Configurer la prise en charge ISE SCEP pour le BYOD

Contenu

Introduction

Ce document décrit les étapes qui sont utilisées afin de configurer correctement le service d'inscription de périphériques réseau Microsoft (NDES) et le protocole SCEP (Simple Certificate Enrollment Protocol) pour Bring Your Own Device (BYOD) sur Cisco Identity Services Engine (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- ISE version 1.1.1 ou ultérieure
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 Standard
- Infrastructure à clé publique (PKI) et certificats

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ISE version 1.1.1 ou ultérieure
- Windows Server 2008 R2 SP1 avec correctifs KB2483564 et KB2633200 installés
- Windows Server 2012 Standard

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Les informations relatives aux services de certificats Microsoft sont fournies comme guide spécifique pour le BYOD de Cisco. Reportez-vous à Microsoft TechNet en tant que source définitive de vérité pour les configurations de serveur liées à Microsoft, NDES (Network Device Enrollment Service) et SCEP.

Informations générales

L'un des avantages de la mise en oeuvre du BYOD Cisco ISE est la capacité des utilisateurs finaux à effectuer l'enregistrement des périphériques en libre-service. Cela élimine la charge administrative pesant sur le service informatique pour distribuer les informations d'identification d'authentification et activer les périphériques sur le réseau. Au coeur de la solution BYOD se trouve le processus de provisionnement des supplicants réseau, qui vise à distribuer les certificats requis aux périphériques appartenant aux employés. Afin de répondre à cette exigence, une autorité de certification Microsoft (CA) peut être configurée afin d'automatiser le processus d'inscription de certificat avec le SCEP.

SCEP est utilisé depuis des années dans des environnements de réseaux privés virtuels (VPN) afin de faciliter l'inscription et la distribution de certificats aux clients et routeurs d'accès à distance. L'activation de la fonctionnalité SCEP sur un serveur Windows 2008 R2 nécessite l'installation de NDES. Lors de l'installation du rôle NDES, le serveur Web Microsoft Internet Information Services (IIS) est également installé. IIS est utilisé afin de mettre fin aux demandes d'enregistrement SCEP HTTP ou HTTPS et aux réponses entre le noeud de stratégie CA et ISE.

Le rôle NDES peut être installé sur une autorité de certification actuelle ou sur un serveur membre. Dans un déploiement autonome, le service NDES est installé sur une autorité de certification existante qui inclut le service Autorité de certification et, éventuellement, le service d'inscription Web de l'autorité de certification. Dans un déploiement distribué, le service NDES est installé sur un serveur membre. Le serveur NDES distribué est ensuite configuré afin de communiquer avec une autorité de certification racine ou sous-racine en amont. Dans ce scénario, les modifications de Registre décrites dans ce document sont effectuées sur le serveur NDES avec le modèle personnalisé, où les certificats résident sur l'autorité de certification en amont.

Scénarios de déploiement CA/NDES testés

Cette section présente brièvement les scénarios de déploiement CA/NDES qui ont été testés dans les travaux pratiques Cisco. Reportez-vous à Microsoft TechNet en tant que source définitive de vérité pour les configurations de serveurs liées à Microsoft CA, NDES et SCEP.

Déploiements autonomes

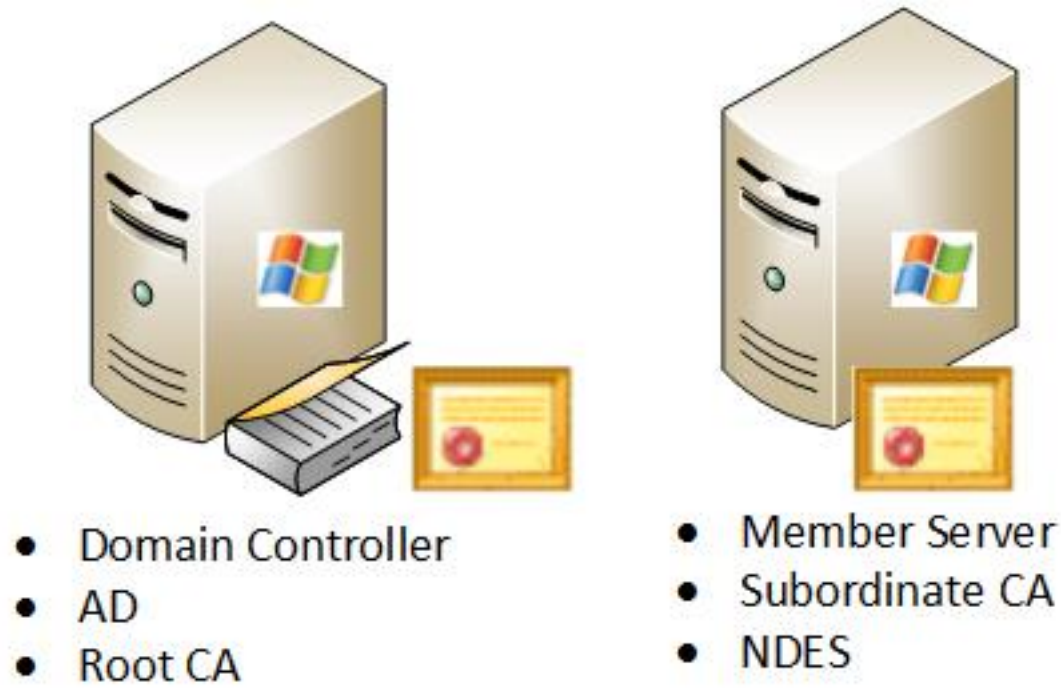
Lorsque ISE est utilisé dans un scénario PoC (Proof of of Concept), il est courant de déployer une machine Windows 2008 ou 2012 autonome qui agit en tant que contrôleur de domaine Active Directory (AD), autorité de certification racine et serveur NDES :

- Domain Controller
- AD
- Root CA
- NDES

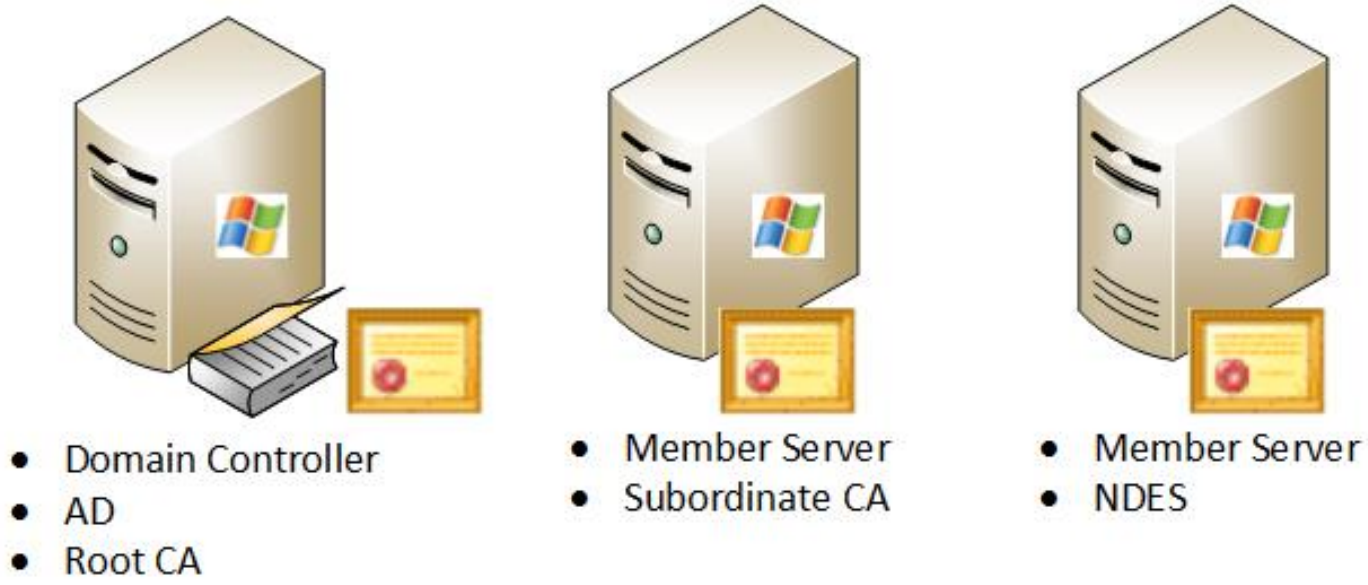
Déploiements distribués

Lorsque l'ISE est intégré dans un environnement de production Microsoft AD/PKI actuel, il est plus courant de voir des services distribués sur plusieurs serveurs Windows 2008 ou 2012 distincts. Cisco a testé deux scénarios pour les déploiements distribués.

Cette image illustre le premier scénario testé pour les déploiements distribués :



Cette image illustre le deuxième scénario testé pour les déploiements distribués :



Correctifs Microsoft importants

Avant de configurer la prise en charge SCEP pour le BYOD, assurez-vous que les correctifs Microsoft suivants sont installés sur le serveur NDES Windows 2008 R2 :

- La demande de renouvellement d'un certificat SCEP échoue dans Windows Server 2008 R2 si le certificat est géré à l'aide de NDES - Ce problème se produit car NDES ne prend pas en charge l'opération **GetCACaps**.

- NDES ne soumet pas de demandes de certificat après le redémarrage de l'autorité de certification d'entreprise dans Windows Server 2008 R2 - Ce message apparaît dans l'**Observateur d'événements** : "*Le service d'inscription de périphérique réseau ne peut pas soumettre la demande de certificat (0x800706ba). Le serveur RPC n'est pas disponible*. »

Avertissement : Lorsque vous configurez l'autorité de certification Microsoft, il est important de comprendre que l'ISE ne prend pas en charge l'algorithme de signature RSASSA-PSS. Cisco vous recommande de configurer la stratégie CA de sorte qu'elle utilise plutôt sha1WithRSAEncryption ou sha256WithRSAEncryption.

Ports et protocoles BYOD importants

Voici une liste des principaux ports et protocoles BYOD :

- TCP: Provisionnement 8909 : Assistant Installation à partir de Cisco ISE (systèmes d'exploitation Windows et Macintosh)
- TCP: 443 Provisioning : Assistant Installation à partir de Google Play (Android)
- TCP: Provisionnement 8905 : Processus d'approvisionnement du demandeur
- TCP: 80 ou TCP : 443 Proxy SCEP vers CA (basé sur la configuration de l'URL RA SCEP)

Note: Pour obtenir la dernière liste des ports et des protocoles requis, reportez-vous au Guide d'installation matérielle ISE 1.2.

Configuration

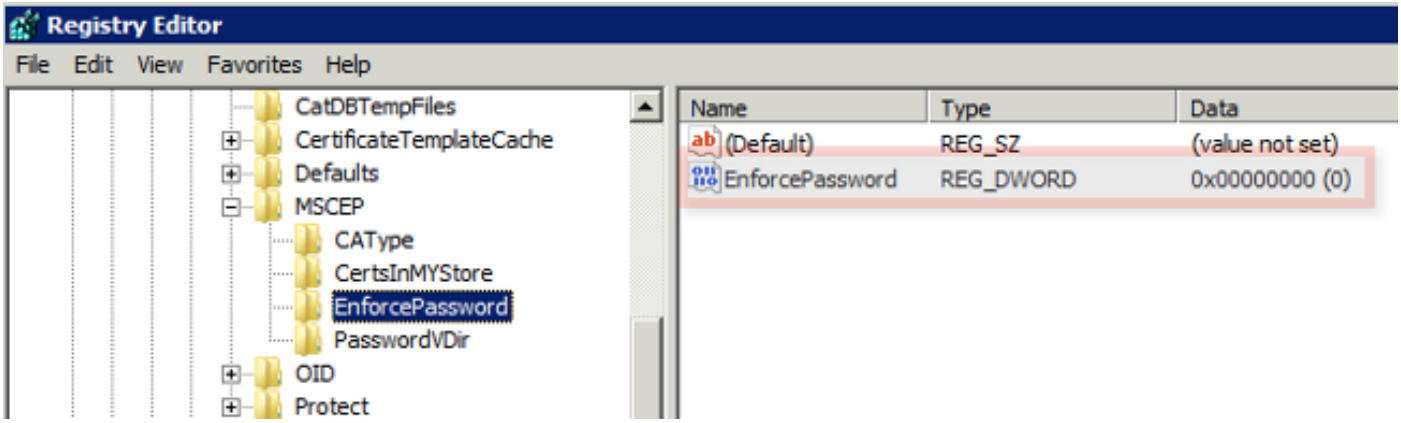
Utilisez cette section afin de configurer la prise en charge NDES et SCEP pour le BYOD sur ISE.

Désactiver la condition de mot de passe du défi d'inscription SCEP

Par défaut, la mise en oeuvre de Microsoft SCEP (MSCEP) utilise un mot de passe de confirmation dynamique afin d'authentifier les clients et les points de terminaison tout au long du processus d'inscription des certificats. Avec cette configuration requise en place, vous devez accéder à l'interface utilisateur graphique Web de l'administrateur MSCEP sur le serveur NDES afin de générer un mot de passe à la demande. Vous devez inclure ce mot de passe dans la demande d'enregistrement.

Dans un déploiement BYOD, l'exigence d'un mot de passe d'interrogation est contraire à l'objectif d'une solution en libre-service utilisateur. Pour supprimer cette condition, vous devez modifier cette clé de Registre sur le serveur NDES :

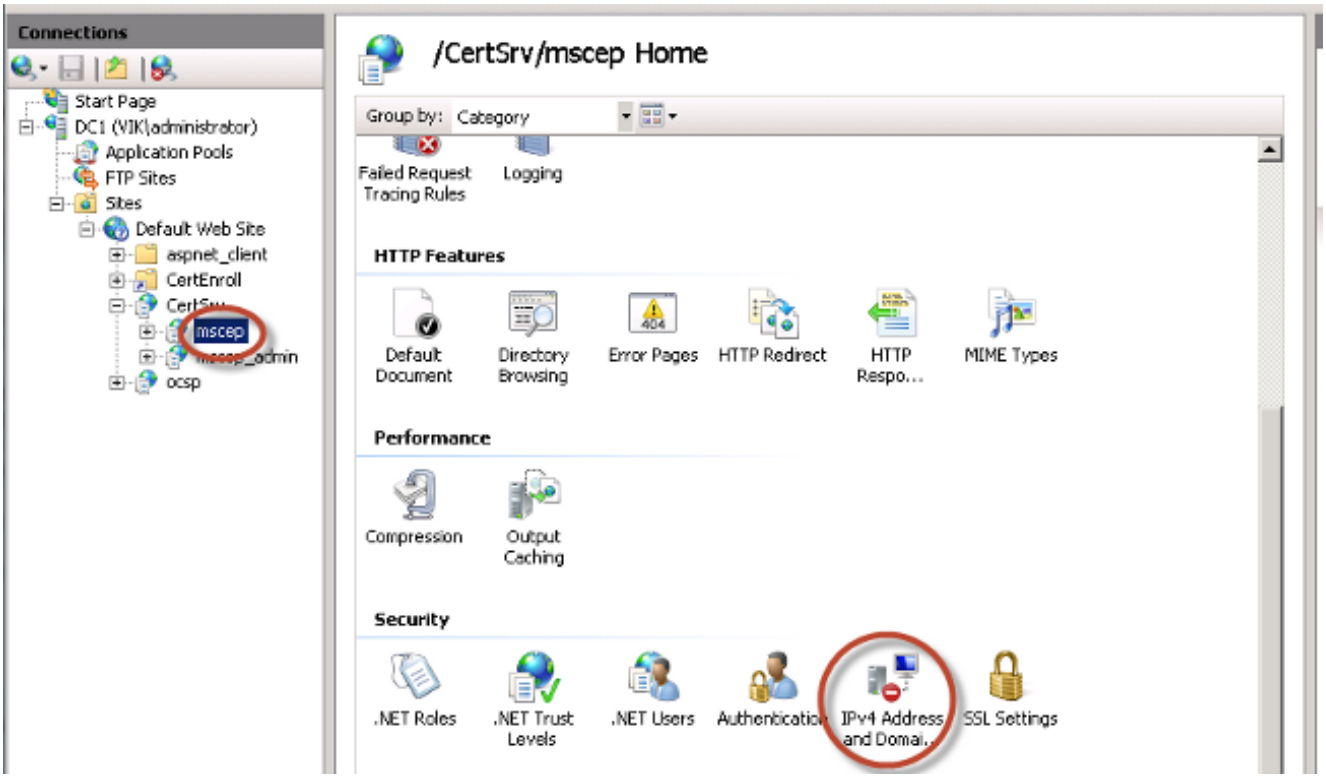
1. Cliquez sur **Démarrer** et saisissez **regedit** dans la barre de recherche.
2. Accédez à Ordinateur > HKEY_LOCAL_MACHINE > LOGICIEL > Microsoft > Cryptographie > **MSCEP** > **EnforcePassword**.
3. Assurez-vous que la valeur **EnforcePassword** est définie sur **0** (la valeur par défaut est **1**).



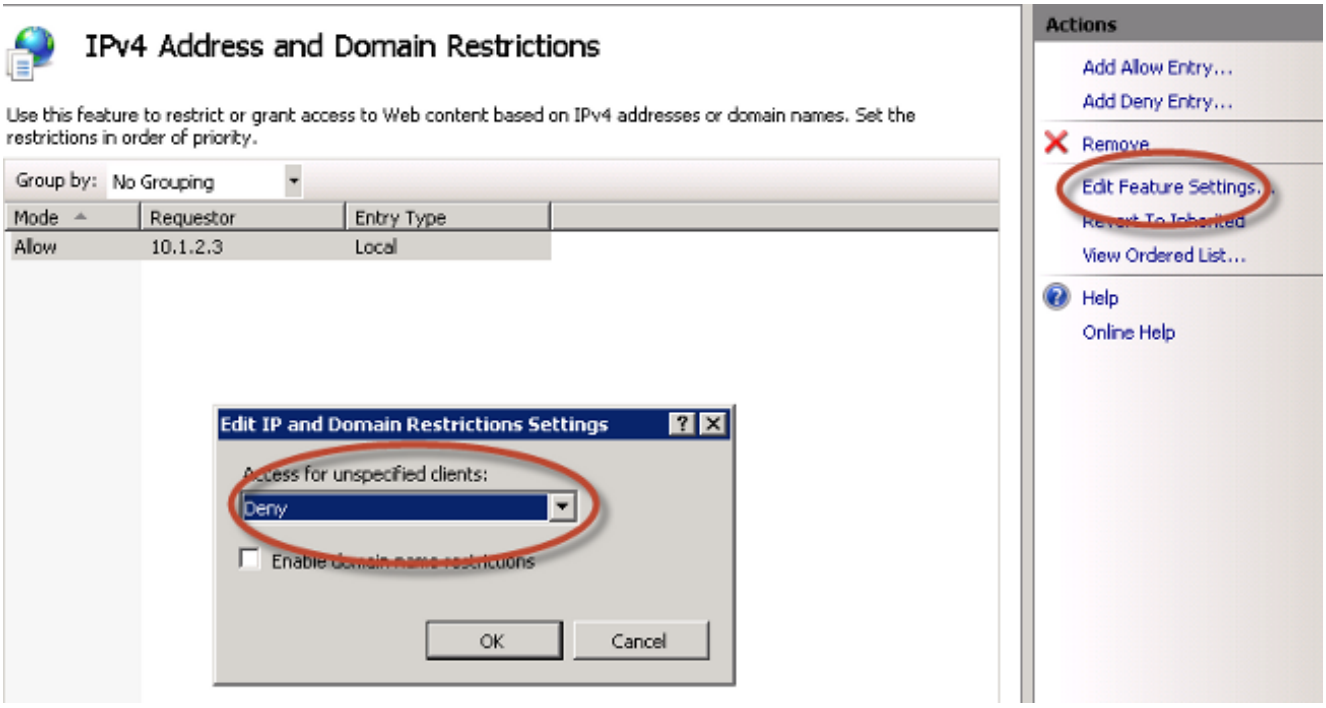
Limiter l'inscription SCEP aux noeuds ISE connus

Dans certains scénarios de déploiement, il peut être préférable de limiter les communications SCEP à une liste de noeuds ISE connus. Pour ce faire, vous pouvez utiliser la fonction IPv4 Address and Domain Restrictions dans IIS :

1. Ouvrez IIS et accédez au site Web **/CertSrv/mscep**.



2. Double-cliquez sur **Security > IPv4 Address and Domain Restrictions.** Utilisez les actions **Add Allow Entry** and **Add Deny Entry** afin d'autoriser ou de restreindre l'accès au contenu Web en fonction des adresses IPv4 ou des noms de domaine du noeud ISE. Utilisez l'action **Modifier les paramètres de fonction** afin de définir une règle d'accès par défaut pour les clients non spécifiés.

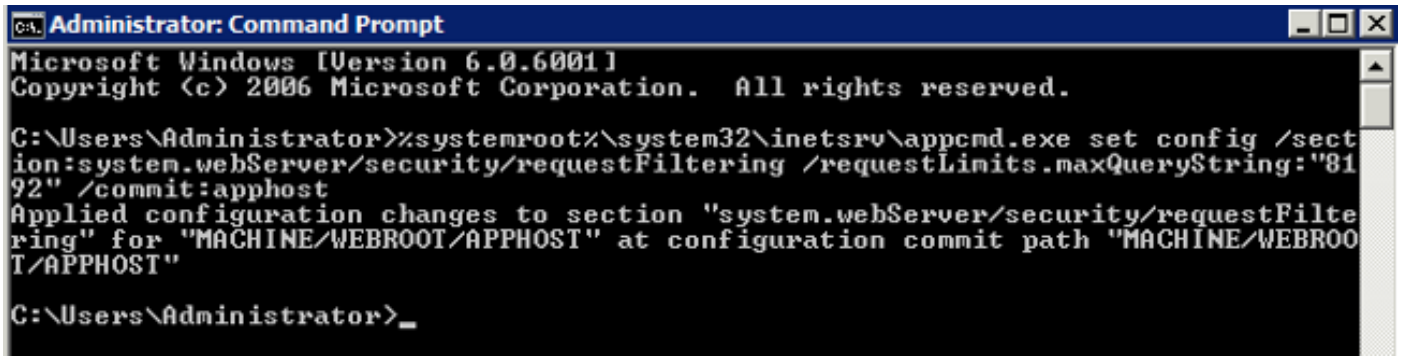


Étendre la longueur d'URL dans IIS

Il est possible pour ISE de générer des URL trop longues pour le serveur Web IIS. Afin d'éviter ce problème, la configuration IIS par défaut peut être modifiée pour autoriser des URL plus longues. Entrez cette commande à partir de l'interface de ligne de commande du serveur NDES :

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

> **Note**: La taille de la chaîne de requête peut varier en fonction de la configuration ISE et des points de terminaison. Entrez cette commande à partir de l'interface de ligne de commande du serveur NDES avec des privilèges d'administration.



Présentation du modèle de certificat

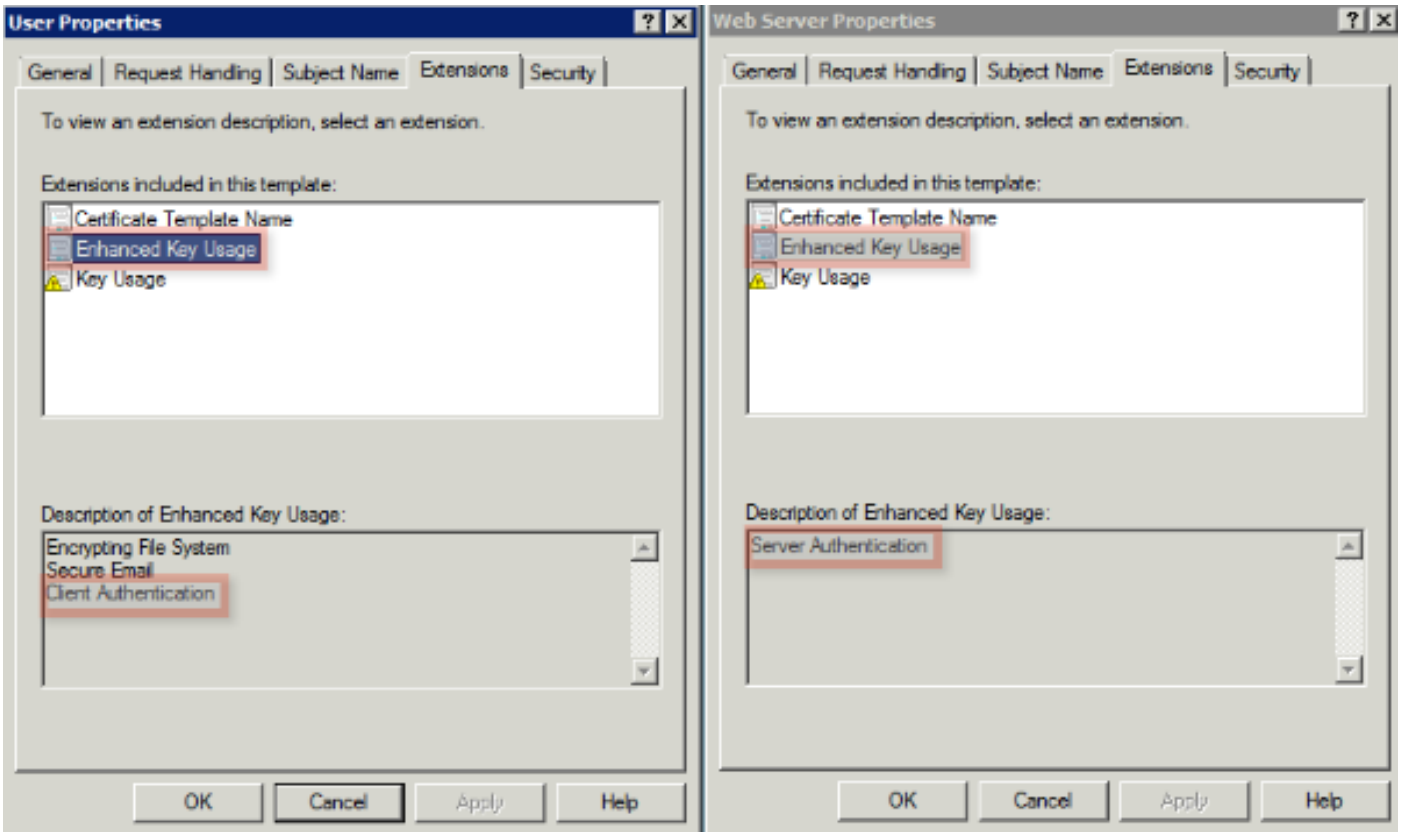
Les administrateurs d'une autorité de certification Microsoft peuvent configurer un ou plusieurs modèles utilisés afin d'appliquer des stratégies d'application à un ensemble commun de certificats. Ces stratégies permettent d'identifier pour quelle fonction le certificat et les clés associées sont utilisés. Les valeurs de stratégie d'application sont contenues dans le champ Utilisation de clé étendue (EKU) du certificat. L'authentificateur analyse les valeurs du champ EKU afin de s'assurer que le certificat présenté par le client peut être utilisé pour la fonction prévue. Parmi les utilisations les plus courantes figurent l'authentification du serveur, l'authentification du client, le VPN IPSec et

la messagerie électronique. En termes d'ISE, les valeurs EKU les plus couramment utilisées incluent l'authentification serveur et/ou client.

Lorsque vous accédez à un site Web de banque sécurisé, par exemple, le serveur Web qui traite la demande est configuré avec un certificat qui a une stratégie d'application d'authentification du serveur. Lorsque le serveur reçoit une demande HTTPS, il envoie un certificat d'authentification de serveur au navigateur Web de connexion pour authentification. L'important ici est qu'il s'agit d'un échange unidirectionnel entre le serveur et le client. En ce qui concerne ISE, l'accès à l'interface utilisateur graphique d'administration est une utilisation courante pour un certificat d'authentification de serveur. ISE envoie le certificat configuré au navigateur connecté et ne s'attend pas à recevoir de nouveau un certificat du client.

En ce qui concerne les services tels que le BYOD qui utilisent EAP-TLS, l'authentification mutuelle est préférable. Afin d'activer cet échange de certificats bidirectionnel, le modèle utilisé pour générer le certificat d'identité ISE doit posséder une stratégie d'application minimale d'authentification du serveur. Le modèle de certificat du serveur Web répond à cette condition. Le modèle de certificat qui génère les certificats de point de terminaison doit contenir une stratégie d'application minimale d'authentification client. Le modèle de certificat utilisateur satisfait à cette condition. Si vous configurez ISE pour des services tels que iPEP (Inline Policy Enforcement Point), le modèle utilisé pour générer le certificat d'identité de serveur ISE doit contenir des attributs d'authentification client et serveur si vous utilisez ISE version 1.1.x ou antérieure. Cela permet aux noeuds d'administration et en ligne de s'authentifier mutuellement. La validation EKU pour iPEP a été supprimée dans ISE version 1.2, ce qui rend cette exigence moins pertinente.

Vous pouvez réutiliser les modèles Microsoft CA Web Server et User par défaut, ou cloner et créer un nouveau modèle avec le processus décrit dans ce document. En fonction de ces exigences de certificat, la configuration de l'autorité de certification et les certificats ISE et terminaux résultants doivent être soigneusement planifiés afin de minimiser toute modification de configuration indésirable lors de son installation dans un environnement de production.



Configuration du modèle de certificat

Comme indiqué dans l'introduction, SCEP est largement utilisé dans les environnements VPN IPSec. Par conséquent, l'installation du rôle NDES configure automatiquement le serveur pour utiliser le modèle **IPSec (Offline Request)** pour SCEP. C'est pourquoi l'une des premières étapes de la préparation d'une autorité de certification Microsoft pour le BYOD consiste à créer un nouveau modèle avec la politique d'application appropriée. Dans un déploiement autonome, les services de l'autorité de certification et de NDES sont regroupés sur le même serveur et les modèles et les modifications de Registre requises sont contenus sur le même serveur. Dans un déploiement NDES distribué, les modifications du Registre sont effectuées sur le serveur NDES ; cependant, les modèles réels sont définis sur le serveur AC racine ou sous-racine spécifié dans l'installation du service NDES.

Complétez ces étapes afin de configurer le modèle de certificat :

1. Connectez-vous au serveur AC en tant qu'**administrateur**.

2. Cliquez sur **Démarrer > Outils d'administration > Autorité de certification**.

3. Développez les détails du serveur AC et sélectionnez le dossier **Modèles de certificat**. Ce dossier contient la liste des modèles actuellement activés.

4. Afin de gérer les modèles de certificat, cliquez avec le bouton droit sur le dossier **Modèles de certificat** et choisissez **Gérer**.

5. Dans la **console Modèles de certificat**, plusieurs modèles inactifs s'affichent.

6. Afin de configurer un nouveau modèle à utiliser avec SCEP, cliquez avec le bouton droit sur un modèle existant, tel que **Utilisateur**, et choisissez **Modèle dupliqué**.

7. Choisissez **Windows 2003** ou **Windows 2008**, en fonction du système d'exploitation CA minimum dans l'environnement.

8. Dans l'onglet **Général**, ajoutez un nom d'affichage, tel que ISE-BYOD, et la période de validité ; ne cochez pas toutes les autres options.
   Note: La période de validité du modèle doit être inférieure ou égale à la période de validité des certificats racine et intermédiaire de l'autorité de certification.
9. Cliquez sur l'onglet **Nom du sujet** et vérifiez que **l'approvisionnement dans la demande** est sélectionné.

10. Cliquez sur l'onglet **Conditions d'émission**. Cisco vous recommande de laisser les **stratégies d'émission** vides dans un environnement CA hiérarchique typique.

11. Cliquez sur l'onglet **Extensions**, **Stratégies d'application**, puis **Modifier**.

12. Cliquez sur **Ajouter**, et assurez-vous que **l'authentification du client** est ajoutée en tant que stratégie d'application. Click OK.

13. Cliquez sur l'onglet **Sécurité**, puis **Ajouter...**. Assurez-vous que le compte de service SCEP

défini dans l'installation du service NDES contrôle entièrement le modèle, puis cliquez sur **OK**.

14. Revenez à l'interface **GUI de l'autorité de certification**.

15. Cliquez avec le bouton droit de la souris sur le répertoire **Certificate Templates**. Accédez à **Nouveau > Modèle de certificat pour émettre**.

16. Sélectionnez le modèle **ISE-BYOD** configuré précédemment, puis cliquez sur **OK**.

    Note: Vous pouvez également activer le modèle via l'interface de ligne de commande à l'aide de la commande **certutil -SetCAtemplates +ISE-BYOD**.
    Le modèle ISE-BYOD doit maintenant être répertorié dans la liste des modèles de certificat activés.

Configuration du registre du modèle de certificat

Complétez ces étapes afin de configurer les clés de Registre du modèle de certificat :

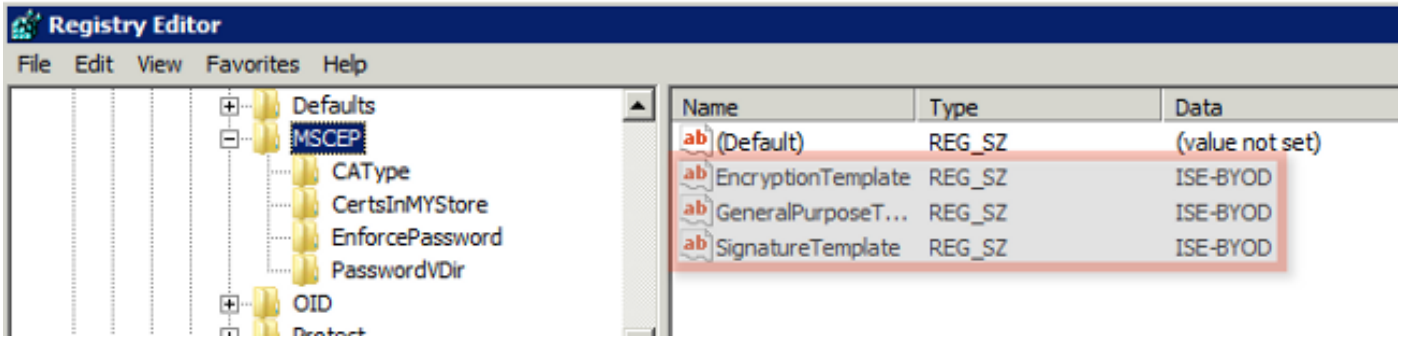
1. Connectez-vous au serveur NDES.

2. Cliquez sur **Démarrer** et saisissez **regedit** dans la barre de recherche.

3. Accédez à Ordinateur > HKEY_LOCAL_MACHINE > LOGICIEL > **Microsoft** > **Cryptographie** > **MSCEP**.

4. Modifiez les clés EncryptionTemplate, **GeneralPurposeTemplate** et **SignatureTemplate** de **IPSec (Offline Request)** au **modèle ISE-BYOD** précédemment créé.

5. Redémarrez le serveur NDES afin d'appliquer le paramètre de Registre.



Configurer ISE en tant que proxy SCEP

Dans un déploiement BYOD, le terminal ne communique pas directement avec le serveur NDES principal. Au lieu de cela, le noeud de stratégie ISE est configuré en tant que proxy SCEP et communique avec le serveur NDES au nom des points d'extrémité. Les terminaux communiquent directement avec l'ISE. L'instance IIS sur le serveur NDES peut être configurée afin de prendre en charge les liaisons HTTP et/ou HTTPS pour les répertoires virtuels SCEP.

Complétez ces étapes afin de configurer ISE en tant que proxy SCEP :

1. Connectez-vous à l'**interface utilisateur graphique ISE** avec les informations d'identification admin.

2. Cliquez sur **Administration**, **Certificats**, puis **Profils CA SCEP**.

3. Cliquez sur **Add**.

4. Saisissez le nom et la description du serveur.

5. Entrez l'URL du serveur SCEP avec l'IP ou le nom de domaine complet (FQDN) (http://10.10.10.10/certsrv/mscep/, par exemple).

6. Cliquez sur **Tester la connectivité**. Une connexion réussie génère un message contextuel de réponse du serveur.

7. Cliquez sur **Enregistrer** afin d'appliquer la configuration.

8. Afin de vérifier, cliquez sur **Administration**, **Certificates**, **Certificate Store,** et confirmez que le certificat d'accès au serveur NDES SCEP a été automatiquement téléchargé sur le noeud ISE.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Utilisez cette section afin de dépanner votre configuration.

Notes générales de dépannage

Voici une liste de remarques importantes que vous pouvez utiliser afin de dépanner votre configuration :

- Décomposer la topologie du réseau BYOD en points de cheminement logiques afin d'identifier les points de débogage et de capture le long du chemin entre les terminaux ISE, NDES et CA.
- Assurez-vous que le noeud ISE et l'autorité de certification partagent une source temporelle NTP (Network Time Protocol) commune.
- Les points de terminaison doivent être en mesure de définir automatiquement leur heure à l'aide des options NTP et de fuseau horaire apprises de DHCP.
- Le serveur DNS du client doit être en mesure de résoudre le nom de domaine complet du noeud ISE.
- Assurez-vous que TCP 80 et/ou TCP 443 sont autorisés bidirectionnellement entre ISE et le

serveur NDES.

- Testez avec un ordinateur Windows en raison de l'amélioration de la journalisation côté client. Vous pouvez éventuellement utiliser un iDevice Apple avec l'utilitaire de configuration de l'iPhone Apple afin de surveiller les journaux de console côté client.

- Surveillez les journaux des applications du serveur AC et NDES pour détecter les erreurs d'enregistrement, et utilisez Google ou TechNet pour rechercher ces erreurs.

- Tout au long de la phase de test, utilisez HTTP pour SCEP afin de faciliter la capture de paquets entre ISE, NDES et CA.

- Utilisez l'utilitaire TCP Dump sur le noeud de service de stratégie ISE (PSN) et surveillez le trafic à destination et en provenance du serveur NDES. Il se trouve sous **Opérations > Outils de diagnostic > Outils généraux**.

- Installez Wireshark sur le serveur CA et NDES, ou utilisez SPAN sur les commutateurs intermédiaires, afin de capturer le trafic SCEP à destination et en provenance du PSN ISE.

- Assurez-vous que la chaîne de certificats CA appropriée est installée sur le noeud de stratégie ISE pour l'authentification des certificats clients.

- Assurez-vous que la chaîne de certificats CA appropriée est automatiquement installée sur les clients lors de l'intégration.

- Affichez un aperçu des certificats d'identité ISE et de point de terminaison et vérifiez que les attributs EKU corrects sont présents.

- Surveillez les journaux d'authentification en direct dans l'interface utilisateur graphique ISE pour détecter les échecs d'authentification et d'autorisation.
  Note: Certains demandeurs n'initialisent pas un échange de certificat client si l'EKU erroné est présent, par exemple un certificat client avec l'EKU de l'authentification du serveur. Par conséquent, les échecs d'authentification peuvent ne pas toujours être présents dans les journaux ISE.
- Lorsque NDES est installé dans un déploiement distribué, une autorité de certification racine ou sous-racine distante est désignée par le nom de l'autorité de certification ou le nom de l'ordinateur dans l'installation du service. Le serveur NDES envoie des demandes d'enregistrement de certificat à ce serveur AC cible. Si le processus d'enregistrement du certificat de point de terminaison échoue, les captures de paquets (PCAP) peuvent indiquer que le serveur NDES renvoie une erreur **404 Not Found** au noeud ISE. Afin de résoudre ce problème, réinstallez le service NDES et sélectionnez l'option Nom de l'ordinateur au lieu du nom de l'autorité de certification.

- Évitez les modifications apportées à la chaîne CA SCEP après l'intégration des périphériques. Les systèmes d'exploitation de terminaux, tels qu'Apple iOS, ne mettent pas automatiquement à jour un profil BYOD précédemment installé. Dans cet exemple d'iOS, le profil actuel doit être supprimé du point de terminaison et le point de terminaison supprimé de la base de données ISE, afin que l'intégration puisse être effectuée à nouveau.

- Vous pouvez configurer un serveur de certificats Microsoft afin de vous connecter à Internet et mettre à jour automatiquement les certificats à partir du programme de certificats racine Microsoft. Si vous configurez cette option de récupération de réseau dans des environnements avec des stratégies Internet restreintes, les serveurs CA/NDES qui ne peuvent pas se connecter à Internet peuvent prendre 15 secondes à expiration par défaut. Cela peut ajouter un délai de 15 secondes au traitement des demandes SCEP à partir de proxys SCEP tels que ISE. ISE est programmé afin de temporiser les demandes SCEP après 12 secondes si aucune réponse n'est reçue. Afin de résoudre ce problème, autorisez l'accès Internet pour les serveurs CA/NDES ou modifiez les paramètres de délai d'expiration de récupération réseau dans la stratégie de sécurité locale des serveurs CA/NDES Microsoft. Afin de localiser cette configuration sur le serveur Microsoft, accédez à **Démarrer > Outils d'administration > Stratégie de sécurité locale > Stratégies de clé publique > Paramètres de validation du chemin d'accès du certificat > Récupération du réseau**.

Journalisation côté client

Voici une liste des techniques utiles utilisées pour résoudre les problèmes de journalisation côté client :

- Entrez le **journal %temp%\spwProfileLog.txt.** afin d'afficher les journaux côté client pour les applications Microsoft Windows.
  Note: WinHTTP est utilisé pour la connexion entre le point de terminaison Microsoft Windows et ISE. Reportez-vous à l'article Messages d'erreur Microsoft Windows pour obtenir une liste de codes d'erreur.
- Entrez la commande **/sdcards/downloads/spw.log** afin d'afficher les journaux côté client des applications Android.

- Pour **MAC OSX**, utilisez l'application Console et recherchez le processus **SPW**.

- Pour **Apple iOS**, utilisez Apple Configurator 2.0 pour afficher les messages.

Journalisation ISE

Complétez ces étapes afin d'afficher le journal ISE :

1. Accédez à **Administration > Logging > Debug Log Configuration**, puis sélectionnez le noeud de stratégie ISE approprié.

2. Définissez les journaux **client** et **approvisionnement** sur debug ou trace, selon les besoins.

3. Reproduisez le problème et documentez les informations de démarrage pertinentes afin de faciliter la recherche, telles que MAC, IP et utilisateur.

4. Accédez à **Operations > Download Logs**, puis sélectionnez le noeud ISE approprié.

5. Sous l'onglet **Journaux de débogage**, téléchargez les journaux nommés **ise-psc.log** sur le bureau.

6. Utilisez un éditeur intelligent, tel que Bloc-notes ++ pour analyser les fichiers journaux.

7. Une fois le problème isolé, retournez les niveaux de journal au niveau par défaut.

Journalisation et dépannage NDES

Pour plus d'informations, référez-vous à AD CS : Dépannage de l'article Windows Server du service d'inscription de périphérique réseau.

Informations connexes

- Guide de solutions BYOD - Configuration du serveur d'autorité de certification
- Présentation de NDES sous Windows 2008 R2
- Livre blanc MSCEP
- Configuration du serveur NDES pour prendre en charge SSL
- Exigences de certificat lorsque vous utilisez EAP-TLS ou PEAP avec EAP-TLS
- Documentation et assistance techniques