BYOD に対する ISE SCEP サポートの設定

内容

概要

このドキュメントでは、Cisco Identity Service Engine（ISE）で個人所有デバイス持ち込み（BYOD）のために、Microsoft ネットワーク デバイス登録サービス（NDES）および Simple Certificate Enrollment Protocol（SCEP）を正常に設定するための手順について説明します。

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。

- ISE リリース 1.1.1 以降
- Microsoft Windows Server 2008 R2

- Microsoft Windows Server 2012 Standard
- Public Key Infrastructure（PKI）および証明書

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。

- ISE リリース 1.1.1 以降
- Windows Server 2008 R2 SP1、ホットフィックス KB2483564 および KB2633200 がインストール済み
- Windows Server 2012 Standard

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。 対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

Microsoft 証明書サービスに関する情報は、シスコの BYOD 用の指針として特に提供されたものです。Microsoft の証明機関、ネットワーク デバイス登録サービス（NDES）、および SCEP 関連のサーバ設定の信頼できる情報源として、Microsoft TechNet を参照してください。

背景説明

Cisco ISE 対応 BYOD 実装のメリットの 1 つは、エンド ユーザがデバイス登録をセルフサービスで実行できることです。これにより、認証クレデンシャルを配布して、ネットワーク上でデバイスを使用可能にするための IT 管理の負担がなくなります。BYODソリューションの中心は、従業員が所有するデバイスに必要な証明書を配布するネットワークサプリカントプロビジョニングプロセスです。この要件を満たすために、Microsoft Certificate Authority(CA)を設定して、SCEPによる証明書登録プロセスを自動化できます。

SCEP は、バーチャル プライベート ネットワーク（VPN）環境において証明書の登録とリモート アクセス クライアントおよびルータへの配布を容易にするために長年にわたって使用されてきました。Windows 2008 R2 Server 上で SCEP 機能を使用するには、NDES のインストールが必要です。NDES ロールをインストールする際、Microsoft インターネット インフォメーション サービス（IIS）Web サーバもインストールされます。IIS は、CA と ISE ポリシー ノードの間の HTTP または HTTPS SCEP 登録要求および応答を停止するために使用されます。

NDES ロールは現行の CA にインストールしたり、メンバー サーバにインストールしたりできます。スタンドアロン導入では、NDES サービスは既存の CA にインストールされ、この CA には認証局サービスと、オプションで証明機関 Web 登録サービスが含まれています。分散した展開の場合、NDES サービスはメンバー サーバにインストールされます。次に、分散された NDES サーバは、アップストリームのルート CA またはサブルート CA と通信するように設定されます。 このシナリオでは、このドキュメントに概略を示すレジストリ変更が NDES サーバ上で行われ、カスタム テンプレートを使用します。証明書はアップストリーム CA に存在します。

テストされた CA/NDES の導入シナリオ

このセクションでは、シスコのラボでテストされた CA/NDES の導入シナリオの概要を示します。Microsoft の CA、NDES、および SCEP 関連のサーバ設定の信頼できる情報源として、Microsoft TechNet を参照してください。

スタンドアロン導入

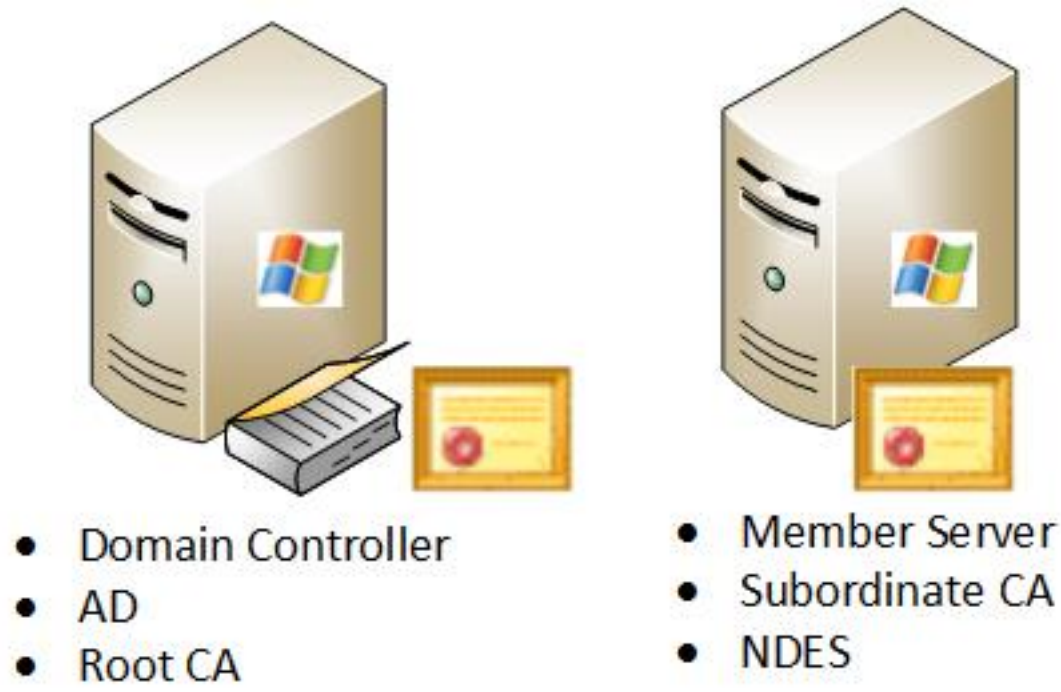
ISE がコンセプト実証（PoC）シナリオで使用される場合、Active Directory（AD）のドメイン コントローラ、ルート CA、および NDES サーバとして機能する自己完結型 Windows 2008 または 2012 マシンを導入することが一般的です。

- Domain Controller
- AD
- Root CA
- NDES

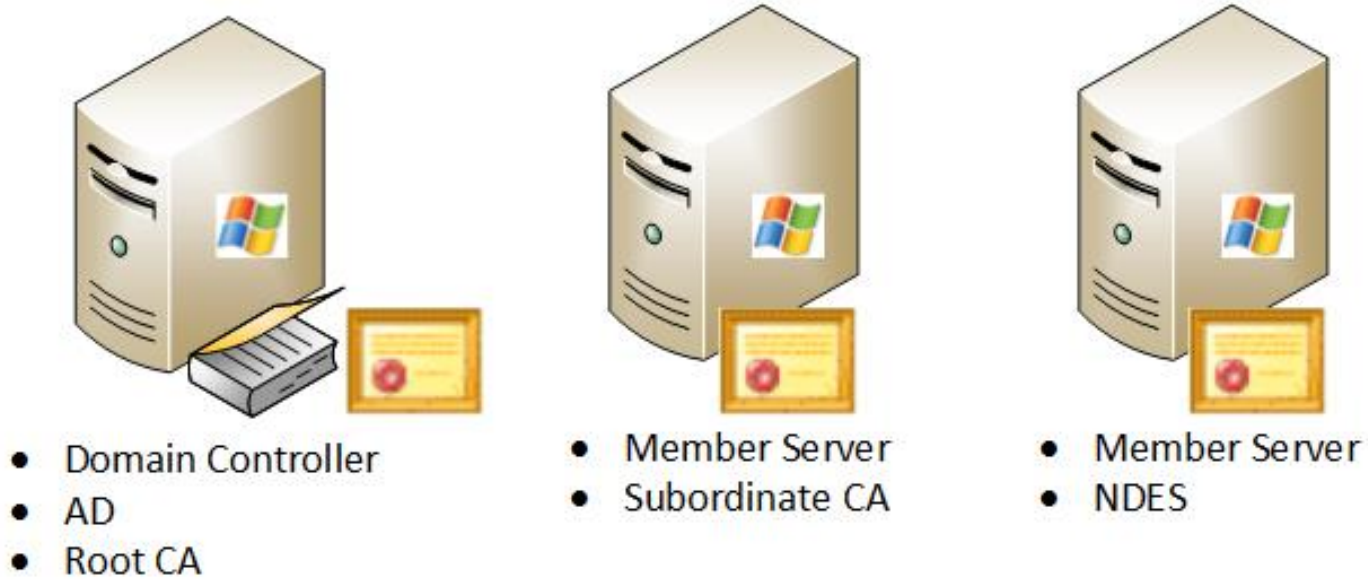
分散型導入

ISE が現在の Microsoft AD/PKI 実稼働環境に統合されている場合は、複数の Windows 2008 または 2012 サーバにサービスを分散することがきわめて一般的です。シスコでは、分散導入用に 2 種類のシナリオをテストしました。

この画像は、分散配置用にテストされた最初のシナリオを示しています。



この画像は、分散配置用にテストされた第 2 のシナリオを示しています。



Microsoft の重要なホットフィックス

BYOD 用の SCEP サポートを設定する前に、次の Microsoft ホットフィックスが Windows 2008 R2 NDES サーバにインストールされていることを確認してください。

- SCEP 証明書が NDES を使用して管理されている場合、Windows Server 2008 R2 で SCEP 証明書の更新要求が失敗します。：この問題は、NDES が **GetCACaps 操作をサポートしないため発生します。**

- エンタープライズ CA が Windows Server 2008 R2 で再起動された後、NDES が証明書要求を送信しない：次のメッセージが**イベント ビューア**で表示されます。「*The Network Device Enrollment Service cannot submit the certificate request (0x800706ba). The RPC server is unavailable*。」

警告：Microsoft CA を設定するときは、ISE が RSASSA-PSS シグニチャ アルゴリズムをサポートしていないことを理解することが重要です。シスコでは代わりに sha1WithRSAEncryption または sha256WithRSAEncryption を使用するように CA ポリシーを設定することを推奨します。

BYOD で重要なポートおよびプロトコル

BYOD で重要なポートとプロトコルの一覧を次に示します。

- TCP：8909 プロビジョニング：Cisco ISE からのウィザード インストール（Windows および Macintosh のオペレーティング システム（OS））
- TCP：443 プロビジョニング：Google Play からのウィザード インストール（Android）
- TCP：8905 プロビジョニング：サプリカント プロビジョニング プロセス
- TCP：80 または TCP：CA への 443 SCEP プロキシ（SCEP RA URL 設定に基づく）

注：必要なポートとプロトコルの最新リストについては、ISE 1.2 の『ハードウェア インストレーション ガイド』を参照してください。

設定

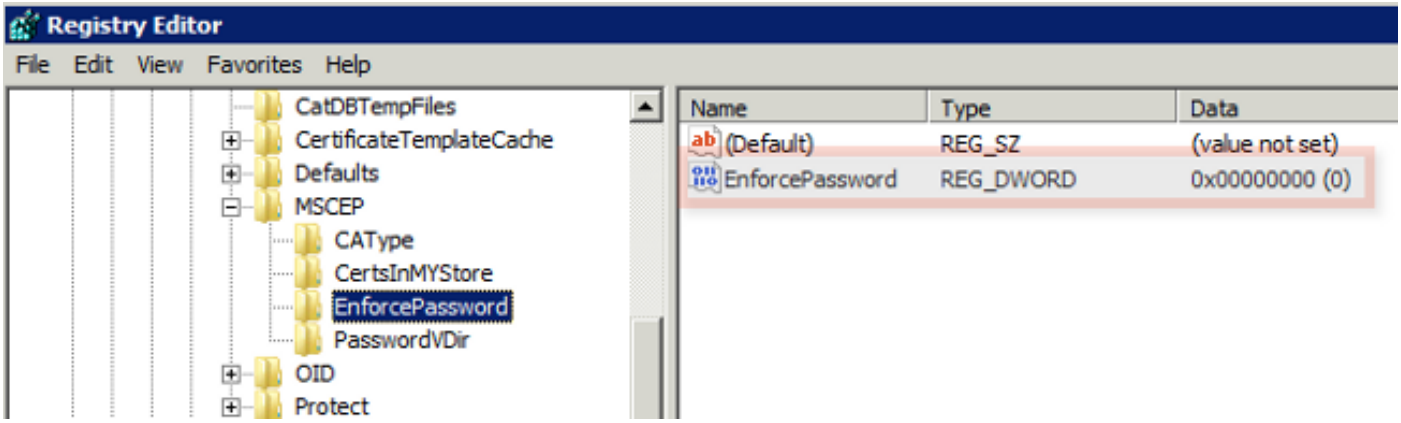
ISE で BYOD のための NDES および SCEP のサポートを設定するには、このセクションを使用します。

SCEP 登録チャレンジ パスワードの要件の無効化

デフォルトで、Microsoft SCEP（MSCEP）の実装では、証明書登録プロセス全体でクライアントとエンドポイントを認証するためにダイナミックなチャレンジ パスワードを使用します。この設定の要件を満たしたうえで、パスワードをオンデマンドで生成するために、NDES サーバで MSCEP の管理 Web GUI を参照する必要があります。登録要求の一部として、このパスワードを含める必要があります。

BYOD の展開におけるチャレンジ パスワードの要件は、ユーザのセルフサービス ソリューションの目的と適合しません。この要件を削除するには、NDES サーバの次のレジストリ キーを変更する必要があります。

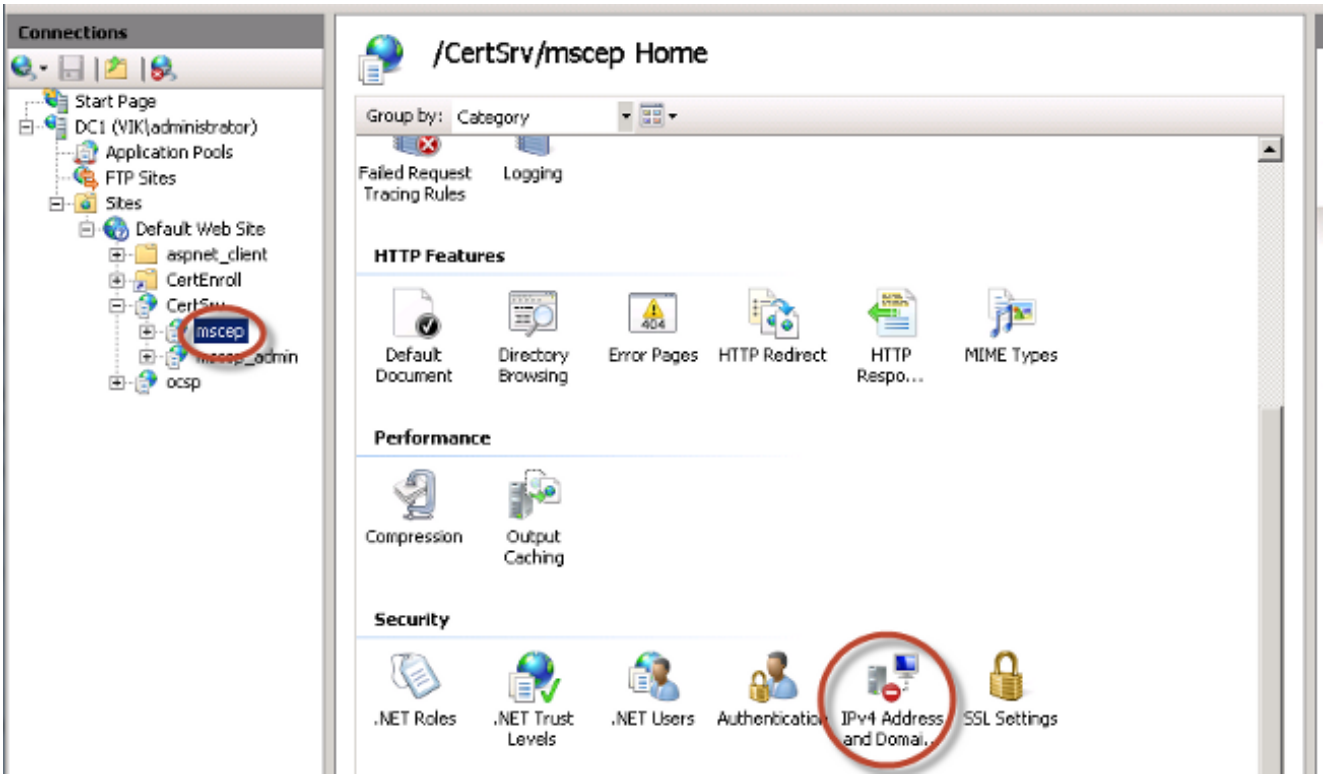
1. [Start] をクリックして、検索バーで **regedit** と入力します。
2. [Computer] > [HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Microsoft] > [Cryptography] > [MSCEP] > [EnforcePassword] に移動します。
3. [EnforcePassword] 値が **0 に設定されていることを確認します（デフォルト値は 1）です。**



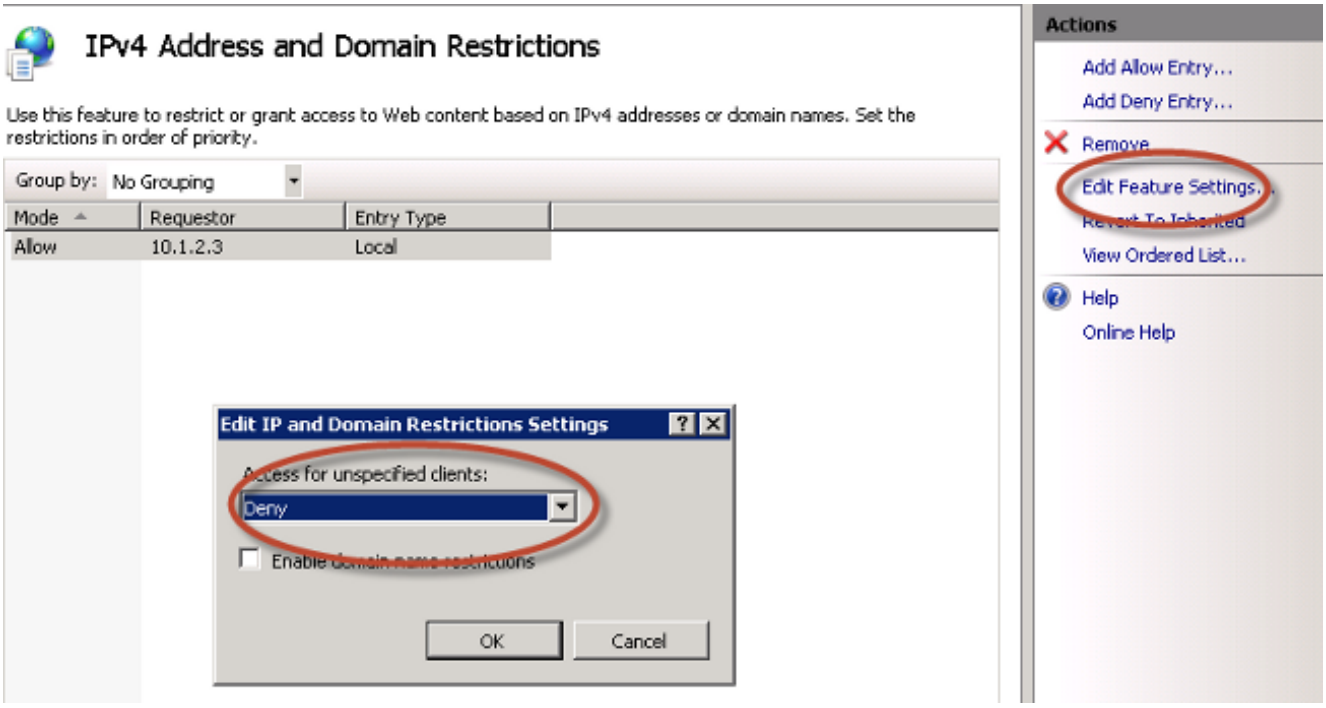
SCEP の登録を既知 ISE ノードに限定

一部の導入シナリオでは、SCEP の通信先を既知の ISE ノードで構成された選択リストに制限する必要がある場合があります。IIS の IPv4 アドレスおよびドメインの制限機能によって実現できます。

1. IIS を開き、/CertSrv/mscep Web サイトにナビゲートします。



2. **[Security] > [IPv4 Address and Domain Restrictions]をダブルクリックします。ISEノードのIPv4アドレスまたはドメイン名に基づいてWebコンテンツへのアクセスを許可または制限するには、**[Add Allow Entry]および[Add Deny Entry]を使用使用します。指定されていないクライアントのデフォルト アクセスのルールを定義するために、[Edit Feature Settings] アクションを使用します。

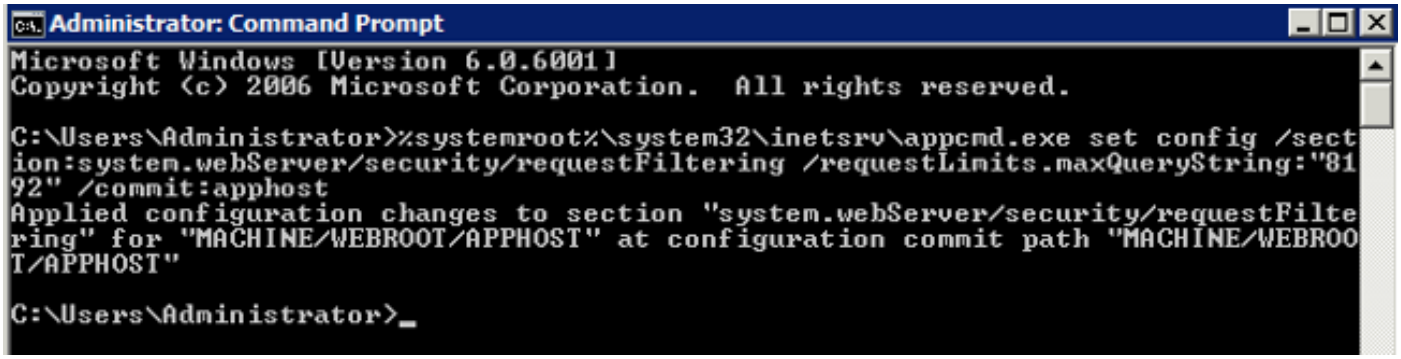


IIS で URL の長さを拡張

ISE では、IIS Web サーバにとって長すぎる URL を生成することがあります。この問題を回避するために、長い URL を許可するようにデフォルト IIS 構成を修正できます。NDES サーバ CLI から次のコマンドを入力します。

```
%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/
 security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost
```

注：クエリ文字列のサイズは ISE およびエンドポイントの設定によって異なる場合があります。管理者権限を使用して NDES サーバ CLI から次のコマンドを入力します。



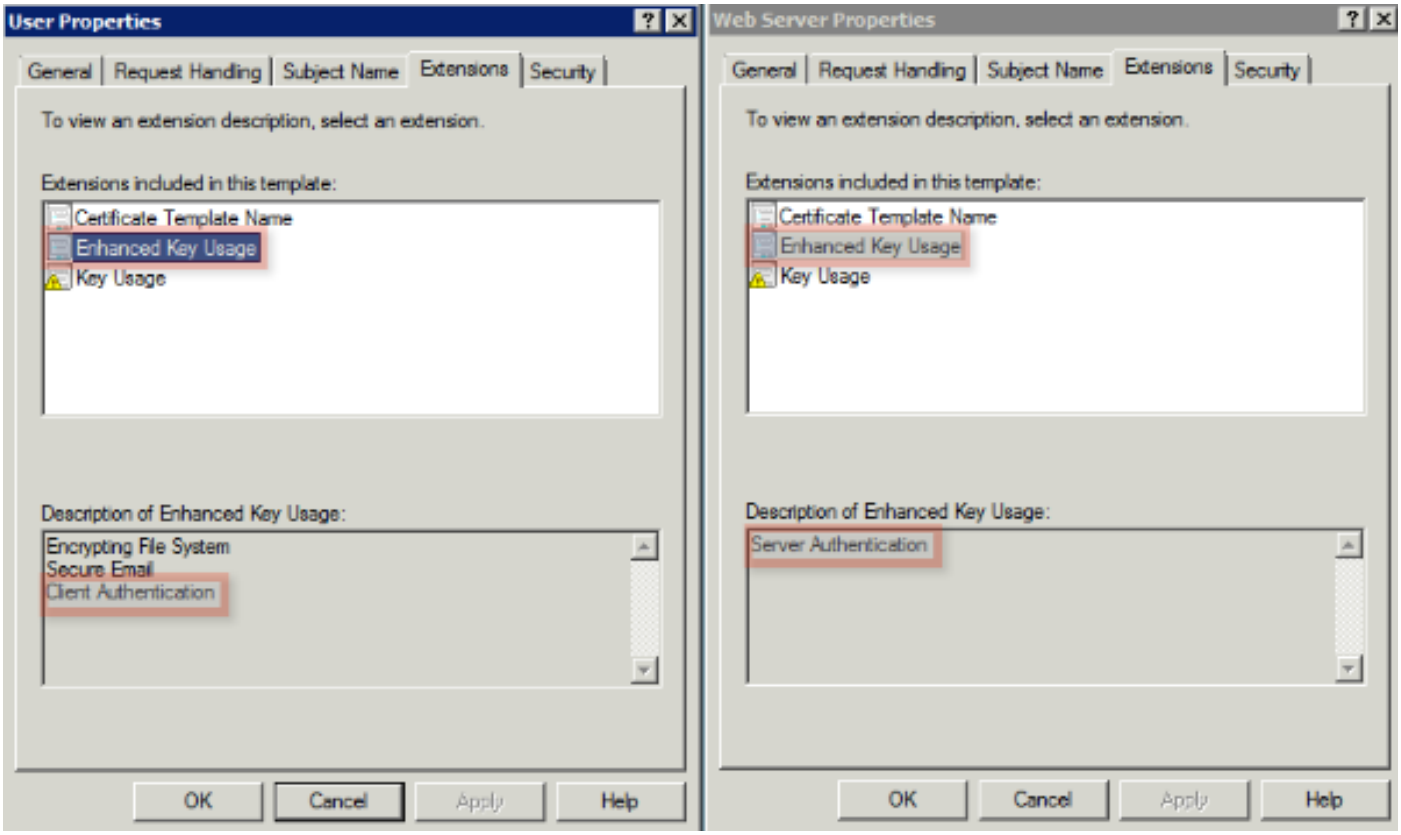
証明書テンプレートの概要

Microsoft CA の管理者は、一般的な証明書一式にアプリケーション ポリシーを適用するために使用する 1 個以上のテンプレートを設定できます。これらのポリシーは、証明書および関連付けられているキーを使用する機能を識別するために役立ちます。アプリケーション ポリシーの値は、証明書のキーの拡張用途（EKU）フィールドに格納されています。オーセンティケータは EKU フィールドの値を解析し、クライアントによって提示された証明書が目的の機能のために使用できるか確認します。もっと一般的な用途としては、サーバ認証、クライアント認証、IPSec VPN、電子メールなどがあります。ISE の観点では、よく使用される EKU 値として、サーバ認証およびクライアント認証などがあります。

たとえば、セキュリティ保護された銀行の Web サイトをブラウズするとき、要求を処理する Web サーバは、サーバ認証のアプリケーション ポリシーを持つ証明書で設定されています。サーバが HTTPS 要求を受け取ると、接続しようとしている Web ブラウザに、認証用のサーバ認証証明書を送信します。ここで重要な点は、これはサーバからクライアントへの単方向の交換だということです。これは ISE に関係するため、サーバ認証証明書の一般的な用途は管理 GUI アクセスです。ISE は設定された証明書を接続したブラウザに送信して、クライアントからの証明書の受信は予期しません。

BYOD などの EAP-TLS を使用するサービスの場合、相互認証が求められます。この双方向の証明書交換をイネーブルにするには、ISE の ID 証明書を生成するために使用するテンプレートは、サーバ認証の最小アプリケーション ポリシーを所有する必要があります。Web サーバ証明書テンプレートがこの要件を満たします。エンドポイント証明書を生成する証明書テンプレートは、クライアント認証の最小限のアプリケーション ポリシーを格納している必要があります。ユーザ証明書テンプレートがこの要件を満たします。Inline Policy Enforcement Point（iPEP）などのサービス用に ISE を設定する場合、ISE のバージョン 1.1.x 以前を使用するのであれば、ISE サーバの ID 証明書の生成に使用されるテンプレートはクライアントとサーバの両方の認証属性を含む必要があります。これにより、管理ノードとインライン ノードが相互認証できます。iPEP 向けの EKU の確認は ISE のバージョン 1.2 で削除されました。このバージョンでこの要件の関連性が低くなくなりました。

デフォルトの Microsoft CA の Web サーバとユーザのテンプレートを再利用できます。このドキュメントで説明されている手順によって新しいテンプレートをクローンおよび作成することもできます。これらの証明書要件に基づき、CA 設定と、結果として生じた ISE 証明書およびエンドポイント証明書を慎重に計画することで、実稼働環境にインストールされたときの不要な設定変更を最小限に抑えるようにする必要があります。



証明書テンプレートの設定

概要で述べたように、SCEP は IPSec VPN 環境で広く使用されています。その結果、NDES ロールのインストールにより、サーバが SCEP 用の **IPSec（オフライン要求）**テンプレートを使用

するように自動設定されます。このため、Microsoft CA を BYOD 用に準備する際の最初のステップの 1 つは、正しいアプリケーション ポリシーで新しいテンプレートを作成することです。スタンドアロン導入では、証明機関と NDES サービスは、同じサーバに配置され、テンプレートおよび必要なレジストリの修正は、同じサーバに含まれています。分散した NDES 展開では、レジストリ変更は NDES サーバ上で実行されます。ただし、実際のテンプレートは、NDES サービスのインストールで指定されたルート CA またはサブルート CA 上に定義されます。

証明書テンプレートを設定するには、次の手順を実行します。

1. **admin** として CA サーバにログオンします。

2. [Start] > [Administrative Tools] > [Certification Authority] を選択します。

3. CA サーバの詳細を開き、[Certificate Templates] フォルダを選択します。このフォルダには現在有効なテンプレートのリストが含まれています。

4. 証明書テンプレートを管理するために、[Certificate Templates] フォルダを右クリックして [Manage] を選択します。

5. [Certificate Templates Console] に、非アクティブなテンプレートが表示されます。

6. SCEP で使用する新規テンプレートを構成するために、User などのすでに存在するテンプレートを右クリックし、[Duplicate Template] を選択します。

7. 環境内の最小 CA OS に応じて、[Windows 2003] または [Windows 2008] を選択します。

8. [General] タブに、ISE-BYOD などの表示名と有効期間を追加します。他のすべてのオプションは、チェックをオフのままにしておきます。
   注：テンプレートの有効期間は CA のルート証明書および中間証明書の有効期間以下にする必要があります。
9. [Subject Name] タブをクリックし、[Supply in the request] が選択されていることを確認します。

10. [Issuance Requirements] タブをクリックします。シスコでは、一般的な階層型 CA の環境では [Issuance policies] を空白のままにしておくことを推奨します。

11. [Extensions] タブ、[Application Policies]、[Edit] の順にクリックします。

12. [Add] をクリックして、[Client Authentication] がアプリケーション ポリシーとして追加されていることを確認します。[OK] をクリックします。

13. [セキュリティ]タブをクリックし、[**追加...]をクリックします。**.NDES サービス インストールに定義されている SCEP のサービス アカウントに、テンプレートに対するの完全な制御権があることを確認し、[OK] をクリックします。

14. [Certification Authority GUI] インターフェイスに戻ります。

15. [Certificate Templates] ディレクトリを右クリックします。[New] [Certificate Template to Issue] に移動します。

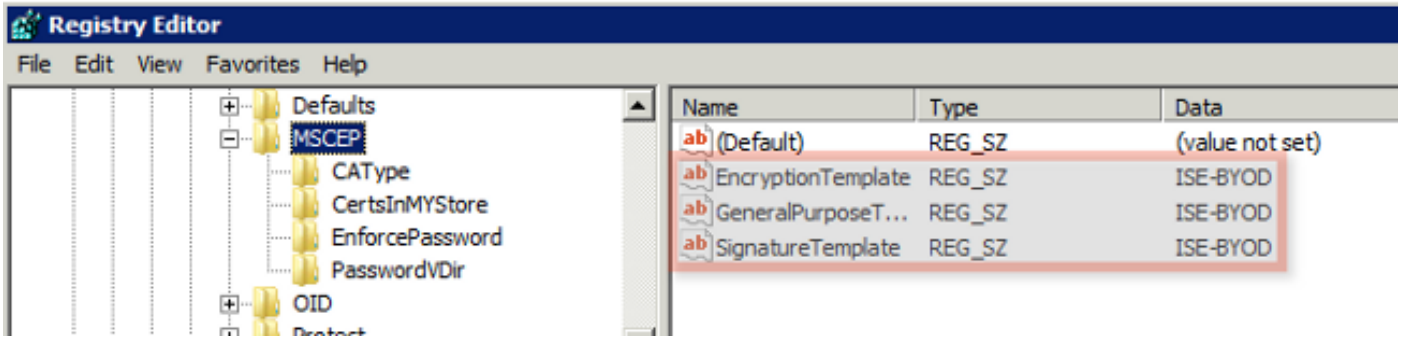
16. 以前設定した [ISE-BYOD] テンプレートを選択し、[OK] をクリックします。

    注：または、certutil -SetCAtemplates +ISE-BYOD コマンドで CLI からテンプレートをイネーブルにできます。
    ISE-BYOD テンプレートが、使用可能な証明書テンプレート リストにリストされます。

証明書テンプレートのレジストリの設定

証明書テンプレートのレジストリ キーを設定するには、次の手順を実行します。

1. NDES サーバに接続します。
2. [Start] をクリックして、検索バーで **regedit** と入力します。
3. [Computer] > [HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Microsoft] > [Cryptography] > [MSCEP] に移動します。
4. [EncryptionTemplate]、[GeneralPurposeTemplate]、および [SignatureTemplate] キーを、[IPSec (Offline Request)] から、以前作成された [ISE-BYOD] テンプレートに変更します。
5. レジストリ設定を適用するために NDES サーバをリブートします。



SCEP プロキシとして ISE を設定する

BYOD 展開では、エンドポイントはバックエンド NDES サーバと直接通信しません。その代わりに、ISE ポリシー ノードが SCEP プロキシとして設定され、エンドポイントの代わりに NDES と通信します。エンドポイントは ISE と直接通信します。NDES サーバの IIS インスタンスは、SCEP 仮想ディレクトリのための HTTP バインディングまたは HTTPS バインディングあるいはその両方をサポートするように設定できます。

SCEP プロキシとして ISE を設定するには、次の手順を実行します。

1. 管理者クレデンシャルを使用して **ISE GUI にログインします。**
2. [Administration]、[Certificates]、[SCEP CA Profiles] の順にクリックします。
3. [Add] をクリックします。
4. サーバの名前と説明を入力します。

5. SCEP サーバの URL を、IP または完全修飾ドメイン名（FQDN）で入力します（例：http://10.10.10.10/certsrv/mscep/）。

6. [Test Connectivity] をクリックします。接続に成功すると、正常なサーバ応答ポップアップメッセージが出ます。

7. [Save] をクリックして設定を適用します。

8. 確認するために、[Administration]、[Certificates]、[Certificate Store] の順にクリックし、SCEP NDES サーバの RA 証明書が ISE ノードに自動的にダウンロードされていることを確認します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

この項では、設定のトラブルシューティングについて説明します。

トラブルシューティングに関する一般的な注意事項

設定をトラブルシュートするために使用可能な重要な注意事項の一覧を次に示します。

- エンドポイントである ISE、NDES、および CA 間のパスに沿ってデバッグ地点および取得地点を識別するのに役立つように、BYOD ネットワーク トポロジを論理的な中継点に分割します。
- ISE ノードと CA で Network Time Protocol（NTP）時刻源が共通していることを確認します。
- エンドポイントでは、DHCP から取得された NTP およびタイム ゾーン オプションを使用して時刻を自動的に設定できる必要があります。
- クライアントの DNS サーバは ISE ノードの FQDN を解決できる必要があります。
- TCP 80 または TCP 443 あるいはその両方が、ISE と NDES サーバの間の双方向で許可されていることを確認します。
- クライアント側のロギングに優れているため、Windows マシンを使用してテストします。オプションで、クライアント側のコンソール ログをモニタするために、Apple の iDevice および Apple iPhone 構成ユーティリティを使用します。
- CA および NDES サーバ アプリケーション ログを監視して登録エラーを確認し、Google または TechNet を使用してこれらのエラーを調査します。

- ISE、NDES、および CA の間でのパケット収集に役立つように、テスト フェース全体で SCEP 用の HTTP を使用します。

- ISE Policy Service Node（PSN）で TCP ダンプ ユーティリティを使用し、NDES サーバとの間のトラフィックをモニタします。これは [Operations] > [Diagnostic Tools] > [General Tools] にあります。

- ISE PSN とやりとりする SCEP トラフィックを取得するために、CA および NDES サーバに Wireshark をインストールするか、中継スイッチ上で SPAN を使用します。

- 適切な CA 証明書チェーンがクライアント証明書の認証のために ISE ポリシー ノードにインストールされていることを確認します。

- 適切な CA 証明書チェーンがオンボーディング中にクライアントに自動的にインストールされるようにします。

- ISE およびエンドポイント ID 証明書をプレビューし、正しい EKU 属性が存在することを確認します。

- ISE GUI でライブ認証ログを監視し、認証の失敗および許可の失敗がないか確認します。
注：サーバ認証の EKU を持つクライアント証明書など、間違った EKU が存在する場合、サプリカントがクライアント証明書交換を初期化しないことがあります。したがって、認証の失敗は常に ISE ログに存在するとは限りません。
- NDES が分散展開にインストールされた場合、サービスのインストール内ではリモートのルート CA またはサブルート CA が CA 名またはコンピュータ名によって指定されます。NDES サーバは、このターゲット CA サーバに対して証明書登録要求を送信します。エンドポイントの証明書登録プロセスに失敗すると、パケット キャプチャ（PCAP）によって、NDES サーバが ISE ノードに 404 Not Found エラーを返したことが表示されることがあります。この問題を解決するには、NDES サービスを再インストールし、CA の名前ではなく [Computer Name] オプションを選択します。

- デバイスのオンボーディング後に SCEP CA のチェーンが変更されないようにしてください。Apple iOS などのエンドポイント OS では、事前にインストールされていた BYOD プロファイルが自動的に更新されません。この iOS の例では、現在のプロファイルをエンドポイントから削除する必要があり、エンドポイントを ISE データベースから削除する必要があります。これにより、オンボーディングを再度実行できるようになります。

- インターネットに接続して Microsoft ルート証明書プログラムで自動的に証明書を更新するために Microsoft 証明書サーバを設定できます。インターネット ポリシーで制限された環境でこのネットワーク取得オプションを設定すると、インターネットに接続できない CA/NDES サーバはデフォルトではタイムアウトに 15 秒かかる場合があります。これにより、ISE などの SCEP プロキシからの SCEP 要求を処理するめに 15 秒の遅延が加わることがあります。ISE は応答を受信しなかった 12 秒後に SCEP 要求をタイムアウトさせるようにプログラムされています。この問題を解決するには、CA/NDES サーバのインターネット アクセスを許可するか、Microsoft CA/NDES サーバのローカル セキュリティ ポリシーでネットワークの取得のタイムアウト設定を変更します。Microsoft サーバでこの設定を見つけるには、[Start] > [Administrative Tools] > [Local Security Policy] > [Public Key Policies] > [Certificate Path Validation Settings] > [Network Retrieval] に移動します。

クライアント側のロギング

クライアント側のロギングに関する問題をトラブルシュートするために使用する便利なテクニックの一覧を以下に示します。

- ログ**%temp%\spwProfileLog.txtを入力します。**コマンドを発行して、Microsoft Windowsアプリケーションのクライアント側ログを表示します。
  注：WinHTTP は、Microsoft Windows エンドポイントと ISE 間の通信に使用されます。エラー コードのリストについては Microsoft Windows の記事『Error Messages』を参照してください。
- Android アプリケーションのクライアント側の口グを表示するには、**/sdcards/downloads/spw.log コマンドを入力します。**

- MAC OSX の場合は、コンソール アプリケーションを使用し、**SPW プロセスを探します。**

- **Apple iOSの場合、**Apple Configurator 2.0を使用してメッセージを表示します。

ISE のロギング

ISE ログを表示するには、次の手順を実行します。

1. [Administration] > [Logging] > [Debug Log Configuration] に移動し、適切な ISE ポリシー ノードを選択します。

2. デバッグまたはトレースするために必要に応じて**クライアントおよびプロビジョニング**のログを設定します。

3. 問題を再現し、検索を容易にするために、MAC、IP、ユーザなどの関連するシード情報を記録します。

4. [Operations] > [Download Logs] に移動し、適切な ISE ノードを選択します。

5. [Debug Logs] タブで、**ise-psc.log** という名前のログをデスクトップにダウンロードします。

6. Notepad ++ などの高機能エディタを使用して、ログ ファイルを解析します。

7. 問題の切り分けが終了したら、ログ レベルをデフォルト レベルに戻します。

NDES のロギングおよびトラブルシューティング

詳細については、次の資料を参照してください。『AD CS:Troubleshooting Network Device Enrollment Service』（ Windows Server 技術情報 ）。

関連情報

- **BYOD ソリューション ガイド - 認証権限サーバ設定**

- Windows 2008 R2 の NDES 概要
- MSCEP ホワイト ペーパー
- SSL のサポートのための NDES サーバの設定
- EAP-TLS、または EAP-TLS と PEAP を組み合わせて使用する場合の証明書の必要条件
- テクニカル サポートとドキュメント