Konfigurieren der ISE SCEP-Unterstützung für BYOD

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte, die zur erfolgreichen Konfiguration des Microsoft Network Device Enrollment Service (NDES) und Simple Certificate Enrollment Protocol (SCEP) für Bring Your Own Device (BYOD) auf der Cisco Identity Services Engine (ISE) erforderlich sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ISE Version 1.1.1 oder höher
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012-Standard
- Public Key Infrastructure (PKI) und Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ISE Version 1.1.1 oder höher
- Windows Server 2008 R2 SP1 mit installierten Hotfixen im KB2483564 und im KB2633200
- Windows Server 2012-Standard

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Die Informationen zu Microsoft-Zertifikatsdiensten werden als Leitfaden speziell für Cisco BYOD bereitgestellt. Verweisen Sie auf das Microsoft TechNet als endgültige Quelle der Wahrheit für Microsoft-Zertifizierungsstelle, Network Device Enrollment Service (NDES) und SCEP-bezogene Serverkonfigurationen.

Hintergrundinformationen

Einer der Vorteile der Cisco ISE-fähigen BYOD-Implementierung besteht in der Möglichkeit für Endbenutzer, Self-Service-Geräteregistrierung durchzuführen. Dadurch entfällt der Verwaltungsaufwand für die IT, Authentifizierungsdaten zu verteilen und Geräte im Netzwerk zu aktivieren. Das Kernstück der BYOD-Lösung bildet der Bereitstellungsprozess für Netzwerkkomponenten, bei dem die erforderlichen Zertifikate an private Endgeräte der Mitarbeiter verteilt werden sollen. Um diese Anforderung zu erfüllen, kann eine Microsoft Certificate Authority (CA) konfiguriert werden, um den Registrierungsprozess für Zertifikate mit dem SCEP zu automatisieren.

SCEP wird seit Jahren in VPN-Umgebungen (Virtual Private Network) verwendet, um die Registrierung und Verteilung von Zertifikaten für Clients und Router mit Remote-Zugriff zu vereinfachen. Die Aktivierung der SCEP-Funktionalität auf einem Windows 2008 R2-Server erfordert die Installation der NDES. Während der NDES-Rolleninstallation wird auch der Microsoft Internet Information Services (IIS)-Webserver installiert. IIS wird verwendet, um HTTP- oder HTTPS SCEP-Registrierungsanforderungen und -Antworten zwischen der CA und dem ISE-Richtlinienknoten zu terminieren.

Die NDES-Rolle kann auf einer aktuellen CA installiert oder auf einem Mitgliedsserver installiert werden. In einer Standalone-Bereitstellung wird der NDES-Dienst auf einer vorhandenen Zertifizierungsstelle installiert, die den Zertifizierungsstellen-Service und optional den Certification Authority Web Enrollment-Service umfasst. In einer verteilten Bereitstellung wird der NDES-Dienst auf einem Mitgliedsserver installiert. Der verteilte NDES-Server wird so konfiguriert, dass er mit einer Upstream-Root- oder Subroot-CA kommuniziert. In diesem Szenario werden die in diesem Dokument beschriebenen Änderungen an der Registrierung auf dem NDES-Server mit der benutzerdefinierten Vorlage vorgenommen, auf dem Zertifikate auf der Upstream-CA gespeichert

sind.

Getestete Bereitstellungsszenarien für CA/NDES

Dieser Abschnitt bietet einen kurzen Überblick über die im Cisco Labor getesteten CA/NDES-Bereitstellungsszenarien. Verweisen Sie auf das Microsoft TechNet als endgültige Quelle der Wahrheit für Microsoft CA-, NDES- und SCEP-bezogene Serverkonfigurationen.

Standalone-Bereitstellungen

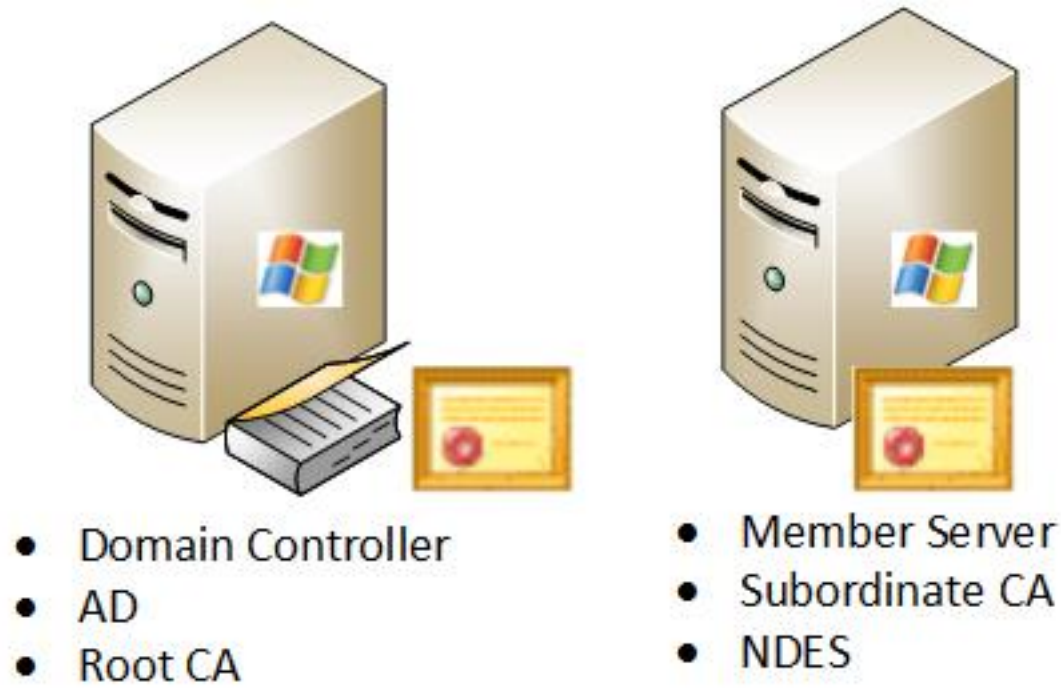
Wenn die ISE in einem Proof of Concept (PoC)-Szenario verwendet wird, ist es üblich, einen eigenständigen Windows 2008- oder 2012-Computer bereitzustellen, der als Active Directory (AD)-Domänen-Controller, Root CA und NDES-Server fungiert:

- Domain Controller
- AD
- Root CA
- NDES

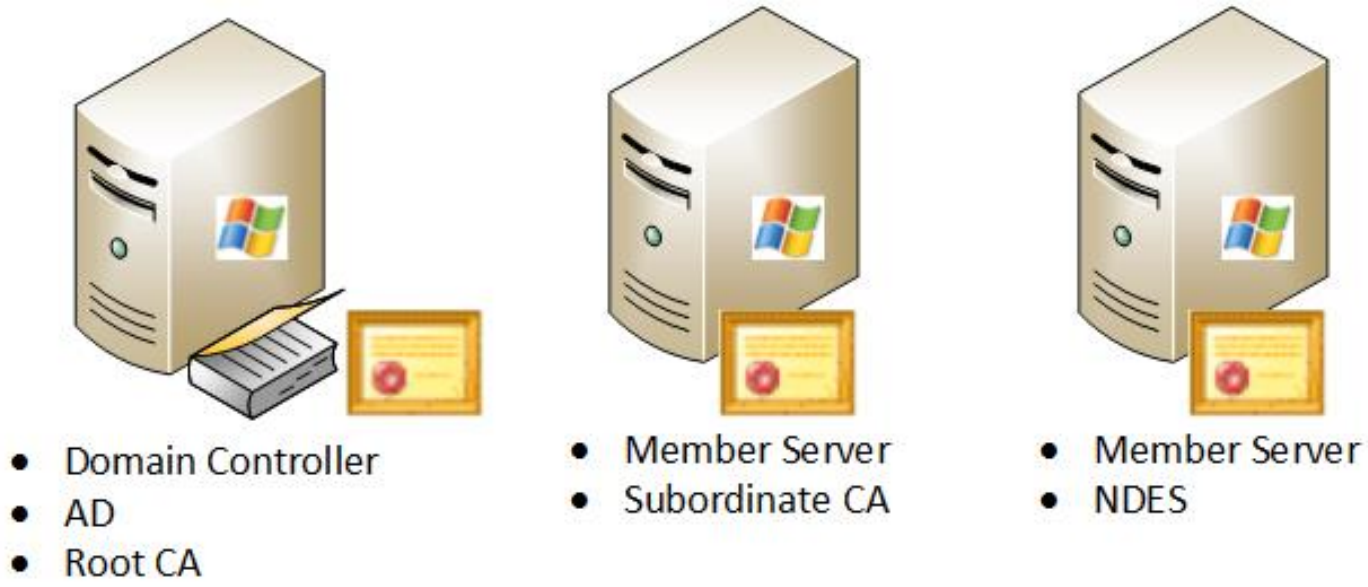
Verteilte Bereitstellungen

Wenn die ISE in eine aktuelle Microsoft AD/PKI-Produktionsumgebung integriert ist, wird es häufiger angezeigt, dass Services auf mehreren, unterschiedlichen Windows 2008- oder 2012-Servern verteilt werden. Cisco hat zwei Szenarien für verteilte Bereitstellungen getestet.

Dieses Image zeigt das erste getestete Szenario für verteilte Bereitstellungen:



Dieses Image zeigt das zweite getestete Szenario für verteilte Bereitstellungen:



Wichtige Microsoft-Hotfixe

Bevor Sie die SCEP-Unterstützung für BYOD konfigurieren, stellen Sie sicher, dass auf dem Windows 2008 R2 NDES-Server folgende Microsoft-Hotfixe installiert sind:

- Die Verlängerungsanfrage für ein SCEP-Zertifikat schlägt in Windows Server 2008 R2 fehl, wenn das Zertifikat mithilfe von NDES verwaltet wird - Dieses Problem tritt auf, weil NDES den **GetCACaps-**Vorgang nicht unterstützt.

- NDES sendet keine Zertifikatsanforderungen, nachdem die Enterprise CA in Windows Server 2008 R2 neu gestartet wurde - Diese Meldung wird in der **Ereignisanzeige** angezeigt: "*Der Network Device Enrollment Service kann die Zertifikatsanforderung (0x800706ba) nicht einreichen. Der RPC-Server ist nicht verfügbar.*"

Warnung: Wenn Sie die Microsoft CA konfigurieren, ist es wichtig zu verstehen, dass die ISE den RSASSA-PSS-Signaturalgorithmus nicht unterstützt. Cisco empfiehlt, die CA-Richtlinie so zu konfigurieren, dass sie stattdessen sha1WithRSAEncryption oder sha256WithRSAEncryption verwendet.

Wichtige BYOD-Ports und -Protokolle

Nachfolgend finden Sie eine Liste wichtiger BYOD-Ports und -Protokolle:

- TCP: 8909-Bereitstellung: Installation des Assistenten über die Cisco ISE (Windows- und Macintosh-Betriebssysteme (OS))
- TCP: 443 Bereitstellung: Installation des Assistenten über Google Play (Android)
- TCP: 8905-Bereitstellung: Supplicant Provisioning-Prozess
- TCP: 80 oder TCP: 443 SCEP-Proxy zu CA (basierend auf der SCEP RA URL-Konfiguration)

Hinweis: Eine aktuelle Liste der erforderlichen Ports und Protokolle finden Sie im ISE 1.2 Hardware Installation Guide.

Konfiguration

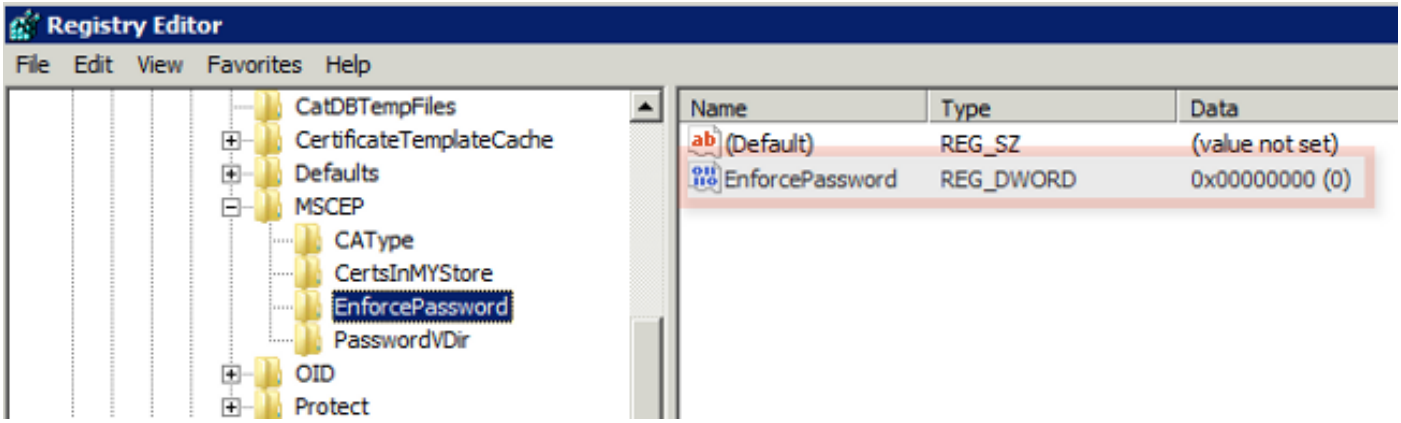
In diesem Abschnitt können Sie die NDES- und SCEP-Unterstützung für BYOD auf der ISE konfigurieren.

Kennwortanforderung für SCEP-Anmeldung deaktivieren

Standardmäßig verwendet die Microsoft SCEP (MSCEP)-Implementierung ein dynamisches Kennwort für die Anrufweiterleitung, um Clients und Endpunkte während des gesamten Zertifikatregistrierungsprozesses zu authentifizieren. Wenn diese Konfigurationsanforderung erfüllt ist, müssen Sie auf dem NDES-Server zur MSCEP-Admin-Web-GUI navigieren, um ein Kennwort bei Bedarf zu generieren. Sie müssen dieses Kennwort als Teil der Registrierungsanfrage angeben.

Bei einer BYOD-Bereitstellung wird der Zweck einer Self-Service-Lösung durch das Erfordernis eines "Challenge Passworts" außer Kraft gesetzt. Um diese Anforderung zu entfernen, müssen Sie diesen Registrierungsschlüssel auf dem NDES-Server ändern:

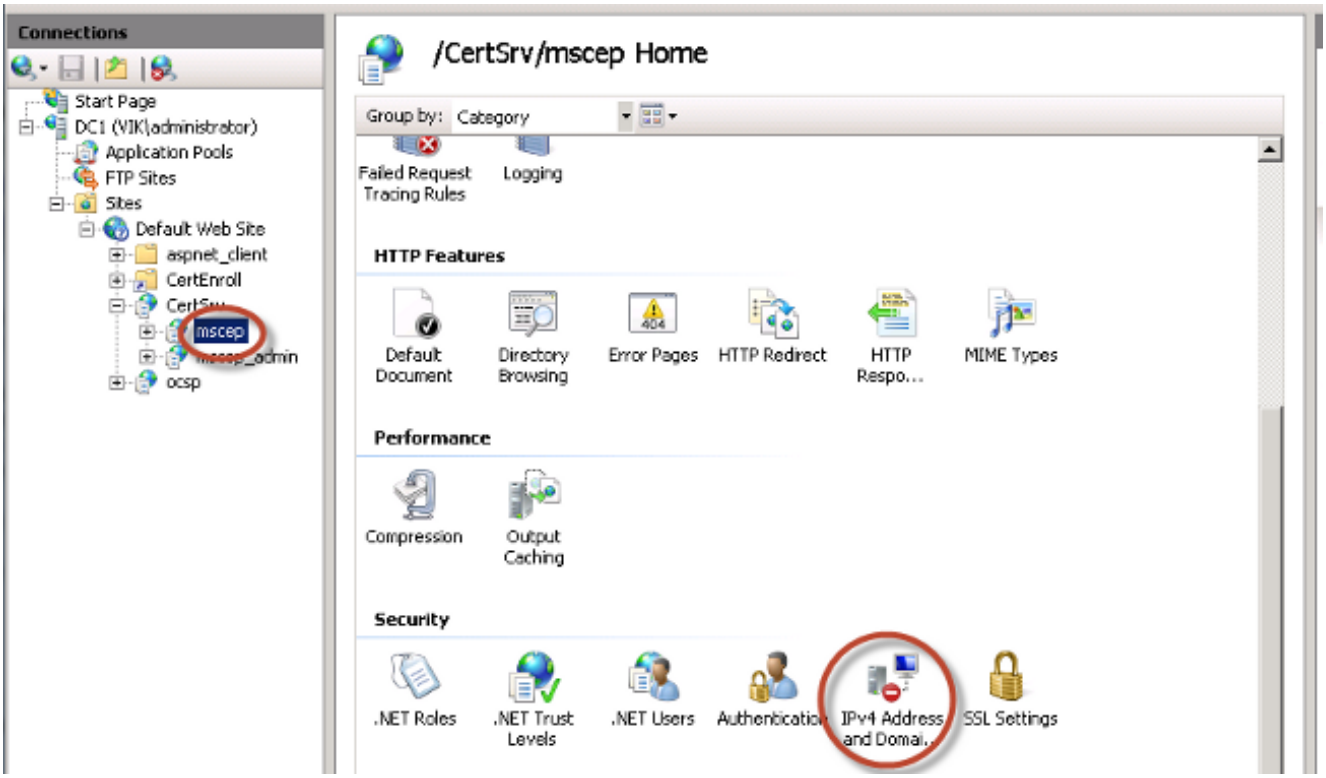
1. Klicken Sie auf **Start** und geben Sie **regedit** in die Suchleiste ein.
2. Navigieren Sie zu **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword.**
3. Stellen Sie sicher, dass der **EnforcePassword**-Wert auf **0** festgelegt ist (der Standardwert ist **1**).



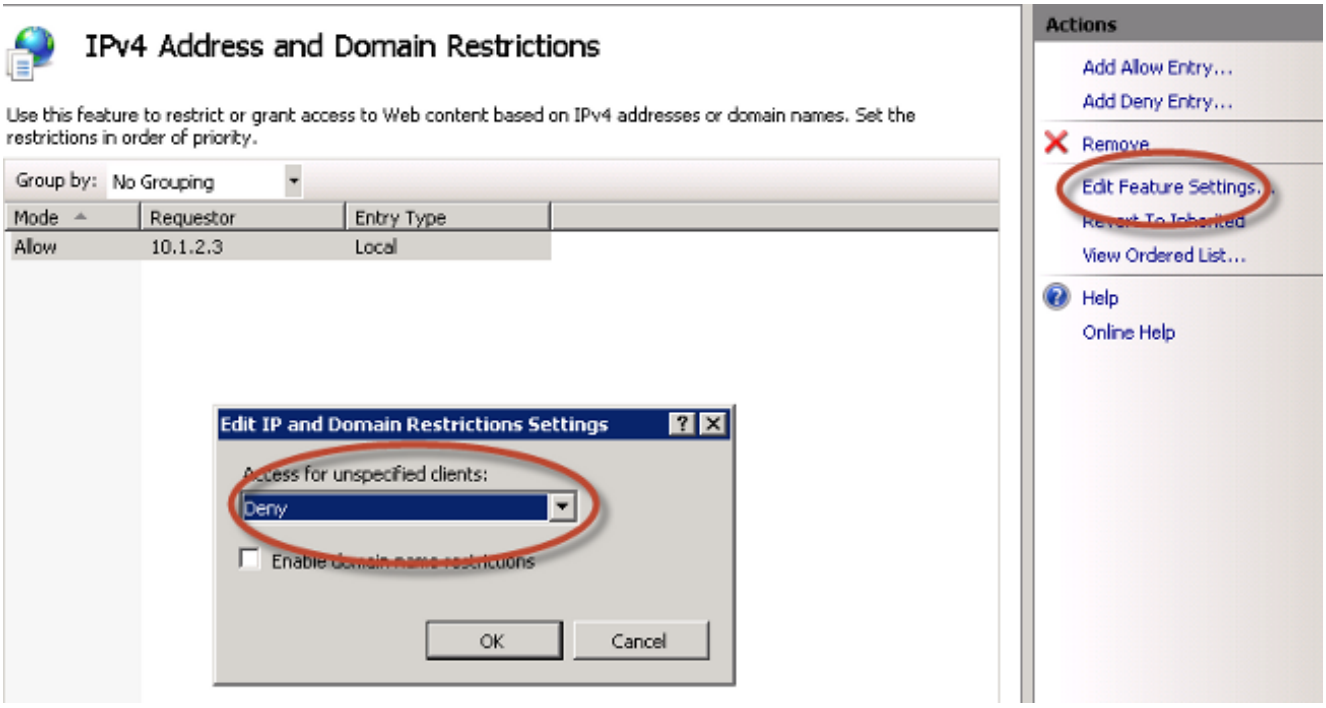
Einschränken der SCEP-Registrierung auf bekannte ISE-Knoten

In einigen Bereitstellungsszenarien ist es möglicherweise vorzuziehen, die SCEP-Kommunikation auf eine ausgewählte Liste bekannter ISE-Knoten zu beschränken. Dies kann mithilfe des Features IPv4 Address and Domain Restrictions (IPv4-Adresseneinschränkungen und Domäneneinschränkungen) in IIS erreicht werden:

1. Öffnen Sie IIS, und navigieren Sie zur Website **/CertSrv/mscep**.



2. Doppelklicken Sie auf **Sicherheit > IPv4-Adressen- und Domänenbeschränkungen.** Verwenden Sie die Aktionen **Add Allow Entry** und **Add Deny Entry**, um den Zugriff auf Webinhalte basierend auf IPv4-Adressen oder Domänennamen des ISE-Knotens zuzulassen oder zu beschränken. Verwenden Sie die Aktion **Feature Settings** bearbeiten, um eine Standardzugriffsregel für nicht angegebene Clients zu definieren.

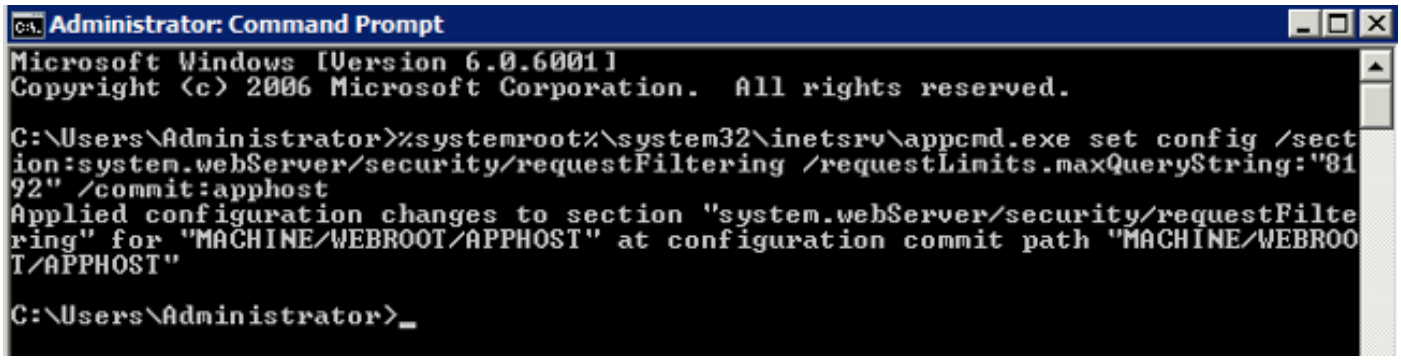


Erweitern der URL-Länge in IIS

ISE kann URLs generieren, die für den IIS-Webserver zu lang sind. Um dieses Problem zu vermeiden, kann die IIS-Standardkonfiguration so geändert werden, dass längere URLs zulässig sind. Geben Sie diesen Befehl über die CLI des NDES-Servers ein:

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

> **Hinweis:** Die Größe der Abfragezeichenfolge kann je nach ISE- und Endpunktkonfiguration variieren. Geben Sie diesen Befehl über die CLI des NDES-Servers mit Administratorberechtigungen ein.



Übersicht über Zertifikatsvorlagen

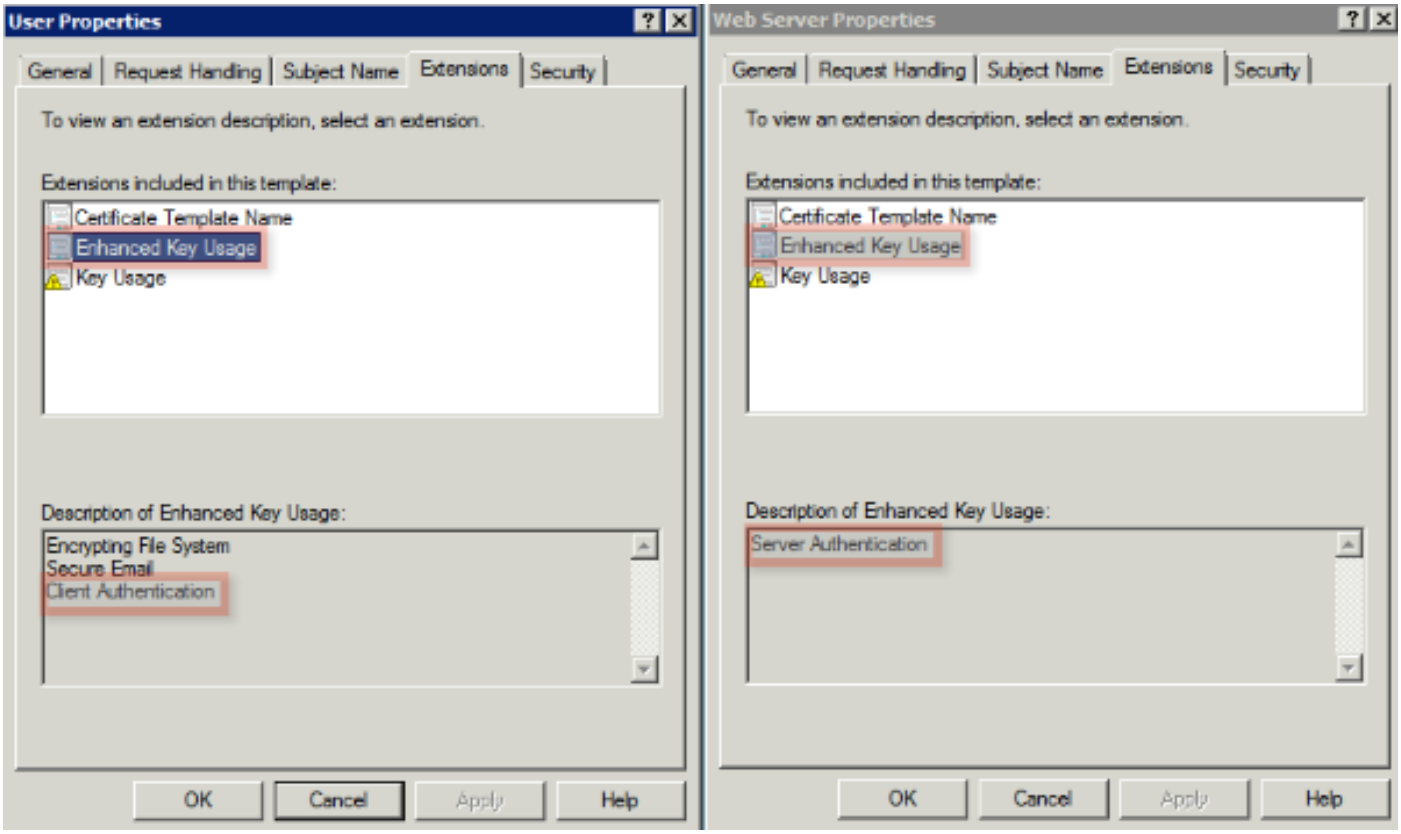
Administratoren einer Microsoft CA können eine oder mehrere Vorlagen konfigurieren, die verwendet werden, um Anwendungsrichtlinien auf einen gemeinsamen Satz von Zertifikaten anzuwenden. Mithilfe dieser Richtlinien können Sie ermitteln, für welche Funktion das Zertifikat und die zugehörigen Schlüssel verwendet werden. Die Werte der Anwendungsrichtlinien sind im Feld Extended Key Usage (EKU) des Zertifikats enthalten. Der Authentifizierer analysiert die Werte im EKU-Feld, um sicherzustellen, dass das vom Kunden präsentierte Zertifikat für die beabsichtigte Funktion verwendet werden kann. Zu den gängigsten Anwendungsbereichen

gehören Serverauthentifizierung, Client-Authentifizierung, IPSec VPN und E-Mail. Im Hinblick auf die ISE umfassen die am häufigsten verwendeten EKU-Werte die Server- und/oder Client-Authentifizierung.

Wenn Sie beispielsweise eine sichere Bank-Website aufrufen, wird der Webserver, der die Anforderung verarbeitet, mit einem Zertifikat konfiguriert, das über eine Anwendungsrichtlinie für die Serverauthentifizierung verfügt. Wenn der Server eine HTTPS-Anforderung empfängt, sendet er ein Serverauthentifizierungszertifikat zur Authentifizierung an den angeschlossenen Webbrowser. Der wichtige Punkt hierbei ist, dass es sich um einen unidirektionalen Austausch vom Server zum Client handelt. Im Zusammenhang mit der ISE wird ein Administrator-GUI-Zugriff häufig für ein Serverauthentifizierungszertifikat verwendet. Die ISE sendet das konfigurierte Zertifikat an den verbundenen Browser und erwartet nicht, dass das Zertifikat vom Client zurückgesendet wird.

Bei Services wie BYOD, die EAP-TLS verwenden, wird eine gegenseitige Authentifizierung bevorzugt. Um diesen bidirektionalen Zertifikataustausch zu aktivieren, muss die Vorlage, die zum Generieren des ISE-Identitätszertifikats verwendet wird, über eine Mindestanwendungsrichtlinie für die Serverauthentifizierung verfügen. Die Webserver-Zertifikatvorlage erfüllt diese Anforderung. Die Zertifikatsvorlage, die die Endpunktzertifikate generiert, muss eine Mindestanwendungsrichtlinie für die Clientauthentifizierung enthalten. Die Vorlage des Benutzerzertifikats erfüllt diese Anforderung. Wenn Sie die ISE für Services wie Inline Policy Enforcement Point (iPEP) konfigurieren, sollte die Vorlage zum Generieren des ISE-Serveridentitätszertifikats sowohl Client- als auch Server-Authentifizierungsattribute enthalten, wenn Sie ISE Version 1.1.x oder früher verwenden. Dadurch können sich die Admin- und Inline-Knoten gegenseitig authentifizieren. Die EKU-Validierung für iPEP wurde in ISE Version 1.2 entfernt, wodurch diese Anforderung weniger relevant wird.

Sie können die Microsoft CA-Standardwebserver- und Benutzervorlagen wiederverwenden oder mit dem in diesem Dokument beschriebenen Prozess eine neue Vorlage klonen und erstellen. Auf der Grundlage dieser Zertifikatsanforderungen sollten die CA-Konfiguration und die daraus resultierenden ISE- und Endgerätezertifikate sorgfältig geplant werden, um unerwünschte Konfigurationsänderungen bei der Installation in einer Produktionsumgebung zu minimieren.



Zertifikatvorlagenkonfiguration

Wie bereits in der Einführung erwähnt, wird SCEP häufig in IPSec VPN-Umgebungen verwendet. Durch die Installation der NDES-Rolle wird der Server automatisch für die Verwendung der **IPSec-**Vorlage **(Offline Request)** für SCEP konfiguriert. Aus diesem Grund besteht einer der ersten Schritte bei der Vorbereitung einer Microsoft CA für BYOD darin, eine neue Vorlage mit der richtigen Anwendungsrichtlinie zu erstellen. In einer Standalone-Bereitstellung werden die Zertifizierungsstelle und die NDES-Dienste auf demselben Server angeordnet, und die Vorlagen und erforderlichen Registrierungsänderungen sind auf demselben Server enthalten. In einer verteilten NDES-Bereitstellung werden die Registrierungsänderungen auf dem NDES-Server vorgenommen. Die eigentlichen Vorlagen werden jedoch auf dem in der NDES-Dienstinstallation angegebenen Root- oder Sub-Root-CA-Server definiert.

Gehen Sie wie folgt vor, um die Zertifikatvorlage zu konfigurieren:

1. Melden Sie sich als **admin** beim CA-Server an.

2. Klicken Sie auf **Start** > **Verwaltung** > **Zertifizierungsstelle**.

3. Erweitern Sie die CA-Serverdetails, und wählen Sie den Ordner **Zertifikatsvorlagen aus**. Dieser Ordner enthält eine Liste der Vorlagen, die derzeit aktiviert sind.

4. Um die Zertifikatsvorlagen zu verwalten, klicken Sie mit der rechten Maustaste auf den Ordner **Zertifikatsvorlagen** und wählen **Verwalten**.

5. In der **Konsole Zertifikatsvorlagen** werden eine Reihe inaktiver Vorlagen angezeigt.

6. Um eine neue Vorlage für die Verwendung mit SCEP zu konfigurieren, klicken Sie mit der rechten Maustaste auf eine bereits vorhandene Vorlage, z. B. **Benutzer**, und wählen Sie

Vorlage duplizieren aus.

7. Wählen Sie **Windows 2003** oder **Windows 2008 aus**, abhängig vom minimalen CA-Betriebssystem in der Umgebung.

8. Fügen Sie auf der Registerkarte **Allgemein** einen Anzeigenamen wie ISE-BYOD und die Gültigkeitsdauer hinzu. Lassen Sie alle anderen Optionen deaktiviert.
   Hinweis: Die Gültigkeitsdauer der Vorlage muss kleiner oder gleich der Gültigkeitsdauer der CA-Root- und Zwischenzertifikate sein.
9. Klicken Sie auf die Registerkarte **Betreffname**, und bestätigen Sie, dass **in der Anfrage** die Option **Angebot** ausgewählt ist.

10. Klicken Sie auf die Registerkarte Ausgabeanforderungen. Cisco empfiehlt, die **Richtlinien** für **die Ausgabe** in einer typischen hierarchischen CA-Umgebung leer zu lassen.

11. Klicken Sie auf die Registerkarte **Erweiterungen**, **Anwendungsrichtlinien**, und **bearbeiten Sie**.

12. Klicken Sie auf **Hinzufügen**, und stellen Sie sicher, dass die **Client-Authentifizierung** als Anwendungsrichtlinie hinzugefügt wird. Klicken Sie auf **OK**.

13. Klicken Sie auf die Registerkarte **Sicherheit** und anschließend auf **Hinzufügen...**. Stellen Sie sicher, dass das in der NDES-Dienstinstallation definierte SCEP-Dienstkonto über die vollständige Kontrolle über die Vorlage verfügt, und klicken Sie dann auf **OK**.

14. Kehren Sie zur **GUI-**Schnittstelle **der Zertifizierungsstelle zurück**.

15. Klicken Sie mit der rechten Maustaste auf das Verzeichnis **Zertifikatsvorlagen**. Navigieren Sie zu **Neu > Zertifikatvorlage zur Ausgabe**.

16. Wählen Sie die zuvor konfigurierte **ISE-BYOD-**Vorlage aus und klicken Sie auf **OK**.

    Hinweis: Alternativ können Sie die Vorlage über die CLI mit dem Befehl **certutil -SetCAtemplate +ISE-BYOD** aktivieren.
    Die ISE-BYOD-Vorlage sollte nun in der Liste der aktivierten Zertifikatsvorlagen aufgeführt werden.

Registrierungskonfiguration für Zertifikatsvorlage

Gehen Sie wie folgt vor, um die Registrierungsschlüssel für die Zertifikatsvorlage zu konfigurieren:

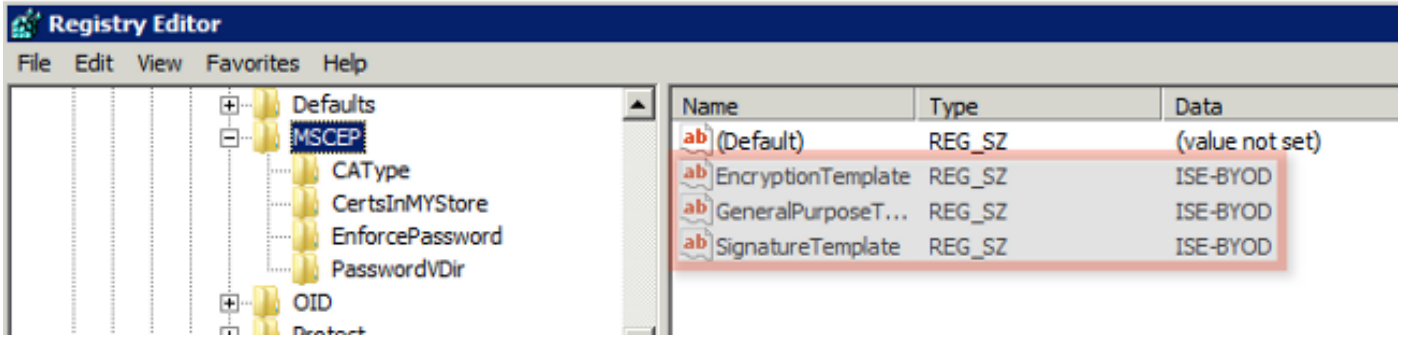
1. Stellen Sie eine Verbindung zum NDES-Server her.

2. Klicken Sie auf **Start** und geben Sie **regedit** in die Suchleiste ein.

3. Navigieren Sie zu **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP.**

4. Ändern Sie die **EncryptionTemplate**-, **GeneralPurposeTemplate**- und **SignatureTemplate**-Schlüssel von **IPSec (Offline Request)** in die **zuvor erstellte ISE-BYOD-Vorlage.**

5. Starten Sie den NDES-Server neu, um die Registrierungseinstellung anzuwenden.



Konfigurieren der ISE als SCEP-Proxy

Bei einer BYOD-Bereitstellung kommuniziert das Endgerät nicht direkt mit dem Back-End-NDES-Server. Stattdessen wird der ISE-Richtlinienknoten als SCEP-Proxy konfiguriert und kommuniziert mit dem NDES-Server im Namen der Endpunkte. Die Endpunkte kommunizieren direkt mit der ISE. Die IIS-Instanz auf dem NDES-Server kann so konfiguriert werden, dass sie HTTP- und/oder HTTPS-Bindungen für die virtuellen SCEP-Verzeichnisse unterstützt.

Gehen Sie wie folgt vor, um die ISE als SCEP-Proxy zu konfigurieren:

1. Melden Sie sich mit Administratorberechtigungen bei der **ISE-GUI an**.

2. Klicken Sie auf **Administration**, **Certificates** und dann **SCEP CA Profiles**.

3. Klicken Sie auf **Hinzufügen**.

4. Geben Sie den Servernamen und die Beschreibung ein.

5. Geben Sie die URL für den SCEP-Server mit dem IP-Namen oder dem FQDN (Fully Qualified Domain Name, z. B. http://10.10.10.10/certsrv/mscep/) ein.

6. Klicken Sie auf **Verbindung testen**. Eine erfolgreiche Verbindung führt zu einer erfolgreichen Popup-Meldung für die Serverantwort.

7. Klicken Sie auf **Speichern**, um die Konfiguration zu übernehmen.

8. Klicken Sie zum Überprüfen auf **Administration**, **Certificates**, **Certificate Store,** und bestätigen Sie, dass das SCEP NDES Server RA-Zertifikat automatisch auf den ISE-Knoten heruntergeladen wurde.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

In diesem Abschnitt finden Sie Fehlerbehebungen für Ihre Konfiguration.

Allgemeine Hinweise zur Fehlerbehebung

Im Folgenden finden Sie eine Liste wichtiger Hinweise, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können:

- Unterteilen Sie die BYOD-Netzwerktopologie in logische Wegpunkte, um Debug- und Erfassungspunkte entlang des Pfads zwischen den ISE-, NDES- und CA-Endpunkten zu identifizieren.
- Stellen Sie sicher, dass der ISE-Knoten und die CA eine gemeinsame NTP-Zeitquelle (Network Time Protocol) verwenden.
- Endpunkte sollten ihre Zeit automatisch mit den vom DHCP bezogenen NTP- und Zeitzonenoptionen einstellen können.
- Der DNS-Server des Clients muss in der Lage sein, den FQDN des ISE-Knotens aufzulösen.
- Stellen Sie sicher, dass TCP 80 und/oder TCP 443 bidirektional zwischen ISE und dem NDES-Server zugelassen sind.
- Testen Sie mit einem Windows-Computer, da die clientseitige Protokollierung verbessert wurde. Verwenden Sie optional ein Apple iDevice zusammen mit dem Apple iPhone Configuration Utility, um clientseitige Konsolenprotokolle zu überwachen.
- Überwachen Sie die CA- und NDES-Serveranwendungsprotokolle auf Registrierungsfehler, und verwenden Sie Google oder TechNet, um diese Fehler zu untersuchen.
- Verwenden Sie während der Testphase HTTP für SCEP, um die Paketerfassung zwischen ISE, NDES und CA zu vereinfachen.
- Verwenden Sie das TCP-Dump-Dienstprogramm auf dem ISE Policy Service Node (PSN), und überwachen Sie den Datenverkehr zum und vom NDES-Server. Diese finden Sie unter **Operations > Diagnostic Tools > General Tools**.
- Installieren Sie Wireshark auf dem CA- und NDES-Server, oder verwenden Sie SPAN auf zwischengeschalteten Switches, um SCEP-Datenverkehr zum und vom ISE PSN zu erfassen.
- Stellen Sie sicher, dass die entsprechende Zertifizierungsstellenkette der Zertifizierungsstelle auf dem ISE-Richtlinienknoten für die Authentifizierung der Client-Zertifikate installiert ist.
- Stellen Sie sicher, dass die entsprechende Zertifizierungsstellenkette automatisch beim Onboarding auf den Clients installiert wird.

- Überprüfen Sie die ISE- und Endpunkt-Identitätszertifikate, und stellen Sie sicher, dass die richtigen EKU-Attribute vorhanden sind.

- Überwachen Sie die Live-Authentifizierungsprotokolle in der ISE-GUI auf Authentifizierungs- und Autorisierungsfehler.
  Hinweis: Einige Supplicants initialisieren keinen Austausch von Client-Zertifikaten, wenn die falsche EKU vorhanden ist, wie z.B. ein Client-Zertifikat mit EKU der Serverauthentifizierung. Authentifizierungsfehler sind daher möglicherweise nicht immer in den ISE-Protokollen vorhanden.
- Wenn NDES in einer verteilten Bereitstellung installiert wird, wird in der Dienstinstallation eine Remote-Root- oder Sub-Root-CA durch CA Name (CA-Name) oder Computername bestimmt. Der NDES-Server sendet Anfragen zur Zertifikatsregistrierung an diesen Ziel-CA-Server. Wenn der Registrierungsvorgang für Endpunktzertifikate fehlschlägt, zeigen die Paketerfassungen (PCAP) möglicherweise an, dass der NDES-Server einen Fehler **404 Not Found** an den ISE-Knoten zurückgibt. Um dieses Problem zu beheben, installieren Sie den NDES-Service neu, und wählen Sie die Option Computername anstelle des CA-Namens aus.

- Vermeiden Sie Änderungen an der SCEP CA-Kette, nachdem Geräte integriert wurden. Endgeräte-Betriebssysteme wie Apple iOS aktualisieren nicht automatisch ein zuvor installiertes BYOD-Profil. In diesem iOS-Beispiel muss das aktuelle Profil vom Endpunkt gelöscht und der Endpunkt aus der ISE-Datenbank entfernt werden, damit das Onboarding erneut durchgeführt werden kann.

- Sie können einen Microsoft-Zertifikatsserver konfigurieren, um eine Verbindung zum Internet herzustellen, und automatisch Zertifikate aus dem Microsoft Root Certificate-Programm aktualisieren. Wenn Sie diese Option für den Netzwerkabruf in Umgebungen mit eingeschränkten Internet-Richtlinien konfigurieren, können CA/NDES-Server, die keine Verbindung zum Internet herstellen können, standardmäßig 15 Sekunden bis zum Timeout dauern. Dadurch kann die Verarbeitung von SCEP-Anfragen von SCEP-Proxys wie ISE um 15 Sekunden verzögert werden. Die ISE wird so programmiert, dass SCEP-Anfragen nach 12 Sekunden deaktiviert werden, wenn keine Antwort empfangen wird. Um dieses Problem zu beheben, erlauben Sie entweder den Internetzugriff für die CA/NDES-Server oder ändern Sie die Zeitüberschreitungseinstellungen für den Netzwerkabruf in der lokalen Sicherheitsrichtlinie der Microsoft CA/NDES-Server. Um diese Konfiguration auf dem Microsoft-Server zu finden, wählen Sie **Start > Verwaltung > Lokale Sicherheitsrichtlinie > Richtlinien für öffentlichen Schlüssel > Einstellungen für die Zertifikatspfadvalidierung > Netzwerkabruf aus**.

Clientseitige Protokollierung

Im Folgenden finden Sie eine Liste nützlicher Techniken, mit denen Probleme bei der clientseitigen Protokollierung behoben werden können:

- Geben Sie **Log %temp%\spwProfileLog.txt ein.** um die clientseitigen Protokolle für Microsoft Windows-Anwendungen anzuzeigen.
  Hinweis: WinHTTP wird für die Verbindung zwischen dem Microsoft Windows-Endpunkt und der ISE verwendet. Eine Liste von Fehlercodes finden Sie im Artikel Microsoft Windows-Fehlermeldungen.
- Geben Sie den Befehl **/sdcards/downloads/spw.log** ein, um die clientseitigen Protokolle für

Android-Anwendungen anzuzeigen.

- Für **MAC OSX** verwenden Sie die Konsolenanwendung und suchen Sie nach dem **SPW-**Prozess.
- Für **Apple iOS** verwenden Sie Apple Configurator 2.0, um Nachrichten anzuzeigen.

ISE-Protokollierung

Gehen Sie wie folgt vor, um das ISE-Protokoll anzuzeigen:

1. Navigieren Sie zu **Administration > Logging > Debug Log Configuration**, und wählen Sie den entsprechenden ISE-Richtlinienknoten aus.
2. Legen Sie die **Client-** und **Bereitstellungsprotokolle** je nach Bedarf auf Debuggen oder Nachverfolgung fest.
3. Reproduzieren Sie das Problem, und dokumentieren Sie relevante Seed-Informationen, um die Suche zu vereinfachen, z. B. MAC, IP und Benutzer.
4. Navigieren Sie zu **Operations > Download Logs**, und wählen Sie den entsprechenden ISE-Knoten aus.
5. Laden Sie auf der Registerkarte **Debug Logs** die Protokolle mit dem Namen **ise-psc.log** auf den Desktop herunter.
6. Verwenden Sie einen intelligenten Editor, z. B. Notepad ++, um die Protokolldateien zu analysieren.
7. Wenn das Problem isoliert wurde, setzen Sie die Protokollstufen auf die Standardstufe zurück.

NDES-Protokollierung und Fehlerbehebung

Weitere Informationen finden Sie im AD CS: Fehlerbehebung für den Network Device Enrollment Service Windows Server-Artikel.

Zugehörige Informationen

- BYOD-Lösungsleitfaden - Certificate Authority Server-Konfiguration
- NDES-Übersicht in Windows 2008 R2
- MSCEP-Whitepaper
- Konfigurieren des NDES-Servers zur Unterstützung von SSL
- Zertifizierungsanforderungen bei der Verwendung von EAP-TLS oder PEAP mit EAP-TLS
- Technischer Support und Dokumentation