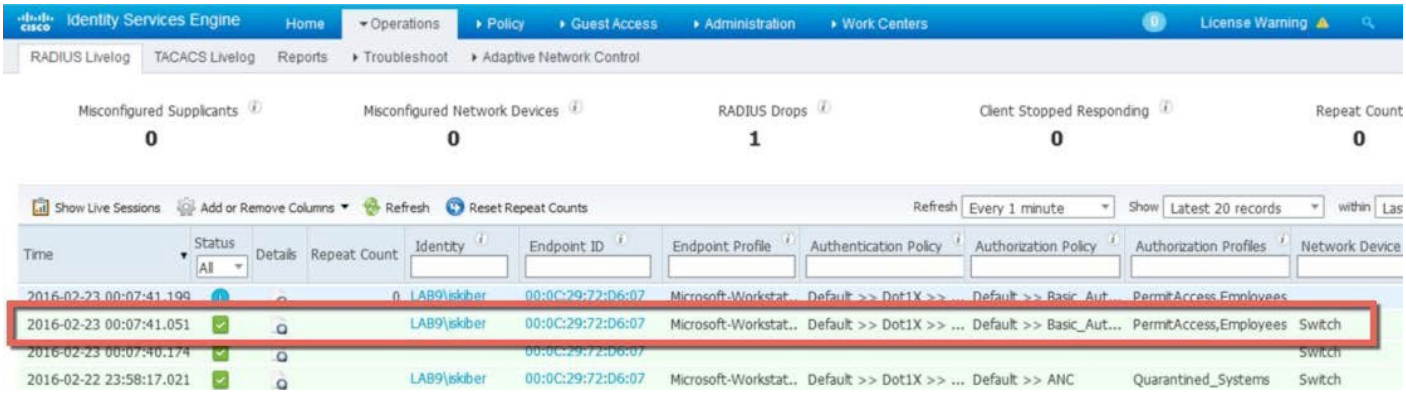
ステップ 6 エンドポイントの検疫を解除するには、SMC の [操作（Operations）] メニューから [検疫解除（Unquarantine）] を選択します。



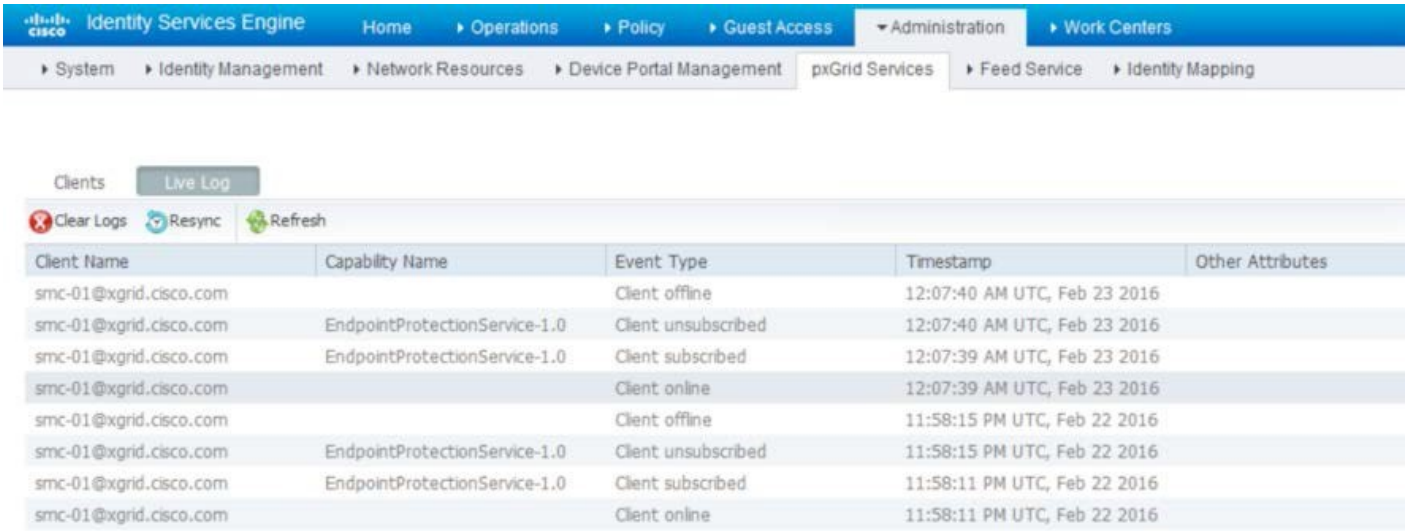
ステップ 7 検疫解除が成功した結果が送信されます。[OK] を選択します。



ステップ 8 ISE メニューの [操作(Operations)] で [RADIUS Livelog] を選択すると、エンドポイントの検疫が解除されたことを確認できます。



ステップ 9 SMC の pxGrid クライアント Live Log を確認します。これは、SMC がエンドポイント保護サービス機能にサブスクライブし、ANC のミティゲーション アクションである、検疫/検疫解除を開始した時刻を示しています。



参考資料

他の pxGrid ドキュメントは、次の場所で参照できます。http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html

- pxGrid による証明書の導入：自己署名 pxGrid クライアントおよび自己署名 ISE pxGrid ノード証明書の使用
- pxGrid による証明書の導入：認証局（CA）署名 pxGrid クライアントおよび自己署名 ISE pxGrid ノード証明書
- pxGrid による証明書の導入：認証局（CA）署名 pxGrid クライアントおよび CA 署名 ISE pxGrid ノード証明書
- Cisco pxGrid との統合の設定およびテスト

付録

MAC での SSH の有効化

ステップ 1 MAC で SSH を有効化します。

```
Johns-Macbook-Pro:Utilities jeppich$ sudo launchctl load -w /System/Library/LaunchDaemons/ssh.plist
Johns-Macbook-Pro:Utilities jeppich$
```

ステップ 2 SMC からローカル PC にファイルをコピーします。

```
Dddd smc:~# scp smc1.crt jeppich@10.0.0.5:/Applications/ise14_certs/
Password:
smc1.crt                                      100%          1.3KB/s   00:00
smc:~#
jeppich@10.0.0.5 smc1.crt smc1.csr smc1.key smc1.key.org
smc:~# scp smc1.key jeppich@10.0.0.5:/Applications/ise14_certs/
Password:
smc1.key                                      100% 1675     1.6KB/s   00:00
smc:~#
```

トラブルシューティング

pxGrid アクティブ スタンバイ設定の使用

ISE の導入ごとに使用できる pxGrid ノードは 2 つのみです。1 つの ISE pxGrid ノードのみをアクティブ化できます。「application status ise」を使用して、正しい ISE pxGrid ノードがアクティブ化されていることを確認してください。

SMC ANC ミティゲーション エラー メッセージ：ISE への検疫要求の送信に失敗しました（Quarantine request failed to be sent to ISE）

[管理（Administration）] > [pxGrid サービス（pxGrid Services）] を選択し、SMC 登録済みクライアントを EPS グループに割り当てください。

ISE pxGrid ノードに pxGrid への接続がない

認証局（CA）署名証明書の場合、ルート CA 証明書が ISE 信頼システム証明書ストアに存在し、ISE pxGrid ノード証明書が ISE システム証明書ストアに存在することを確認してください。pxGrid クライアント証明書には、クライアント認証とサーバ認証の両方の EKU が必要です。

ISE 自己署名証明書の場合、自己署名アイデンティティ証明書がシステム証明書ストアからエクスポートされ、ISE 信頼システム証明書ストアにインポートされていることが必要です。これは、ISE 2.0 では不要です。