Configurez le soutien ISE SCEP de BYOD

Contenu

Introduction

Ce document décrit les étapes qui sont utilisées afin de configurer avec succès le service d'inscription de périphérique de réseau Microsoft (NDES) et l'inscription de certificat simple Protocol (SCEP) pour Bring Your Own Device (BYOD) sur Cisco identifient l'engine de services (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version 1.1.1 ISE ou plus tard

- Microsoft Windows Server 2008 R2
- Norme de la Microsoft Windows Server 2012
- Infrastructure à clés publiques (PKI) et Certificats

Composants utilisés

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

- Version 1.1.1 ISE ou plus tard
- Windows Server 2008 R2 SP1 avec les correctifs KB2483564 et KB2633200 installés
- Norme des Windows Server 2012

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Le relatif à l'information aux services de certificat de Microsoft est donné comme guide spécifiquement pour Cisco BYOD. Référez-vous au TechNet de Microsoft comme source définitive de vérité pour l'autorité de certification de Microsoft, le service d'inscription de périphérique de réseau (NDES), et les configurations du serveur liées SCEP.

Informations générales

Un des avantages de l'implémentation BYOD ISE-activée par Cisco est la capacité des utilisateurs finaux d'exécuter l'enregistrement de périphérique de libre-service. Ceci élimine la charge administrative sur le service informatique afin de distribuer des qualifications d'authentification et des périphériques d'enable sur le réseau. Au coeur de BYOD la solution est le processus d'approvisionnement de suppliant de réseau, qui recherche à distribuer les Certificats requis aux périphériques appartenants aux employés. Afin de répondre à cette exigence, un Microsoft Certificate Authority (CA) peut être configuré afin d'automatiser le procédé d'inscription de certificat avec le SCEP.

SCEP a été utilisé pendant des années dans des environnements du réseau privé virtuel (VPN) afin de faciliter l'inscription de certificat et la distribution aux clients et aux Routeurs d'Accès à distance. L'activation de la fonctionnalité SCEP sur un serveur R2 de Windows 2008 exige l'installation du NDES. Pendant l'installation de rôle NDES, le web server de l'Internet Information Services de Microsoft (IIS) est également installé. IIS est utilisé afin de terminer le HTTP ou les demandes d'enregistrement et les réponses HTTPS SCEP noeud entre CA et ISE stratégie.

Le rôle NDES peut être installé sur un courant CA, ou il peut être installé sur un serveur membre. Dans un déploiement autonome, le service NDES est installé sur un CA existant qui inclut le service d'autorité de certification et, sur option, le service d'inscription de Web d'autorité de certification. Dans un déploiement distribué, le service NDES est installé sur un serveur membre. Le serveur distribué NDES est alors configuré afin de communiquer avec une racine ou une sous-titre-racine en amont CA. Dans ce scénario, les modifications de registre tracées les grandes lignes dans ce document sont apportées sur le serveur NDES avec le modèle personnalisé, où les Certificats résident sur l'en amont CA.

Scénarios testés de déploiement CA/NDES

Cette section fournit une brève présentation des scénarios de déploiement CA/NDES qui ont été testés dans le TP Cisco. Référez-vous au TechNet de Microsoft comme source définitive de vérité pour Microsoft CA, NDES, et configurations du serveur liées SCEP.

Déploiements autonomes

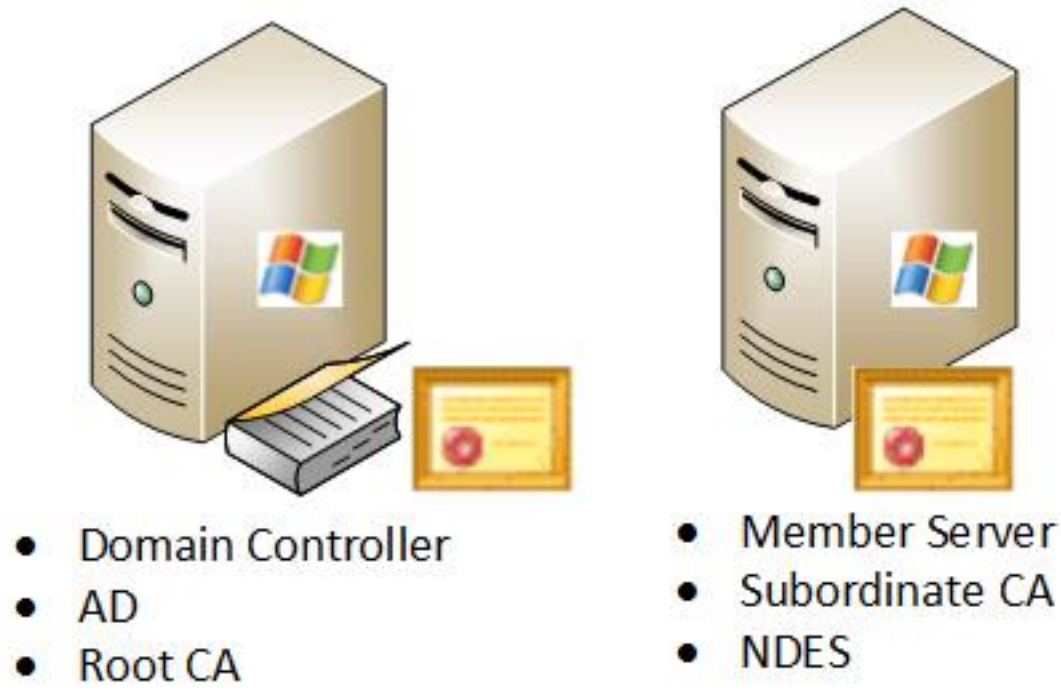
Quand ISE est utilisé dans une validation de principe le scénario (POC), il est commun pour déployer Windows d'un seul bloc 2008 ou 2012 usinent qu'agit en tant que contrôleur de domaine de Répertoire actif (AD), enracinent le serveur CA, et NDES :

- Domain Controller
- AD
- Root CA
- NDES

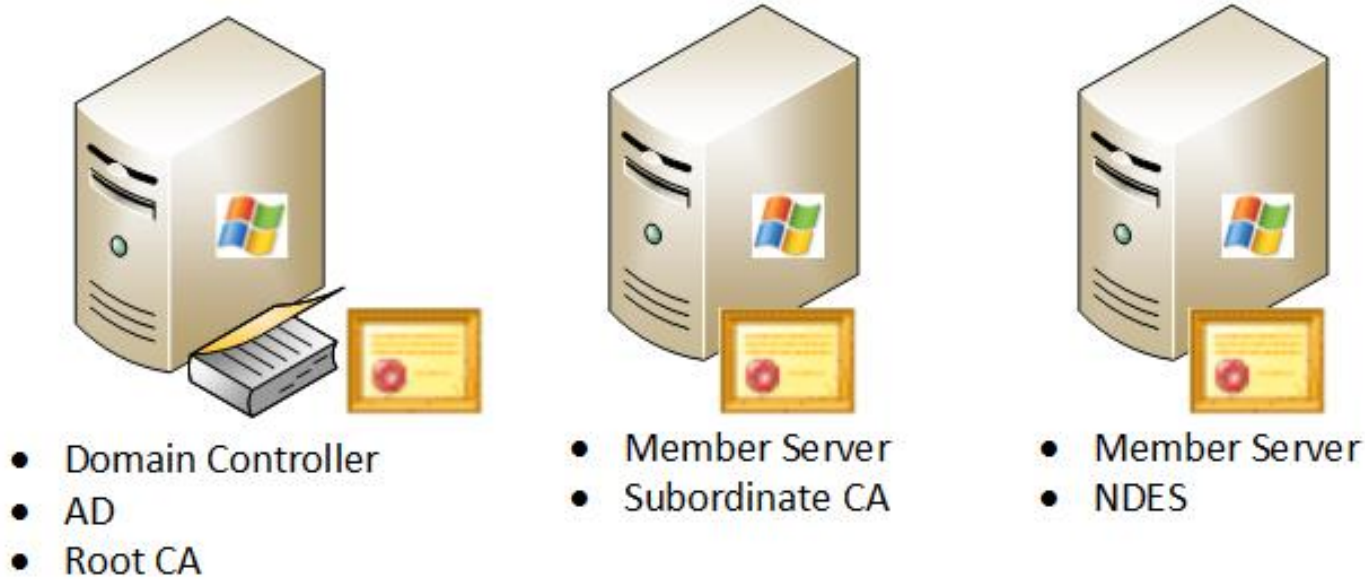
Déploiements distribués

Quand l'ISE est intégré dans un environnement de production en cours de Microsoft AD/PKI, il est plus commun pour voir des services distribués à travers le multiple, les serveurs distincts de Windows 2008 ou 2012. Cisco a testé deux scénarios pour des déploiements distribués.

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



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



Importants correctifs de Microsoft

Avant que vous configuriez le soutien SCEP de BYOD, assurez-vous que le serveur de Windows 2008 R2 NDES fait installer ces correctifs de Microsoft :

- La demande de renouvellement d'un certificat SCEP échoue dans les Windows Server 2008 R2 si le certificat est géré à l'aide de NDES - cette question se produit parce que NDES ne prend en charge pas l'exécution de **GetCACaps**.

- NDES ne soumet pas des demandes de certificat après que l'entreprise CA soit redémarrée dans les Windows Server 2008 R2 - ce message apparaît en cas **visualiseur** : « Le *service d'inscription de périphérique de réseau ne peut pas soumettre la demande de certificat (0x800706ba). Le serveur RPC est indisponible.* »

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

Importants ports et protocoles BYOD

Voici une liste d'importants ports et de protocoles BYOD :

- TCP : Ravitaillement 8909 : L'assistant installent de Cisco ISE (Windows et systèmes d'exploitation Mac (le SYSTÈME D'EXPLOITATION))
- TCP : Ravitaillement 443 : L'assistant installent de Google Play (Android)
- TCP : Ravitaillement 8905 : Processus d'approvisionnement de suppliant
- TCP : 80 ou TCP : Proxy 443 SCEP au CA (basé sur la configuration URL de RA SCEP)

  Remarque: Pour la dernière liste de ports requis et de protocoles, référez-vous au guide d'installation du matériel ISE 1.2.

Configurez

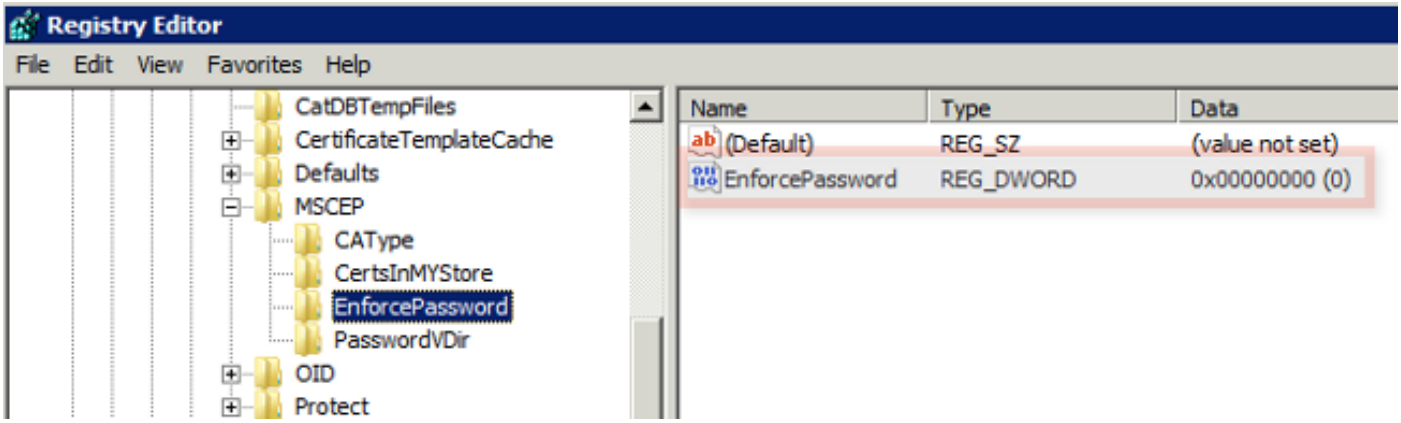
Employez cette section afin de configurer le soutien NDES et SCEP de BYOD sur l'ISE.

Condition requise de mot de passe de défi d'inscription du débronchement SCEP

Par défaut, l'implémentation de Microsoft SCEP (MSCEP) emploie un mot de passe de défi dynamique afin d'authentifier des clients et des points finaux dans tout le procédé d'inscription de certificat. Avec cette configuration requise en place, vous devez parcourir au GUI de Web d'admin MSCEP sur le serveur NDES afin de générer un à la demande de mot de passe. Vous devez inclure ce mot de passe en tant qu'élément de la demande d'enregistrement.

Dans un déploiement BYOD, la condition requise d'un mot de passe de défi défait le but d'une solution de libre-service d'utilisateur. Afin de retirer cette condition requise, vous devez modifier cette clé de registre sur le serveur NDES :

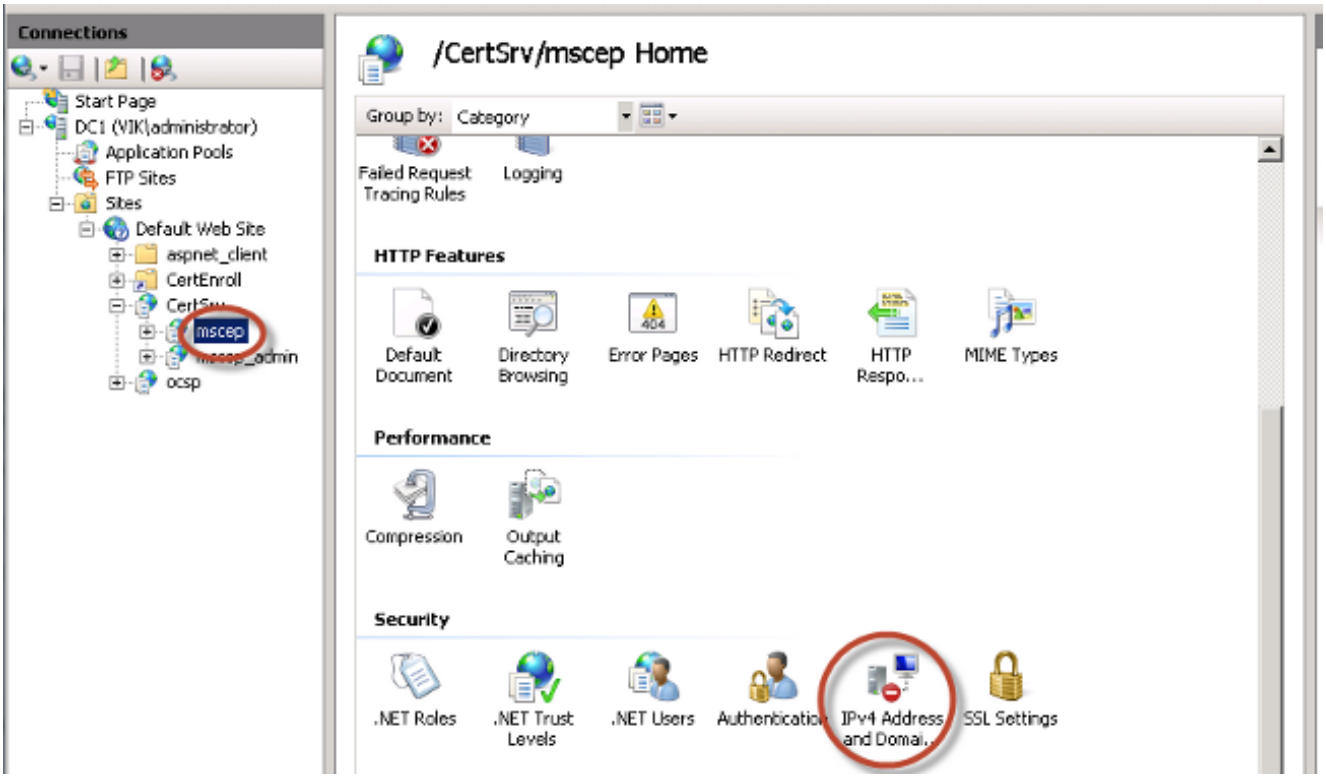
1. Cliquez sur le **début** et écrivez le **regedit** dans la barre de recherche.
2. Naviguez vers l'**ordinateur** > le **HKEY_LOCAL_MACHINE** > le **LOGICIEL** > le **Microsoft** > le **chiffrement** > le **MSCEP** > l'**EnforcePassword**.
3. Assurez-vous que la valeur d'**EnforcePassword** est placée à **0** (la valeur par défaut est **1)**.



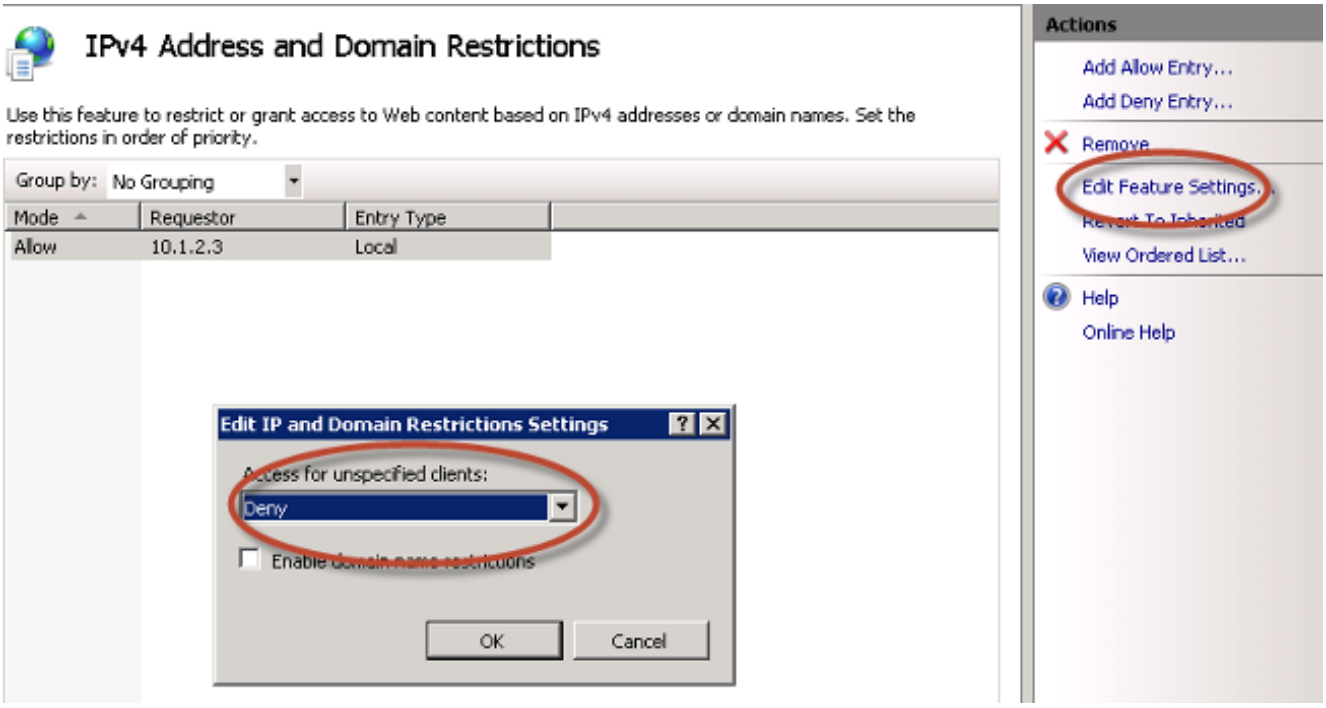
Limitez l'inscription SCEP aux Noeuds connus ISE

Dans quelques scénarios de déploiement, il pourrait préférer limiter des transmissions SCEP à une liste choisie de Noeuds connus ISE. Ceci peut être accompli avec l'ipv4 addres et la configuration de restrictions de domaine dans IIS :

1. Ouvrez IIS et naviguez vers le site Web de **/CertSrv/mscep**.



2. Double-cliquer la **Sécurité > l'ipv4 addres et les restrictions de domaine.** Utilisez l'**ajouter permettent l'entrée** et **ajoutent refusent des** actions d'**entrée** afin de permettre ou limiter l'accès au contenu Web basé sur des adresses ou des noms de domaine d'ipv4 de noeud ISE. Employez l'action de **paramètres de fonctions d'éditer** afin de définir une règle d'accès par défaut pour les clients non spécifiés.

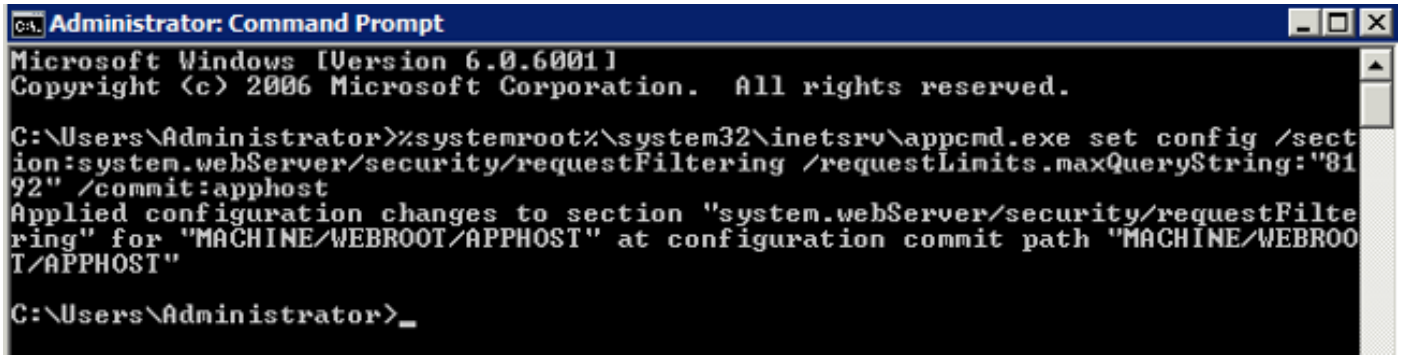


Étendez la longueur URL dans IIS

Il est possible que ISE génèrent l'URLs qui sont trop longs pour le web server IIS. Afin d'éviter ce problème, la configuration du par défaut IIS peut être modifiée pour tenir compte d'un plus long URLs. Sélectionnez cette commande du serveur CLI NDES :

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

> Remarque: La taille de chaîne de requête pourrait varier la personne à charge sur la configuration ISE et de point final. Sélectionnez cette commande du serveur CLI NDES avec des privilèges d'administrateur.



Aperçu de modèle de certificat

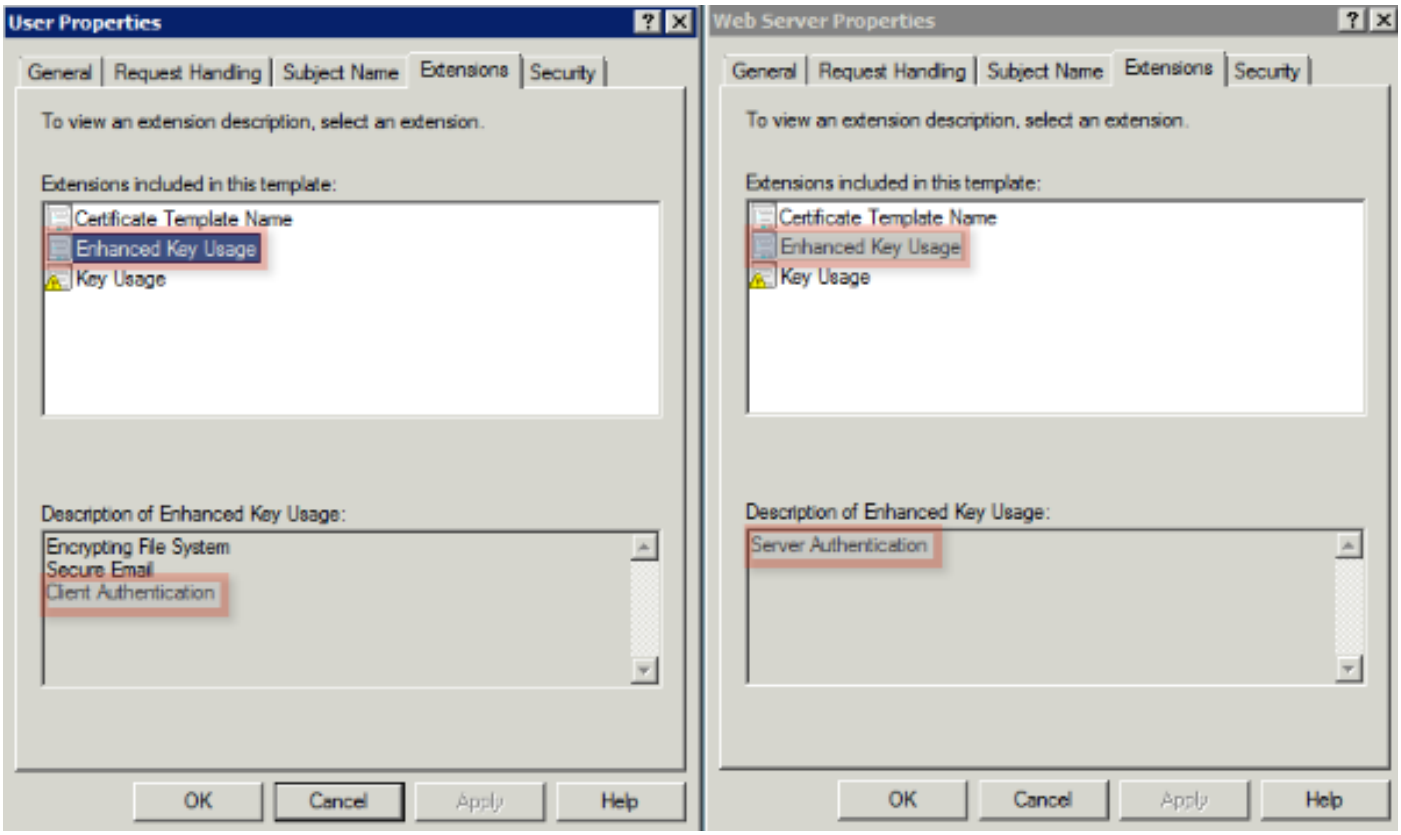
Les administrateurs de Microsoft CA peuvent configurer un ou plusieurs modèles qui sont utilisés afin de s'appliquer des stratégies d'application à un ensemble commun de Certificats. Ces stratégies aident aux identifier pour quelle fonction le certificat et les clés associées sont utilisé. Les valeurs de stratégie d'application sont contenues dans le domaine étendu de l'utilisation principale (EKU) du certificat. L'authentificateur analyse les valeurs dans le domaine EKU afin de s'assurer que le certificat présenté par le client peut être utilisé pour la fonction destinée. Certaines des utilisations plus communes incluent l'authentification de serveur, l'authentification client, l'IPSec VPN, et l'email. En termes d'ISE, les valeurs généralement utilisées EKU incluent le

serveur et/ou l'authentification client.

Quand vous parcourez à un site Web sécurisé de banque, par exemple, le web server qui traite la demande est configuré avec un certificat qui a une stratégie d'application de l'authentification de serveur. Quand le serveur reçoit une demande HTTPS, elle envoie un certificat d'authentification de serveur au navigateur Web se connectant pour l'authentification. Le point important ici est que c'est un échange unidirectionnel du serveur au client. Car il associe à ISE, un d'usage courant pour un certificat d'authentification de serveur est accès GUI d'admin. ISE envoie le certificat configuré au navigateur connecté et ne le compte pas recevoir un certificat de retour du client.

Quand il s'agit de services tels que BYOD qui utilisent l'EAP-TLS, l'authentification mutuelle est préférée. Afin d'activer cet échange bidirectionnel de certificat, le modèle utilisé afin de générer le certificat d'identité ISE doit posséder une stratégie minimum d'application de l'authentification de serveur. Le modèle de certificat de serveur Web répond à cette exigence. Le modèle de certificat qui génère les Certificats de point final doit contenir une stratégie minimum d'application de l'authentification client. Le modèle de certificat utilisateur répond à cette exigence. Si vous configurez ISE pour des services tels que le point intégré d'application de stratégie (iPEP), le modèle utilisé afin de générer le certificat d'identité de serveur ISE devrait contenir des attributs d'authentification de client et de serveur si vous utilisez la version 1.1.x ou antérieures ISE. Ceci permet aux Noeuds d'admin et d'en ligne pour s'authentifier mutuellement. La validation EKU pour l'iPEP a été retirée dans la version 1.2 ISE, qui prévoit cette exigence moins appropriée.

Vous pouvez réutiliser le serveur Web et les grilles utilisateur par défaut de Microsoft CA, ou vous pouvez copier et créer un nouveau modèle avec le processus qui est tracé les grandes lignes dans ce document. Basé sur ces conditions requises de certificat, la configuration CA et l'ISE résultant et des Certificats de point final devraient être soigneusement prévus afin de réduire tous les changements de configuration non désirés une fois installés d'un environnement de production.



Configuration de modèle de certificat

Comme observé dans l'introduction, SCEP est très utilisé dans des environnements d'IPSec VPN. En conséquence, l'installation du rôle NDES configure automatiquement le serveur pour utiliser le modèle d'**IPSec (demande hors ligne)** pour SCEP. Pour cette raison, une des premières étapes dans la préparation de Microsoft CA pour BYOD est d'établir un nouveau modèle avec la stratégie d'application appropriée. Dans un déploiement autonome, l'autorité de certification et des services NDES sont colloqués sur le même serveur, et les modèles et les modifications exigées de registre sont contenus au même serveur. Dans un déploiement distribué NDES, les modifications de registre sont apportées sur le serveur NDES ; cependant, les modèles réels sont définis sur le serveur de racine ou de sous-titre-racine CA spécifié à l'installation de service NDES.

Terminez-vous ces étapes afin de configurer le modèle de certificat :

1. Login au serveur CA comme **admin**.

2. **Début de** clic > **outils d'administration** > **autorité de certification**.

3. Développez les petits groupes de serveur CA et sélectionnez le répertoire de **modèles de certificat**. Ce répertoire contient une liste des modèles qui sont actuellement activés.

4. Afin de gérer les modèles de certificat, le clic droit sur le répertoire de **modèles de certificat** et choisir **gèrent**.

5. Dans la **console de modèles de certificat**, un certain nombre de modèles inactifs sont affichés.

6. Afin de configurer un nouveau modèle pour l'usage avec SCEP, clic droit sur un modèle qui existe déjà, comme l'**utilisateur**, et choisit le **modèle en double**.

7. Choisissez **Windows 2003** ou **Windows 2008**, dépendant sur le SYSTÈME D'EXPLOITATION du minimum CA dans l'environnement.

8. Sur l'**onglet Général**, ajoutez un nom d'affichage, tel qu'ISE-BYOD, et la période de validité ; laissez toutes autres options décochées.
   Remarque: La période de validité de modèle doit être inférieur ou égal à la période de validité des Certificats de racine et d'intermédiaire CA.
9. Cliquez sur en fonction l'onglet de **nom du sujet**, et confirmez cet **approvisionnement dans la demande** est sélectionné.

10. Cliquez sur en fonction les **conditions requises d'émission que** tableau Cisco recommande que vous laissiez le blanc de **stratégies d'émission** dans un environnement hiérarchique typique CA.

11. Cliquez sur en fonction l'onglet d'**extensions**, des **stratégies d'application**, et **l'éditez** alors.

12. Cliquez sur Add, et assurez-vous que l'**authentification client** est ajoutée comme stratégie d'application. Cliquez sur **OK**.

13. Cliquez sur en fonction l'**onglet Sécurité**, et **ajoutez** alors**….** Assurez-vous que le compte des services SCEP défini à l'installation de service NDES a le plein contrôle du modèle, et

puis cliquez sur OK.

14. Revenez à l'**interface gui d'autorité de certification**.

15. Clic droit sur le répertoire de **modèles de certificat**. Naviguez vers **nouveau > modèle de certificat à émettre**.

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

    Remarque: Alternativement, vous pouvez activer le modèle par l'intermédiaire du CLI avec le **certutil -** commande de **SetCAtemplates +ISE-BYOD**.
    Le modèle ISE-BYOD devrait maintenant être répertorié dans la liste activée de modèle de certificat.

Configuration de registre de modèle de certificat

Terminez-vous ces étapes afin de configurer les clés de registre de modèle de certificat :

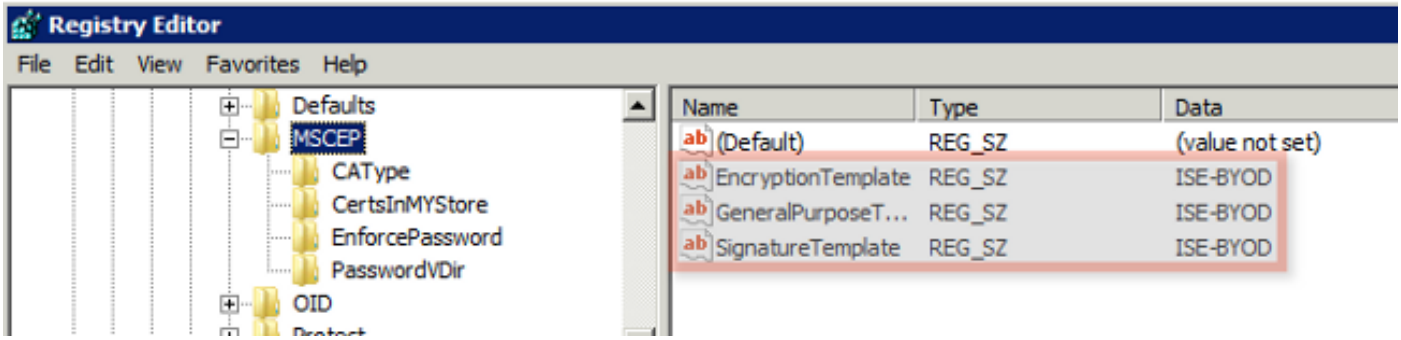
1. Connectez au serveur NDES.

2. Cliquez sur le **début** et écrivez le **regedit** dans la barre de recherche.

3. Naviguez vers l'**ordinateur** > le **HKEY_LOCAL_MACHINE** > le **LOGICIEL** > le **Microsoft** > le **chiffrement** > le **MSCEP**.

4. Changez les clés d'**EncryptionTemplate**, de **GeneralPurposeTemplate**, et de **SignatureTemplate d'IPSec (demande hors ligne) au** modèle **ISE-BYOD** précédemment créé.

5. Redémarrez le serveur NDES afin d'appliquer les paramètres de registre.



Configurez ISE comme proxy SCEP

Dans un déploiement BYOD, le point final ne communique pas directement avec le serveur du backend NDES. Au lieu de cela, le noeud de stratégie ISE est configuré comme proxy SCEP et communique avec le serveur NDES au nom des points finaux. Les points finaux communiquent directement avec l'ISE. L'exemple IIS sur le serveur NDES peut être configuré afin de prendre en charge des attaches de HTTP et/ou HTTPS pour les répertoires virtuels SCEP.

Terminez-vous ces étapes afin de configurer ISE comme proxy SCEP :

1. Connectez-vous dans le **GUI ISE** avec des qualifications d'admin.
2. Cliquez sur la **gestion**, les **Certificats**, et puis les **profils SCEP CA**.
3. Cliquez sur **Add**.
4. Écrivez le nom du serveur et la description.
5. Écrivez l'URL pour le serveur SCEP avec l'IP ou le nom de domaine complet (FQDN) (http://10.10.10.10/certsrv/mscep/, par exemple).
6. **Connectivité de test de** clic. Une connexion réussie a comme conséquence un message réussi de popup de réponse de serveur.
7. **Sauvegarde de** clic afin d'appliquer la configuration.
8. Afin de vérifier, cliquer sur la **gestion**, les **Certificats**, **délivrent un certificat la mémoire,** et la confirment que le certificat de RA de serveur SCEP NDES a été automatiquement téléchargé au noeud ISE.

Vérifiez

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

Dépannez

Utilisez cette section afin de dépanner votre configuration.

Général dépannez les notes

Voici une liste des informations importantes que vous pouvez employer afin de dépanner votre configuration :

- Décomposez la topologie du réseau BYOD en buts logiques afin d'aider à l'identifier mettent au point et capturent des points le long du chemin entre les points finaux ISE, NDES, et CA.
- Assurez-vous que le noeud ISE et le CA partagent une source temporelle commune de Protocole NTP (Network Time Protocol).
- Les points finaux devraient pouvoir placer leur heure automatiquement avec le NTP et les options de fuseau horaire appris du DHCP.
- Le serveur DNS du client doit pouvoir résoudre le FQDN du noeud ISE.
- Assurez-vous qu'on permet bidirectionnel le TCP 80 et/ou le TCP 443 entre ISE et le serveur NDES.

- Testez avec un ordinateur Windows en raison de se connecter amélioré de côté client. Sur option, employez un iDevice d'Apple avec l'utilitaire de configuration d'iPhone d'Apple afin de surveiller des logs de console de côté client.

- Des logs surveillez CA et NDES serveur d'application pour des erreurs d'enregistrement, et employez Google ou le TechNet afin de rechercher ces erreurs.

- Dans toute la phase de test, le HTTP d'utilisation pour SCEP afin de faciliter des captures de paquet entre ISE, le NDES, et le CA.

- Utilisez l'utilitaire de vidage mémoire de TCP sur le noeud de service de stratégie ISE (le RPC), et surveillez le trafic à et du serveur NDES. Ceci se trouve sous des **exécutions >** des **outils de diagnostic >** les **outils généraux**.

- Installez Wireshark sur le serveur CA et NDES, ou employez l'ENVERGURE sur les Commutateurs intermédiaires, afin de capturer le trafic SCEP à et du RPC ISE.

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

- Assurez-vous que la chaîne appropriée de certificat de CA est automatiquement installée sur les clients pendant onboarding.

- Visionnez les certificats d'identité ISE et de point final et les confirmez préalablement que les attributs corrects EKU sont présents.

- Surveillez l'authentification vivante ouvre une session le GUI ISE pour des pannes d'authentification et d'autorisation.
  Remarque: Quelques suppliants n'initialisent pas un échange de certificat client si l'EKU faux est présent, comme un certificat client avec EKU de l'authentification de serveur. Par conséquent, les échecs d'authentification ne pourraient pas toujours être présents dans les logs ISE.
- Quand NDES est installé dans un déploiement distribué, une racine ou une sous-titre-racine distante CA sera indiquée par le nom ou le nom de l'ordinateur CA à l'installation de service. Le serveur NDES envoie des demandes d'enregistrement de certificat à ce serveur de la cible CA. Si la procédure d'enregistrement de certificat de point final échoue, les captures de paquet (PCAP) pourraient afficher au retour de serveur NDES une erreur **404 non trouvée au** noeud ISE. Afin de résoudre ce problème, réinstaller le service NDES et sélectionner l'option de nom de l'ordinateur au lieu du nom CA.

- Évitez les modifications à la chaîne SCEP CA après que des périphériques onboarded. Les systèmes d'exploitation de point final, tels que l'IOS d'Apple, ne mettent pas à jour automatiquement un profil précédemment installé BYOD. Dans cet exemple IOS, le profil en cours doit être supprimé du point final, et du point final retiré de la base de données ISE, de sorte qu'onboarding puisse être exécuté de nouveau.

- Vous pouvez configurer un Microsoft Certificate Server afin de se connecter à l'Internet et mettre à jour automatiquement des Certificats du programme de certificat racine de Microsoft.

Si vous configurez cette option de récupération de réseau dans les environnements avec des stratégies restreintes d'Internet, les serveurs CA/NDES qui ne peuvent pas se connecter à l'Internet peuvent prendre 15 secondes au délai d'attente par défaut. Ceci peut ajouter un retard 15-second au traitement des demandes SCEP des proxys SCEP tels qu'ISE. ISE est des demandes programmées du délai d'attente SCEP après 12 secondes si une réponse n'est pas reçue. Afin de résoudre ce problème, permettez l'accès Internet pour les serveurs CA/NDES, ou modifiez les configurations de délai d'attente de récupération de réseau dans la stratégie de sécurité locale des serveurs de Microsoft CA/NDES. Afin de localiser cette configuration sur le serveur de Microsoft, naviguez **pour commencer > des outils d'administration > stratégie de sécurité locale > des stratégies de clé publique > des configurations de validation de chemin de certificat > récupération de réseau**.

Se connecter de côté client

Voici une liste de techniques utiles qui sont utilisées afin de dépanner le côté client se connectant des questions :

- Sélectionnez la **commande du log %temp% \ spwProfileLog.txt** afin de visualiser les logs de côté client pour des applications Windows de Mircosoft.
  Remarque: WinHTTP est utilisé pour la connexion entre le point final de Microsoft Windows et l'ISE. Mettez en référence l'article de messages d'erreur de Microsoft Windows pour une liste de codes d'erreur.
- Sélectionnez la commande de **/sdcards/downloads/spw.log** afin de visualiser les logs de côté client pour des applications d'Android.

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

- Pour l'**IOS d'Apple**, configurateur 2.0 d'Apple d'utilisation afin de visualiser des messages.

Se connecter ISE

Terminez-vous ces étapes afin de visualiser le log ISE :

1. Naviguez vers la **gestion > en se connectant > configuration de log de debug**, et sélectionnez le noeud approprié de stratégie ISE.

2. Placez le **client** et le **ravitaillement** se connecte pour mettre au point ou tracer, au besoin.

3. Reproduisez le problème et documentez les informations appropriées de graine afin de faciliter le rechercher, comme le MAC, l'IP, et l'utilisateur.

4. Naviguez vers des **exécutions** > des **logs de téléchargement**, et sélectionnez le noeud approprié ISE.

5. Sur le **debug les logs** tabulent, téléchargent les logs nommés **ise-psc.log à l'**appareil de bureau.

6. Employez un éditeur intelligent, tel que Notepad ++ afin d'analyser les fichiers journal.

7. Quand la question a été isolée, alors renvoyez les niveaux de log au niveau par défaut.

NDES se connectant et dépannant

Le pour en savoir plus, se rapportent au CS d'AD : Dépannage de l'article de Windows Server de service d'inscription de périphérique de réseau.

Informations connexes

- Guide de solutions BYOD - Configuration du serveur d'autorité de certification
- Aperçu NDES dans Windows 2008 R2
- Livre Blanc MSCEP
- Configurer le serveur NDES pour prendre en charge le SSL
- Délivrez un certificat les conditions requises quand vous utilisez l'EAP-TLS ou le PEAP avec l'EAP-TLS
- Soutien technique et documentation