ISE SCEP-ondersteuning voor BYOD configureren

Inhoud

Inleiding

Dit document beschrijft de stappen die worden gebruikt om met succes de Microsoft Network Application Services Service (NDES) en Simple certificaatinschrijvingsprotocol (SCEP) te configureren om uw eigen apparaat (BYOD) in Cisco Identify Services Engine (ISE) in te voeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE release 1.1.1 of hoger
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 - standaard
- PKI en certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE release 1.1.1 of hoger
- Windows Server 2008 R2 SP1 met geïnstalleerde hotfixes voor KB2483564 en KB263200
- Windows Server 2012-standaard

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, zijn gestart met een gewalste (standaard) configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

De informatie met betrekking tot Microsoft certificaatservices wordt geleverd als een handleiding specifiek voor Cisco BYOD. Raadpleeg Microsoft TechNet als de definitieve bron van de waarheid voor Microsoft certificeringsinstantie, Network Devices (NDES) en SCEP-gerelateerde serverconfiguraties.

Achtergrondinformatie

Een van de voordelen van de Cisco ISE-enabled BYOD-implementatie is de mogelijkheid van de eindgebruikers om zelf-service apparaatregistratie uit te voeren. Dit heft de administratieve last op voor IT om authenticatie geloofsbrieven te verspreiden en apparaten op het netwerk mogelijk te maken. Aan de basis van de BYOD-oplossing ligt het bevoorradingsproces van de netwerkleveranciers, dat tot doel heeft de vereiste certificaten aan apparaten van de werknemers te verdelen. Om aan deze eis te voldoen kan een Microsoft certificaatinstantie (CA) worden ingesteld om het inlogproces van het certificaat met het SCEP te automatiseren.

SCEP wordt al jaren in VPN-omgevingen (Virtual Private Network) gebruikt om inschrijving en distributie van certificaten aan externe toegangsklanten en routers te vergemakkelijken. Voor het inschakelen van SCEP-functionaliteit op een Windows 2008 R2-server is de installatie van de NDES vereist. Tijdens de NDES-rolinstallatie is ook de Microsoft Internet Information Services (IS)-webserver geïnstalleerd. IS wordt gebruikt om HTTP of HTTPS SCEP registratieverzoeken en reacties tussen het CA- en ISE-beleidsknooppunt te beëindigen.

De NDES-rol kan worden geïnstalleerd op een huidige CA-server of op een aangesloten server. In een standalone plaatsing, wordt de NDES-service geïnstalleerd op een bestaande CA die de dienst van de certificeringsinstantie en, naar keuze, de dienst van de certificeringsinstantie Web Enrollment omvat. In een gedistribueerde toepassing wordt de NDES-service op een aangesloten server geïnstalleerd. De gedistribueerde NDES-server wordt vervolgens geconfigureerd om met een CA-upstream of subroot te communiceren. In dit scenario worden de in dit document geschetste registermodificaties gemaakt op de NDES-server met de aangepaste sjabloon, waar de certificaten op de upstream CA liggen.

Testscenario’s voor CA/NDES-implementaties

Deze sectie verschaft een kort overzicht van de CA/NDES-implementatiescenario's die in het Cisco-lab zijn getest. Raadpleeg Microsoft TechNet als de definitieve bron van de waarheid voor Microsoft CA, NDES en SCEP-gerelateerde serverconfiguraties.

Standalone implementaties

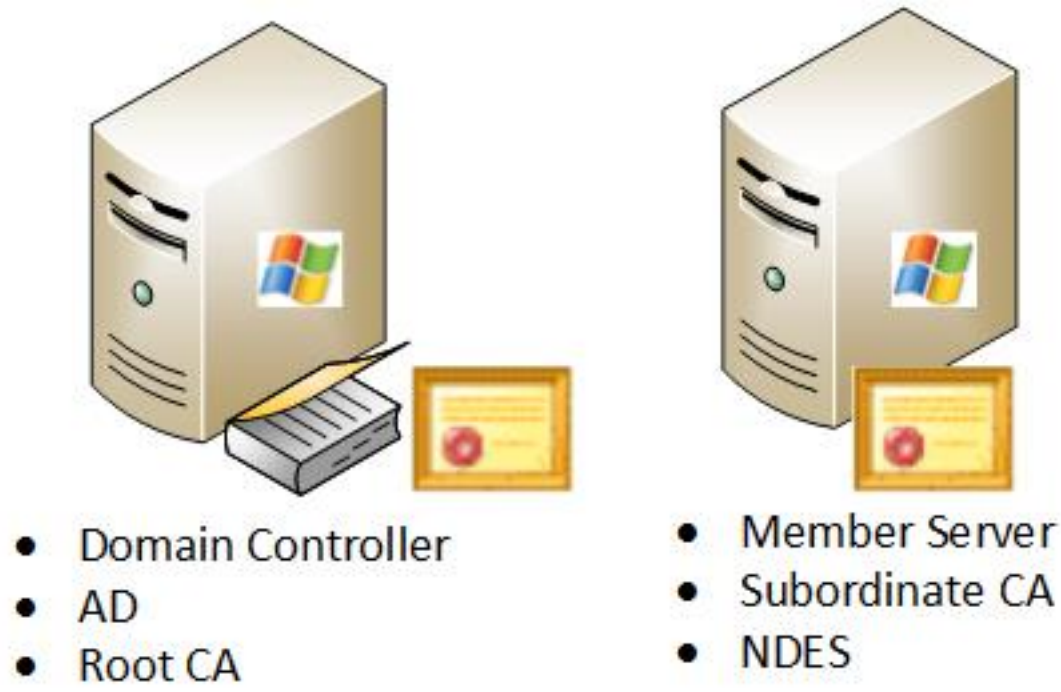
Wanneer ISE in een scenario dat van het Concept van het Bewijs van het Concept (PoC) wordt gebruikt, is het gebruikelijk om een op zichzelf staand Windows 2008 of 2012 machine in te voeren die als een Active Directory (AD) domeincontroller, root CA, en NDES-server werkt:

- Domain Controller
- AD
- Root CA
- NDES

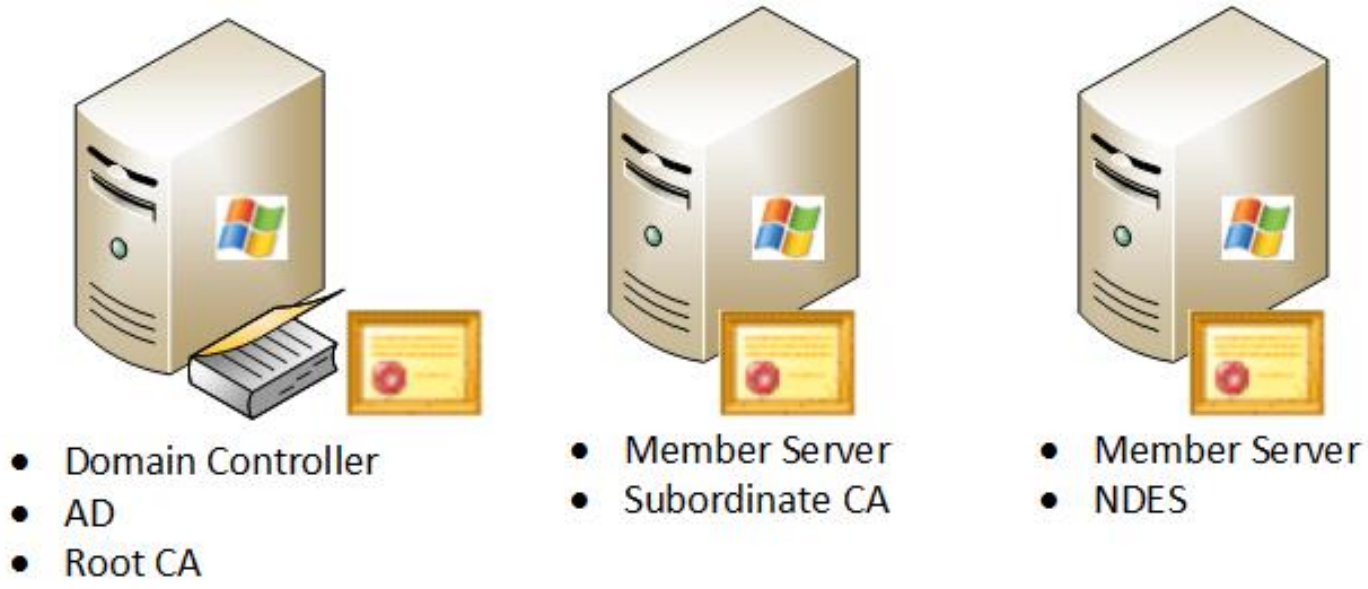
Gedistribueerde implementaties

Wanneer ISE in een huidige Microsoft AD/PKI-productieomgeving is geïntegreerd, is het gebruikelijker om services te zien verdeeld over meerdere, verschillende Windows 2008- of 2012-servers. Cisco heeft twee scenario's voor gedistribueerde implementaties getest.

Dit beeld illustreert het eerste geteste scenario voor gedistribueerde implementaties:



Dit beeld illustreert het tweede geteste scenario voor gedistribueerde implementaties:



Belangrijke Microsoft hotfixes

Voordat u SCEP-ondersteuning voor BYOD configureren, moet u ervoor zorgen dat deze Microsoft hotfixes zijn geïnstalleerd op de Windows 2008 R2 NDES-server:

- Verleng het verzoek om een SCEP certificaat faalt in Windows Server 2008 R2 als het certificaat wordt beheerd door NDES te gebruiken - Deze kwestie komt voor omdat NDES de **GetCACaps-**handeling niet ondersteunt.

- NDES dienen geen certificaatverzoeken in nadat de ondernemings CA opnieuw is opgestart in Windows Server 2008 R2 - Dit bericht verschijnt in het **Event Viewer**: "*De inlogservice voor het netwerkapparaat kan niet de certificaataanvraag indienen (0x800706ba). De RPC-server is niet beschikbaar.*"

Waarschuwing: Wanneer u de Microsoft CA vormt, is het belangrijk om te begrijpen dat ISE het RSASSA-PSS algoritme niet ondersteunt. Cisco raadt u aan het CA-beleid te configureren zodat het sha1WithEncryption of sha256WithRSAEencryptie gebruikt in plaats daarvan.

Belangrijke BYOD-poorten en -protocollen

Hier volgt een lijst met belangrijke BYOD-poorten en -protocollen:

- TCP: 8909 Provisioning: Wizard Installeer vanuit Cisco ISE (Windows- en Macintosh-besturingssystemen (OS)
- TCP: 443 Provisioning: Wizard Installeer vanuit Google Play (Android)
- TCP: 8905 Provisioning: Provisioningproces voor leveranciers
- TCP: 80 of TCP: 443 SCEP proxy voor CA (gebaseerd op de SCEP RA URL-configuratie)

Opmerking: Raadpleeg de ISE 1.2 hardwareinstallatiehandleiding voor de snelste lijst van vereiste poorten en protocollen.

Configureren

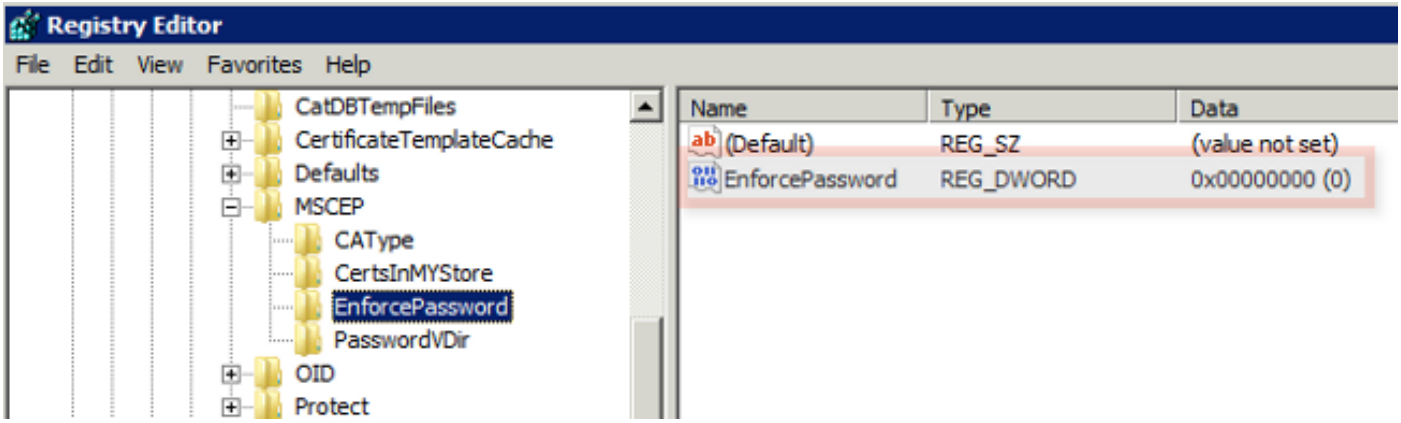
Gebruik dit gedeelte om NDES en SCEP ondersteuning voor BYOD op ISE te configureren.

Wachtwoord voor invoeren van SCEP uitschakelen

Standaard gebruikt de Microsoft SCEP (MSCEP)-implementatie een dynamisch challenge-wachtwoord om klanten en endpoints tijdens het gehele proces van inschrijven van het certificaat voor authentiek te verklaren. Als deze configuratie vereist is, moet u naar de MSCEP admin web GUI op de NDES-server bladeren om een wachtwoord op aanvraag te genereren. U moet dit wachtwoord invoeren als onderdeel van de registratieaanvraag.

In een BYOD-toepassing, heeft de eis van een uitdagingswachtwoord niet langer het doel van een gebruikerszelfservice-oplossing. Om deze vereiste te verwijderen, moet u deze registersleutel op de NDES-server wijzigen:

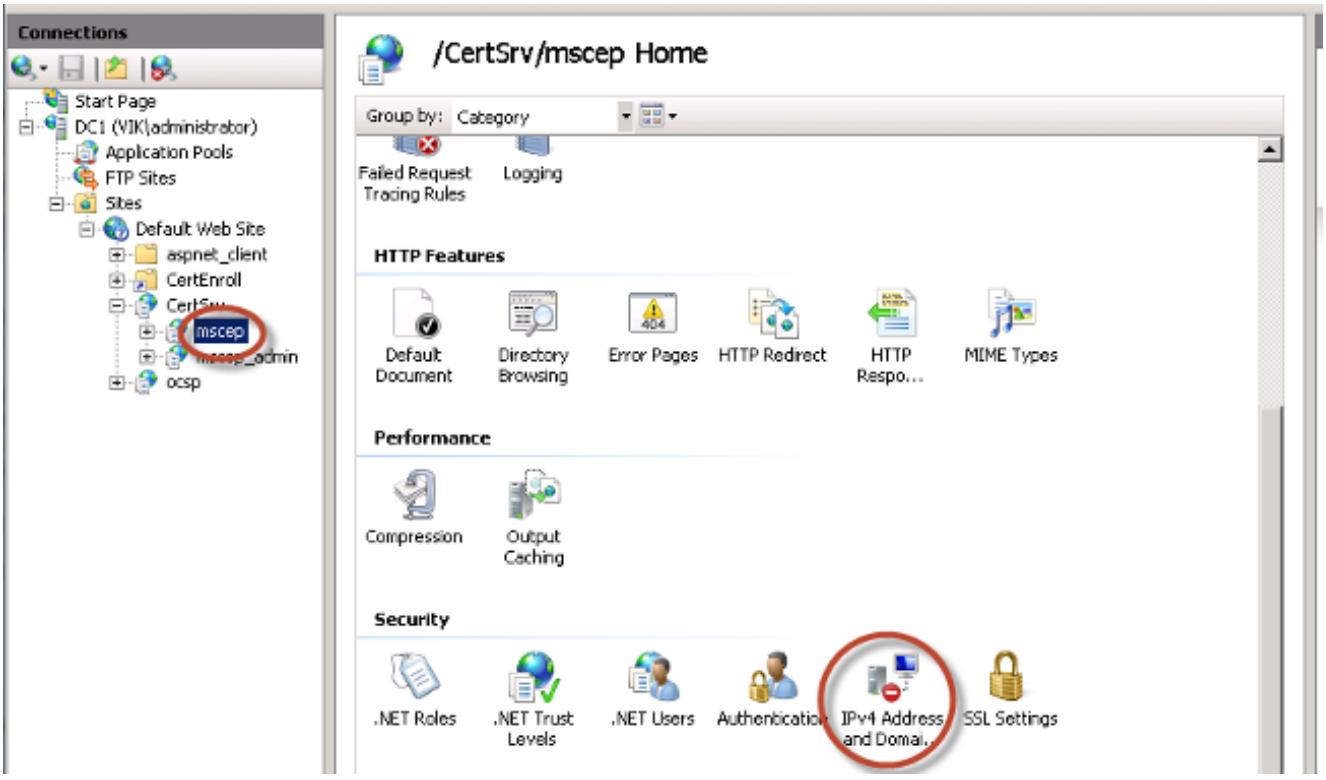
1. Klik op **Start** en voer de **revisie** in de zoekbalk in.
2. Navigatie naar **computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptografie > SCEP > Wachtwoord voor kracht** uitvoeren.
3. Zorg ervoor dat de waarde **EnforcePassword** is ingesteld op **0** (de standaardwaarde is **1**).



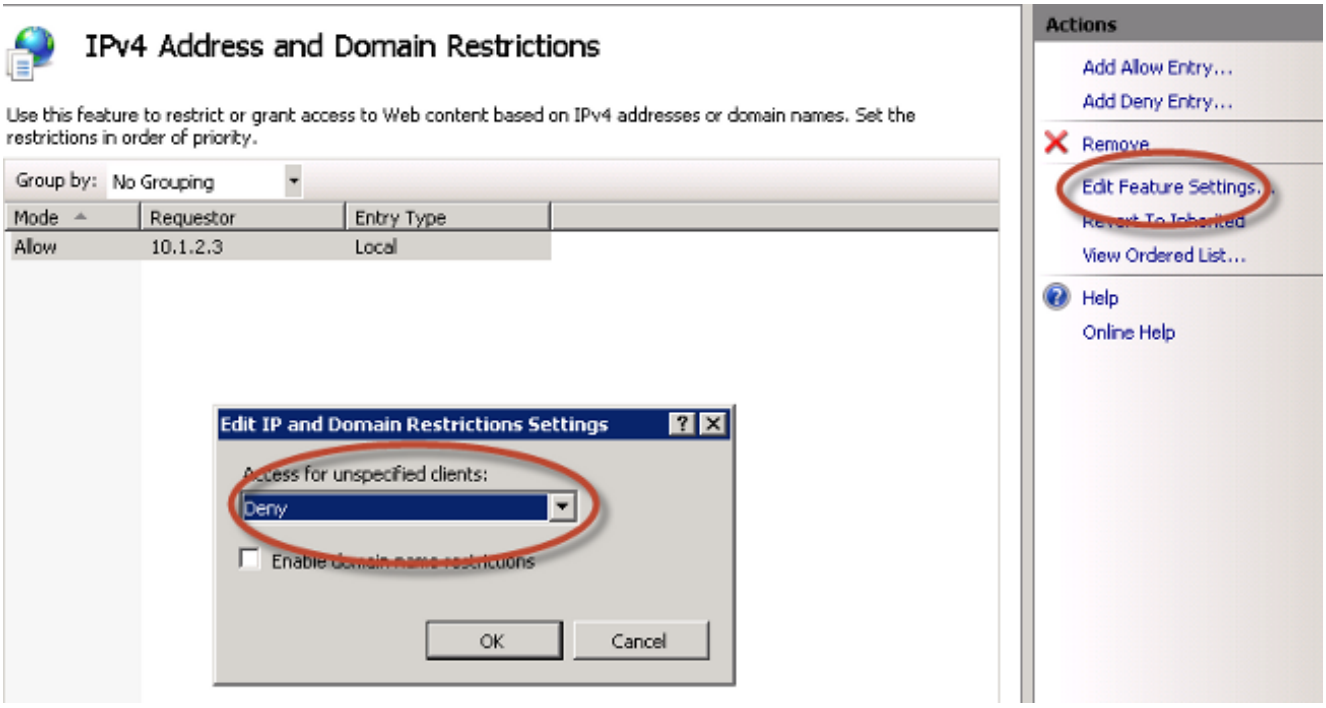
SCEP-inschrijving beperken tot bekende ISE-knooppunten

In sommige implementatiescenario's is het mogelijk om de communicatie van SCEP te beperken tot een selecte lijst met bekende ISE-knooppunten. Dit kan met de optie IPv4-adres en domeinbeperkingen in IS worden verwezenlijkt:

1. Open IS en navigeer naar de website van de / CertSrv/**mscep**.



2. Dubbelklik op **Security > IPv4-adres en domeinbeperkingen.** Gebruik de acties **Add Allow Entry** en **Add Deny Entry** om de toegang tot webinhoud op basis van IPv4-adressen of domeinnamen toe te staan of te beperken. Gebruik de actie **Instellingen optie Bewerken** om een standaard toegangsregel voor niet-gespecificeerde clients te definiëren.

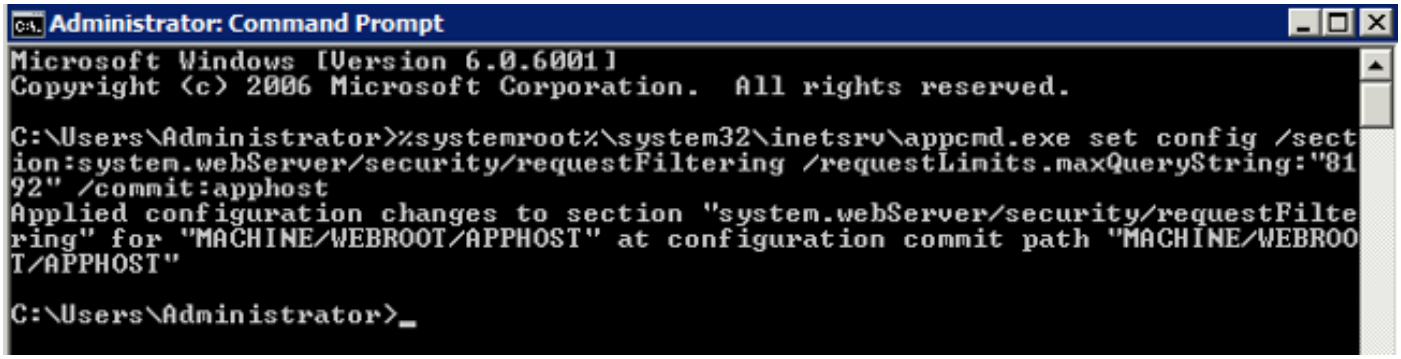


Lijnt de URL-lengte in IS uit

Het is mogelijk voor ISE om URL's te genereren die te lang zijn voor de IS web server. Om dit probleem te vermijden, kan de standaard-IS configuratie worden aangepast om langere URL's toe te staan. Voer deze opdracht in vanaf de NDES-server CLI:

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

Opmerking: De grootte van een query string kan variëren afhankelijk van de ISE en de endpointconfiguratie. Voer deze opdracht in vanaf de NDES-server CLI met beheerrechten.



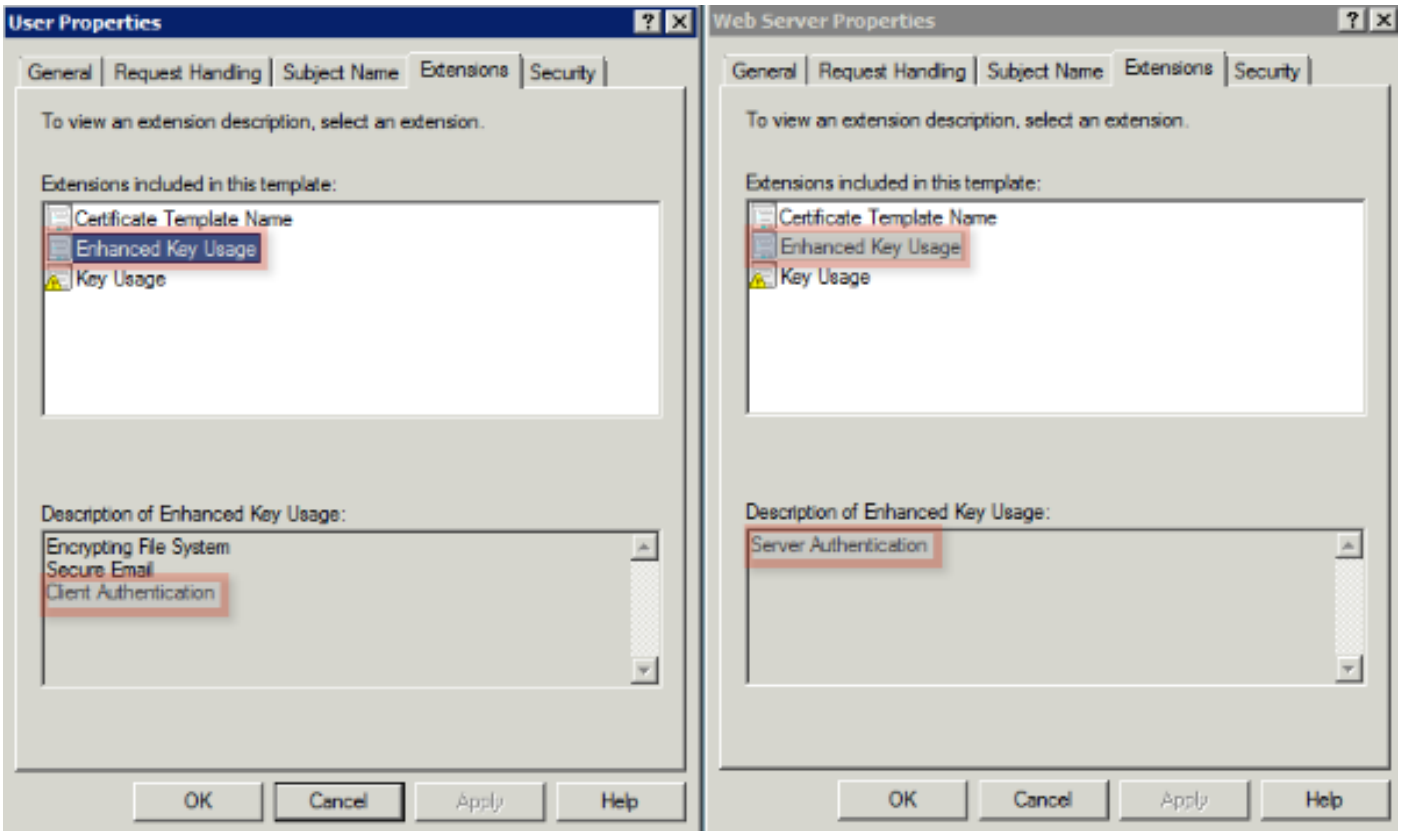
Overzicht van certificaatsjabloon

Beheerders van een Microsoft CA kunnen één of meer sjablonen configureren die worden gebruikt om toepassingsbeleid toe te passen op een gebruikelijke reeks certificaten. Dit beleid helpt te identificeren voor welke functie het certificaat en de bijbehorende toetsen worden gebruikt. De beleidswaarden voor toepassingen zijn vervat in het veld Uitgebreide Key Use (EKU) van het certificaat. De authenticator ontleent de waarden in het EKU-veld om ervoor te zorgen dat het door de cliënt voorgelegde certificaat voor de beoogde functie kan worden gebruikt. Enkele van de meest gebruikelijke toepassingen zijn serververificatie, clientverificatie, IPSec VPN en e-mail. In termen van ISE omvatten de meest gebruikte EKU-waarden server- en/of clientverificatie.

Wanneer u doorbladert naar een beveiligde website van een bank, bijvoorbeeld, wordt de webserver die het verzoek verwerkt ingesteld met een certificaat dat een toepassingsbeleid van serverauthenticatie heeft. Wanneer de server een HTTPS-verzoek ontvangt, stuurt zij een certificaat van serververificatie naar de aangesloten webbrowser voor authenticatie. Het belangrijke punt is dat dit een eenrichtingsuitwisseling is van de server naar de cliënt. Aangezien het betrekking heeft op ISE, is een algemeen gebruik voor een certificaat van serverauthenticatie toegang tot de beheerder GUI. ISE stuurt het geconfigureerde certificaat naar de aangesloten browser en verwacht geen certificaat terug van de client te ontvangen.

Voor diensten als BYOD die met het MAP-TLS werken, verdient wederzijdse authenticatie de voorkeur. Om deze uitwisseling van bidirectionele certificaten mogelijk te maken, moet het sjabloon dat wordt gebruikt om het ISE-identiteitsbewijs te genereren, beschikken over een minimaal toepassingsbeleid van serverauthenticatie. De sjabloon van het webservercertificaat voldoet aan deze eis. De certificeringssjabloon die de eindpuntcertificaten genereert, moet een minimaal toepassingsbeleid van cliënteffectie bevatten. De sjabloon van het gebruikerscertificaat voldoet aan deze eis. Als u ISE voor services zoals Inline Policy Encapsulation Point (iPEP) configureren moet de sjabloon die gebruikt wordt om het ISE server Identity Certificate te genereren zowel client- als serverauthenticatie eigenschappen bevatten indien u ISE versie 1.1.x of eerder gebruikt. Dit maakt het mogelijk om de admin- en inline knooppunten onderling te authentiseren. De EKU-validatie voor iPEP werd verwijderd in ISE versie 1.2, waardoor deze eis minder relevant is.

U kunt de standaard Microsoft CA Web Server en de gebruikerssjablonen opnieuw gebruiken of u kunt een nieuwe sjabloon klonen en maken met het proces dat in dit document is beschreven. Op basis van deze certificeringsvereisten moeten de CA-configuratie en de resulterende ISE- en endpointcertificaten zorgvuldig worden gepland om ongewenste configuratiewijzigingen te minimaliseren wanneer ze in een productieomgeving zijn geïnstalleerd.



Configuratie van certificaatsjabloon

Zoals in de introductie wordt opgemerkt, wordt SCEP veel gebruikt in IPSec VPN-omgevingen. Hierdoor wordt de NDES-rol automatisch in de installatie van de server ingesteld om de **IPSec-**sjabloon **(offline request)** voor SCEP te gebruiken. Daarom is een van de eerste stappen bij de voorbereiding van een Microsoft CA voor BYOD het bouwen van een nieuwe sjabloon met het juiste toepassingsbeleid. In een standalone-plaatsing, worden de certificeringsinstantie en NDES-diensten op dezelfde server ondergebracht, en worden de sjablonen en de vereiste registerwijzigingen op dezelfde server ingesloten. Bij een gedistribueerde NDES-toepassing worden de wijzigingen van de registratie aangebracht op de NDES-server; de werkelijke sjablonen worden echter gedefinieerd op de CA-server die in de NDES-service-installatie is gespecificeerd.

Voltooi deze stappen om de certificaatsjabloon te configureren:

1. Log in op de CA server als **beheerder**.

2. Klik op **Start > Administratieve hulpmiddelen > certificeringsinstantie**.

3. Vul de CA-servergegevens uit en selecteer de map **certificaatsjablonen**. Deze map bevat een lijst met sjablonen die op dit moment zijn ingeschakeld.

4. Om de certificaatsjablonen te beheren, klikt u met de rechtermuisknop op de map **certificaatsjablonen** en vervolgens kiest u **Beheer**.

5. In de **console van sjablonen** wordt een aantal inactieve sjablonen weergegeven.

6. Om een nieuwe sjabloon voor gebruik met SCEP te configureren klikt u met de rechtermuisknop op een sjabloon die al bestaat, zoals **Gebruiker**, en kiest u **Dubbele sjabloon**.

7. Kies **Windows 2003** of **Windows 2008**, afhankelijk van de minimale CA-OS in de omgeving.

8. Voeg in het **tabblad General** een weergavenaam toe, zoals ISE-BYOD, en een validatieperiode Laat alle andere opties ongecontroleerd.
   Opmerking: De geldigheidsduur van de sjabloon moet kleiner zijn dan of gelijk zijn aan de geldigheidsperiode van de CA-wortel- en intermediaire certificaten.
9. Klik op het tabblad **Onderwerp** en bevestig dat **Levering in het verzoek** is geselecteerd.

10. Klik op het tabblad **Eisen** voor **uitgifte**. Cisco raadt u aan het **beleid van** de **Uitgifte** te laten blanco in een typische hiërarchische CA-omgeving.

11. Klik op het tabblad **Uitbreidingen**, **Toepassingsbeleid** en **Bewerk** vervolgens.

12. Klik op **Add** en zorg ervoor dat **Clientverificatie** wordt toegevoegd als toepassingsbeleid. Klik op **OK**.

13. Klik op het tabblad **Beveiliging** en vervolgens **op Toevoegen...**. Zorg ervoor dat de SCEP-servicekaart die in de NDES-servicesinstallatie is gedefinieerd, volledige controle over de sjabloon heeft en klik vervolgens op **OK**.

14. Ga terug naar de **GUI van de certificeringsinstantie**.

15. Klik met de rechtermuisknop op de map **certificaatsjablonen**. Navigeer naar **Nieuw > certificaatsjabloon voor afgifte**.

16. Selecteer de eerder ingestelde **ISE-BYOD**-sjabloon en klik op **OK**.

    Opmerking: U kunt de sjabloon ook activeren via de CLI met de opdracht **certutil -SetCAsjablonen +ISE-BYOD**.
    De ISE-BYOD-sjabloon moet nu in de lijst met toegestane certificaatsjablonen worden opgenomen.

Configuratie van certificaatsjabloon

Voltooi deze stappen om de toetsen van de certificaatsjabloonregistratie aan te passen:

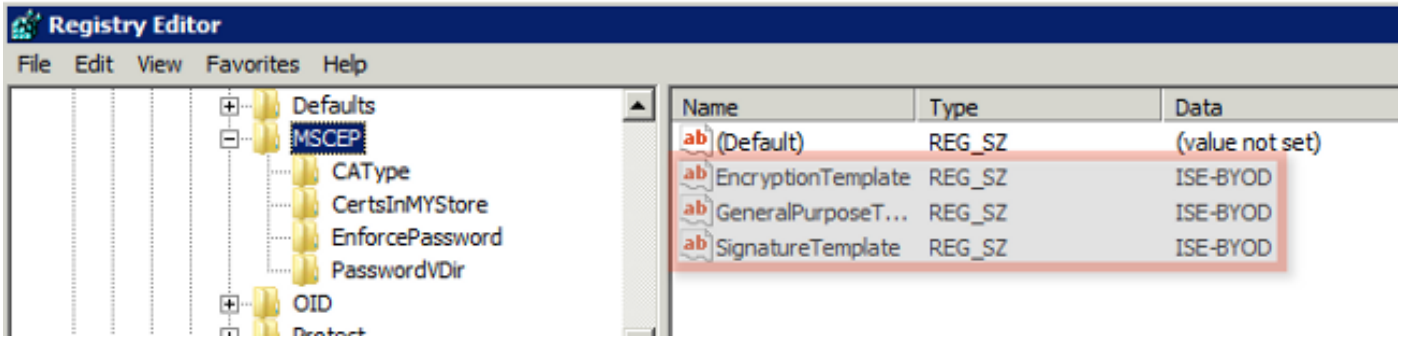
1. Sluit aan op de NDES-server.

2. Klik op **Start** en voer de **revisie** in de zoekbalk in.

3. Navigeren naar **computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptografie > MSCEP.**

4. Verander de toetsen **EncryptionSjabloon**, **GeneralPurposeSjabloon** en **Signaturejabloon** van **IPSec (Offline request)** naar de **eerder gemaakte ISE-BYOD-sjabloon.**

5. Herstart de NDES-server om de registratieinstelling toe te passen.



ISE configureren als SCEP proxy

In een BYOD-toepassing, communiceert het eindpunt niet rechtstreeks met de backend-NDES-server. In plaats daarvan wordt het ISE-beleidsknooppunt geconfigureerd als een SCEP-proxy en communiceert het met de NDES-server namens de endpoints. De eindpunten communiceren rechtstreeks met de ISE. De IS-instantie op de NDES-server kan worden geconfigureerd voor ondersteuning van HTTP- en/of HTTPS-verbindingen voor de virtuele SCEP-directories.

Volg deze stappen om ISE als een SCEP proxy te configureren:

1. Log in op de **ISE GUI** met admin geloofsbrieven.

2. Klik op **Administratie**, **Certificaten**, en dan **SCEP CA profielen**.

3. Klik op **Add** (Toevoegen).

4. Voer de naam en beschrijving van de server in.

5. Voer de URL voor de SCEP server in met de IP of Full Qualified Domain Name (FQDN) (http://10.10.10.10/certsrv/mscep/, bijvoorbeeld).

6. Klik op **Test Connectivity**. Een geslaagde verbinding resulteert in een succesvol server-responsbericht.

7. Klik op **Opslaan** om de configuratie toe te passen.

8. Klik om dit te controleren op **Administratie**, **Certificaten**, **certificaatopslag en bevestig dat het SCEP NDES server RA certificaat automatisch is gedownload naar het ISE-knooppunt.**

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat troubleshooting-informatie voor uw configuratie.

Algemene opmerkingen voor probleemoplossing

Hier is een lijst met belangrijke opmerkingen die u kunt gebruiken om problemen met uw configuratie op te lossen:

- Breek de topologie van het BYOD-netwerk naar logische toegangspunten om te helpen debug- en opnamepunten langs het pad tussen de ISE-, NDES- en CA-endpoints te identificeren.
- Zorg ervoor dat het ISE-knooppunt en CA een gezamenlijke Network Time Protocol (NTP)-tijdbron delen.
- Endpoints moeten hun tijd automatisch met de NTP- en tijdzoneopties kunnen instellen die met DHCP zijn geleerd.
- De DNS server van de client moet de FQDN van het ISE-knooppunt kunnen oplossen.
- Verzeker dat TCP 80 en/of TCP 443 bidirectioneel is toegestaan tussen ISE en de NDES-server.
- Test met een Windows machine vanwege verbeterde vastlegging aan de kant van de client. Gebruik optioneel een Apple iDevices in combinatie met het Apple iPhone Configuration-hulpprogramma om de logbestanden van de klant-zijconsole te controleren.

- Controleer de logbestanden van de CA- en NDES-servertoepassing op registratiefouten en gebruik Google of TechNet om deze fouten te onderzoeken.

- Gebruik in de hele testfase HTTP voor SCEP om pakketvastlegging tussen ISE, NDES en CA te vergemakkelijken.

- Gebruik de TCP Dump voorziening in het ISE Policy Service Node (PSN) en controleer verkeer naar en van de NDES-server. Dit bevindt zich onder **Operations > Diagnostische tools > General Tools**.

- Installeer Wireless-shark op de CA- en NDES-server of gebruik SPAN op intermediaire switches om SCEP-verkeer naar en van ISE PSN op te nemen.

- Zorg ervoor dat de juiste CA-certificeringsketen op het ISE-beleidsknooppunt is geïnstalleerd voor de echtheidscontrole van de client-certificaten.

- Zorg ervoor dat de juiste CA-certificeringsketen tijdens het instappen automatisch op de klanten wordt geïnstalleerd.

- Bekijk vooraf de ISE- en endpointidentiteitsbewijzen en bevestig dat de juiste EKU-eigenschappen aanwezig zijn.

- monitoren van de live authenticatie logbestanden in de ISE GUI voor authenticatie en autorisatiefouten.
  Opmerking: Sommige leveranciers initialiseren geen uitwisseling van klantcertificaten indien de verkeerde EKU aanwezig is, zoals een client-certificaat met EKU van serververificatie. Daarom is het mogelijk dat echtheidsfouten niet altijd in de ISE-documenten aanwezig zijn.
- Wanneer NDES in een gedistribueerde installatie is geïnstalleerd, wordt een CA-naam op afstand of een CA-subbasis door CA-naam of Computer-naam in de servicesinstallatie aangewezen. De NDES-server stuurt een certificaatregistratieaanvraag naar deze CA-server. Als het registratieproces voor endpointcertificaten faalt, kan de PCAP-server (NDES) een **404 Not Found** error aan het ISE-knooppunt weergeven. Installeer de NDES-service opnieuw om dit probleem op te lossen en selecteer de optie Computer Name in plaats van de CA-naam.

- Vermijd wijzigingen in de SCEP CA-ketting nadat de apparatuur aan boord is. Endpoint OS's, zoals Apple iOS, werken niet automatisch een eerder geïnstalleerd BYOD-profiel bij. In dit iOS-voorbeeld moet het huidige profiel uit het eindpunt worden verwijderd en moet het eindpunt uit de ISE-database worden verwijderd, zodat instappen opnieuw kan worden uitgevoerd.

- U kunt een Microsoft certificaatserver configureren om verbinding te maken met internet en automatisch certificaten te uploaden via het Microsoft Root certificaatprogramma. Als u deze optie voor het ophalen van een netwerk aanpast in omgevingen met beperkt internetbeleid, kunnen CA/NDES-servers die geen verbinding kunnen maken met het internet standaard 15 seconden nodig hebben voor de tijdelijke oplossing. Dit kan een vertraging van 15 seconden toevoegen aan de verwerking van SCEP-verzoeken van SCEP proxy's zoals ISE. ISE wordt geprogrammeerd om SCEP-verzoeken na 12 seconden op te schorten indien er geen

antwoord wordt ontvangen. Om dit probleem op te lossen, staat of internettoegang toe voor de CA/NDES-servers, of wijzigt u de tijdelijke instellingen voor netwerkopslag in het plaatselijke beveiligingsbeleid van de Microsoft CA/NDES-servers. Om deze configuratie op de Microsoft server te vinden, navigeer dan naar **Start > Administratieve hulpmiddelen > Plaatselijk beveiligingsbeleid > Openbaar sleutelbeleid > Instellingen voor validatie van het certificaatpad > Netwerkvernieuwing**.

Vastlegging aan clientzijde

Hier is een lijst met bruikbare technieken die worden gebruikt om problemen met de vastlegging aan de kant van de klant op te lossen:

- Voer het **logbestand %temp%\spwProfileLog.txt in.** opdracht om de client-side logbestanden voor Microsoft Windows-toepassingen te bekijken.
  Opmerking: WinHTTP wordt gebruikt voor de verbinding tussen het Microsoft Windows-eindpunt en ISE. Verwijs het artikel van de foutenmeldingen van Microsoft Windows voor een lijst met foutcodes.
- Voer de opdracht **/sdcards/downloads/spw.log in** om de client-side logbestanden voor Android-toepassingen te bekijken.
- Voor **MAC OSX**, gebruik de Console-toepassing en kijk naar het **SPW-**proces.
- Voor **Apple iOS**, gebruik Apple Configurator 2.0 om berichten te bekijken.

ISE-vastlegging

Volg deze stappen om het ISE-logbestand te bekijken:

1. Navigeer naar **Administratie > Vastlegging > Logconfiguratie** van het **bug logbestand** zuiveren, en selecteer het juiste ISE-beleidsknooppunt.
2. Stel de **client**- en **provisioninglogboeken in** om deze te debug of overtrekken, naar wens.
3. Reproduceren het probleem en documenteren relevante zaadinformatie om het zoeken te vergemakkelijken, zoals MAC, IP en gebruiker.
4. Navigeer naar **bewerkingen > Downloadbestanden**, en selecteer het juiste ISE-knooppunt.
5. Download in het tabblad **Debug Logs** de logs **ise-psc.log** naar het bureaublad.
6. Gebruik een intelligente editor, zoals Kladblok ++ om de logbestanden te parseren.
7. Wanneer de kwestie geïsoleerd is, dan keert u de logniveaus terug naar het standaardniveau.

NDES-vastlegging en probleemoplossing

Raadpleeg voor meer informatie het AD CS: Artikel voor Windows-server voor probleemoplossing

bij netwerkapparaatinschrijving.

Gerelateerde informatie

- BYOD-oplossingsgids - Configuratie van certificeringsinstanties
- NDES - Overzicht in Windows 2008 R2
- Witboek SCEP
- NDES-server configureren voor ondersteuning van SSL
- Certificaatvereisten bij gebruik van EAP-TLS of PEAP met EAP-TLS
- Technische ondersteuning en documentatie