Konfigurieren der HTTPS-Unterstützung für ISE SCEP-Integration

Inhalt

Einführung

In diesem Dokument werden die Schritte beschrieben, die zur Konfiguration der Hypertext Transfer Protocol Secure (HTTPS)-Unterstützung für die Integration des Secure Certificate Enrollment Protocol (SCEP) in die Identity Services Engine (ISE) erforderlich sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse des Internetinformationsdienste-Webservers (IIS) von Microsoft
- Erfahrung in der Konfiguration von SCEP und Zertifikaten auf ISE

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ISE Version 1.1.x

- Windows Server 2008 R2 Enterprise mit Hotfixen für installierte KB2483564 und KB2633200

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Die Informationen zu Microsoft-Zertifikatsdiensten werden als Leitfaden speziell für Cisco Bring Your Own Device (BYOD) bereitgestellt. Weitere Informationen finden Sie im Microsoft TechNet als Quelle der Wahrheit für Microsoft-Zertifizierungsstellen, Network Device Enrollment Service (NDES) und SCEP-bezogene Serverkonfigurationen.

Hintergrundinformationen

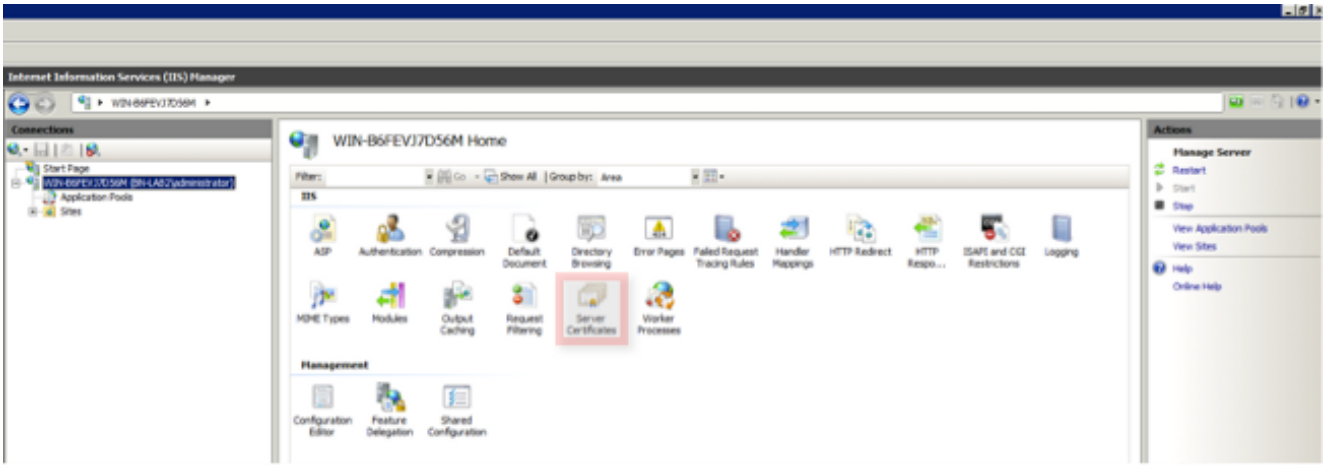
Bei einer BYOD-Bereitstellung ist eine der Kernkomponenten ein Microsoft 2008 R2 Enterprise-Server, auf dem die NDES-Rolle installiert ist. Dieser Server ist Teil des Active Directory-Waldes (AD). Während der Erstinstallation von NDES wird der IIS-Webserver von Microsoft automatisch installiert und konfiguriert, um die HTTP-Beendigung des SCEP zu unterstützen. In einigen BYOD-Bereitstellungen möchten Kunden möglicherweise die Kommunikation zwischen ISE und NDES mithilfe von HTTPS weiter sichern. In diesem Verfahren werden die erforderlichen Schritte zum Anfordern und Installieren eines SSL-Zertifikats (Secure Socket Layer) für die SCEP-Website beschrieben.

Konfigurieren

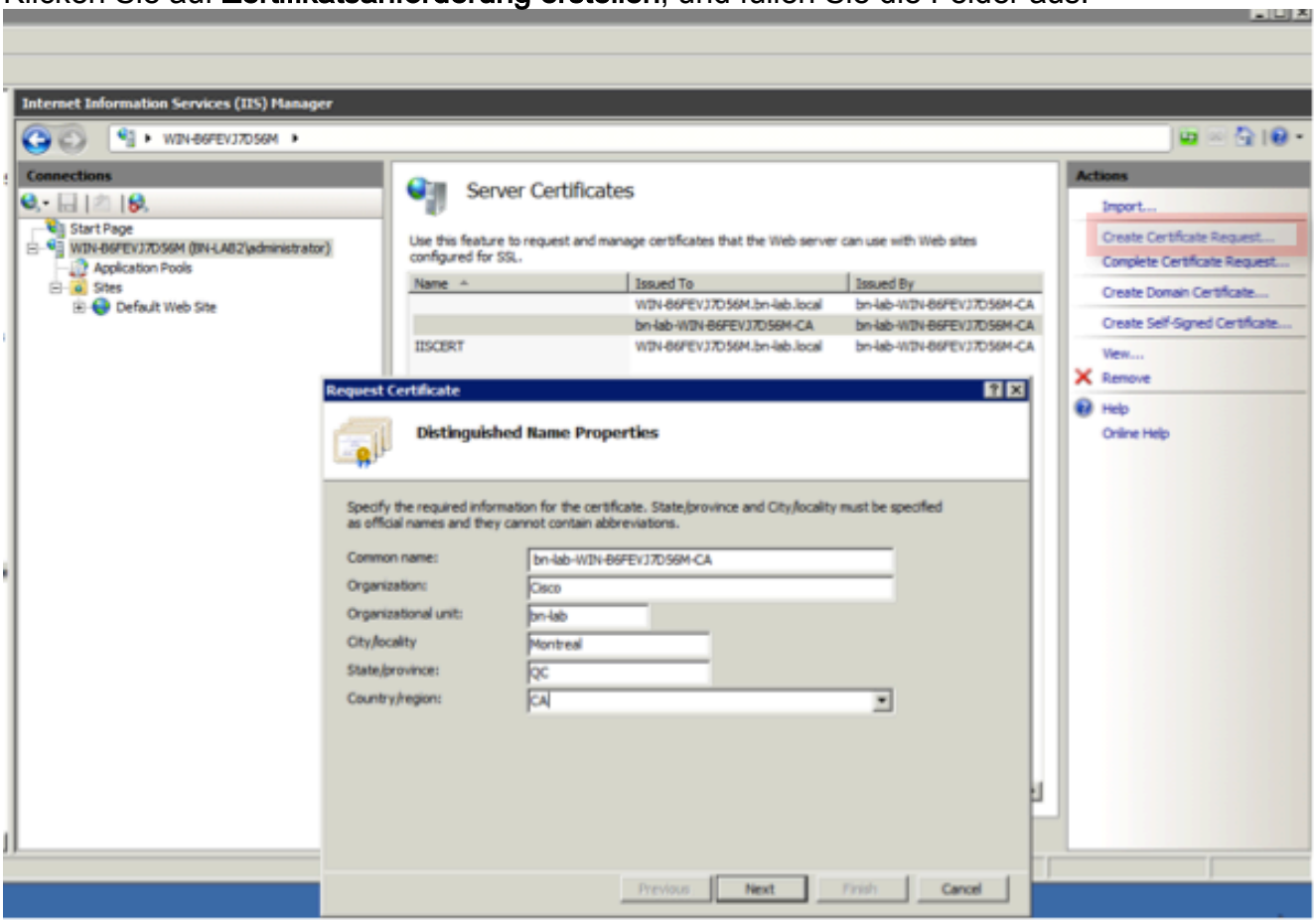
NDES-Serverzertifikatkonfiguration

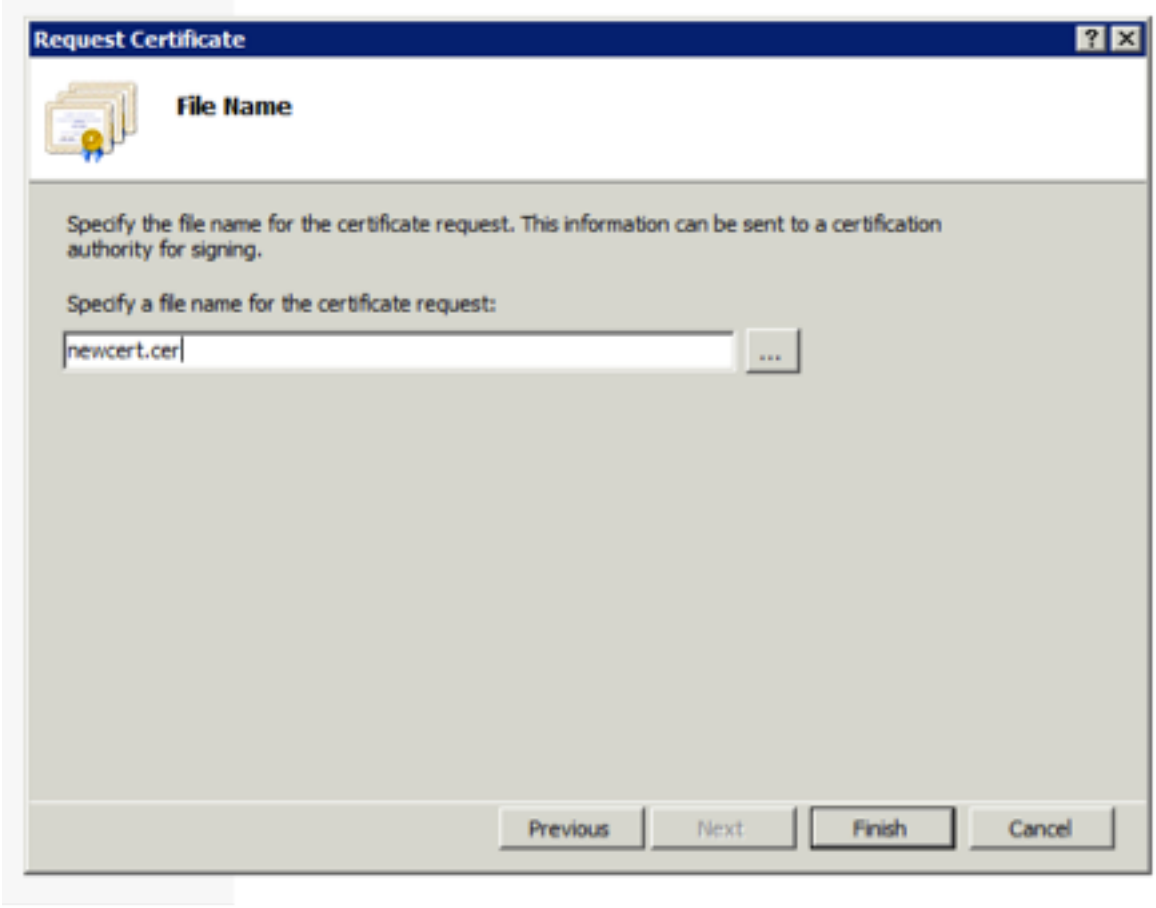
> **Hinweis**: Sie müssen ein neues Zertifikat für IIS konfigurieren (nur erforderlich, wenn IIS in eine PKI eines Drittanbieters wie Verisign integriert ist oder wenn die CA- und NDES-Serverrollen auf separate Server aufgeteilt werden). Wenn sich die NDES-Rolle bei der Installation auf einem aktuellen Microsoft CA-Server befindet, verwendet IIS das beim Einrichten der CA erstellte Serveridentitätszertifikat. Bei Standalone-Konfigurationen wie diesen können Sie direkt zum Abschnitt **NDES-Server IIS Binding Configuration** in diesem Dokument wechseln.

1. Herstellen einer Verbindung zum NDES-Server über Konsole oder RDP.
2. Klicken Sie auf **Start -> Verwaltung -> Internetinformationsdienste (IIS)-Manager**.
3. Markieren Sie den IIS-Servernamen, und klicken Sie auf das Symbol **Serverzertifikate**.

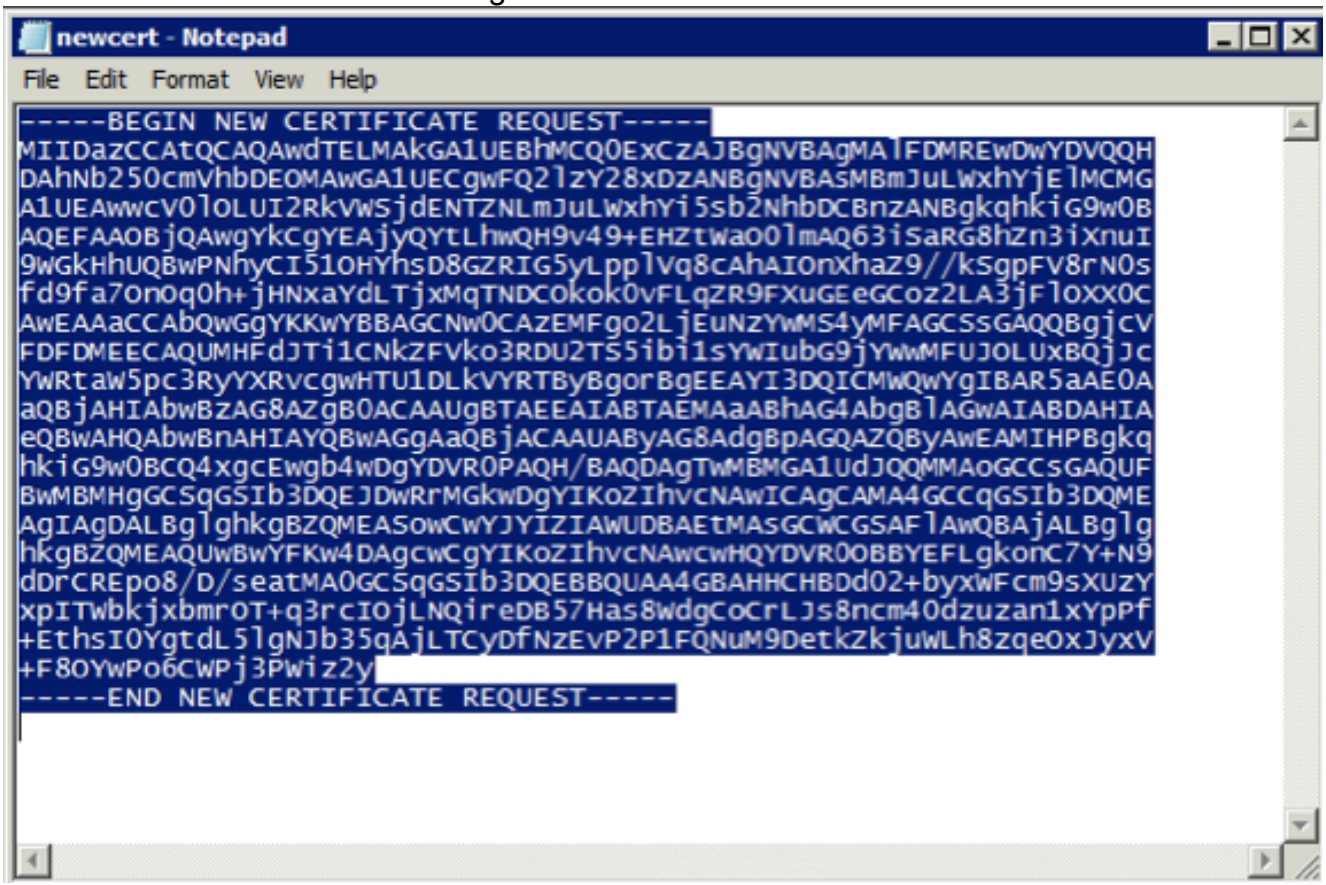


4. Klicken Sie auf **Zertifikatsanforderung erstellen**, und füllen Sie die Felder aus.

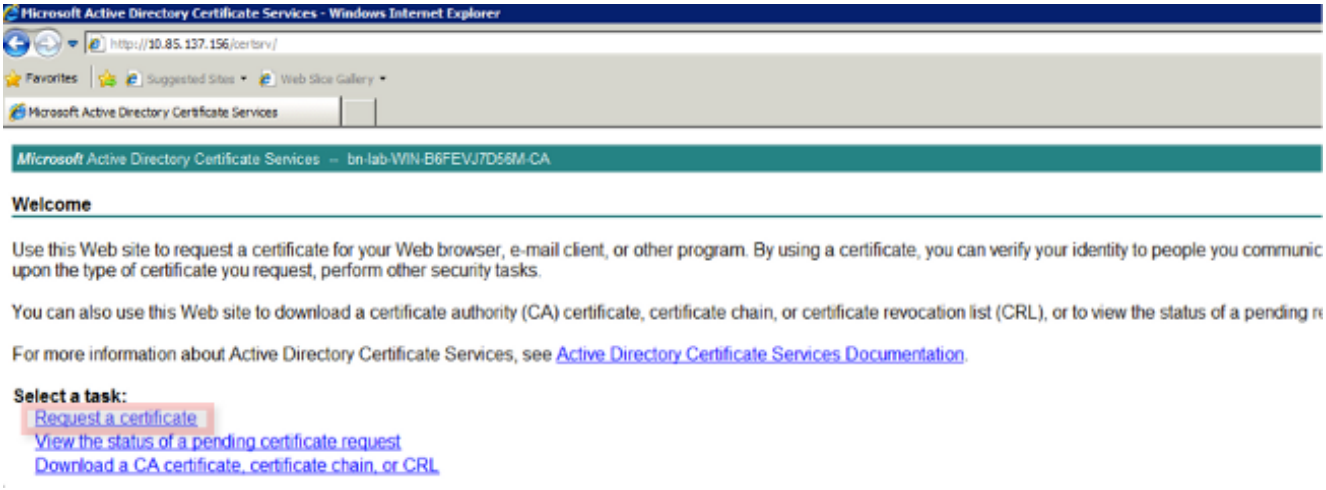




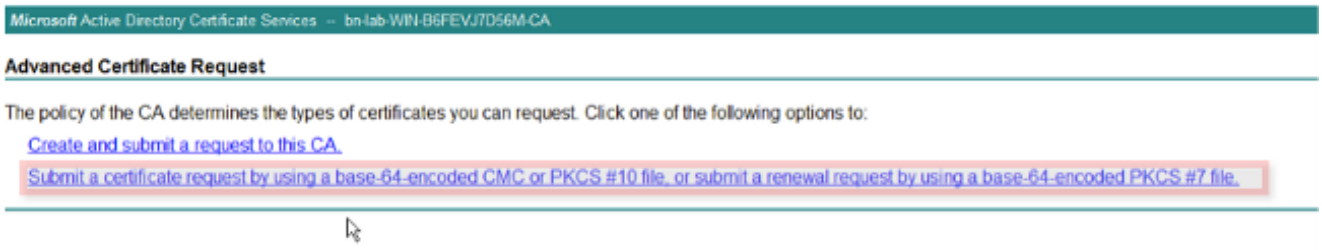
5. Öffnen Sie die im vorherigen Schritt erstellte Cer-Datei mit einem Texteditor, und kopieren Sie den Inhalt in die Zwischenablage.



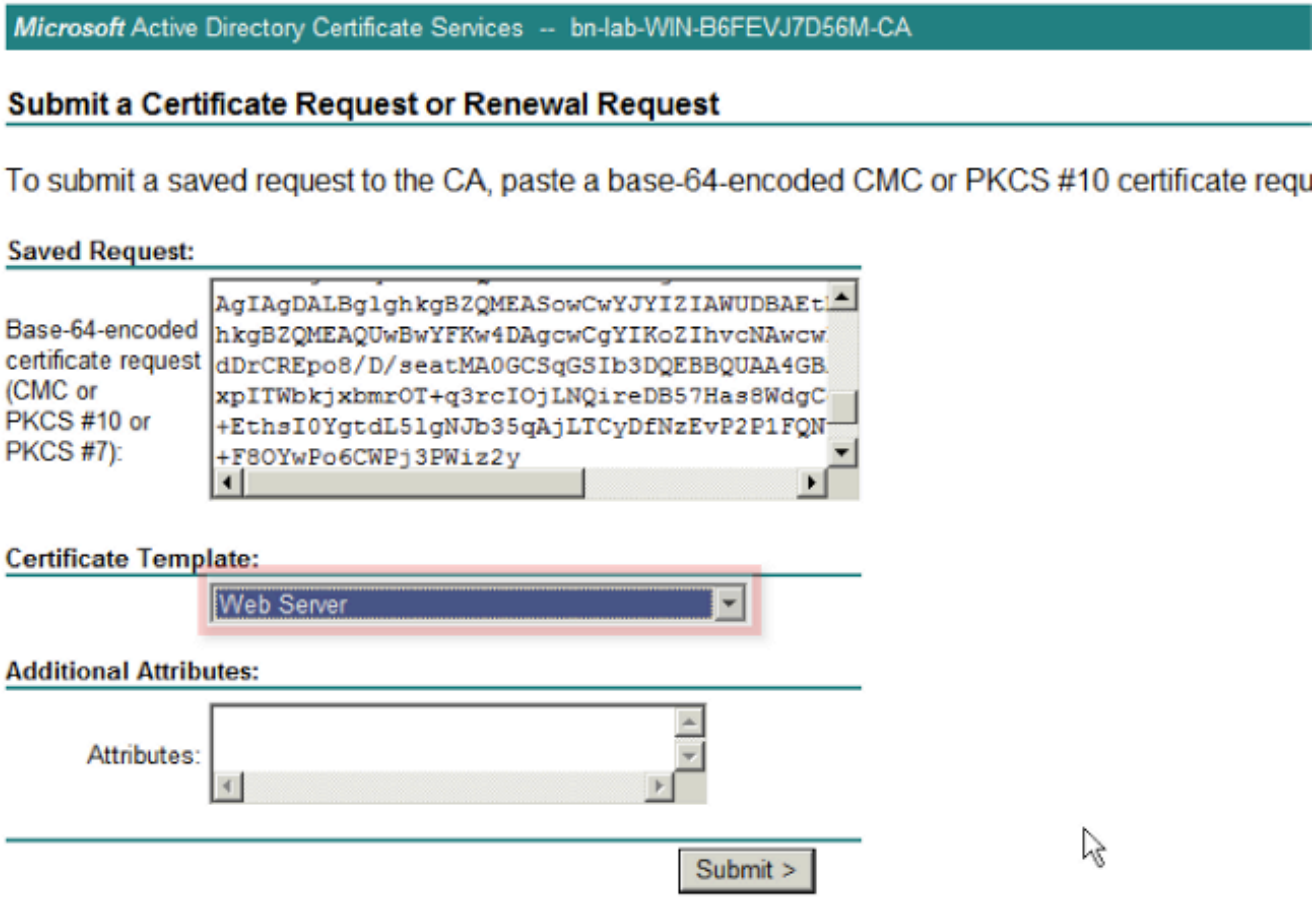
6. Rufen Sie die Microsoft CA Web Enrollment-Website auf, und klicken Sie auf **Zertifikat anfordern**.Beispiel-URL: http://yourCAIP/certsrv



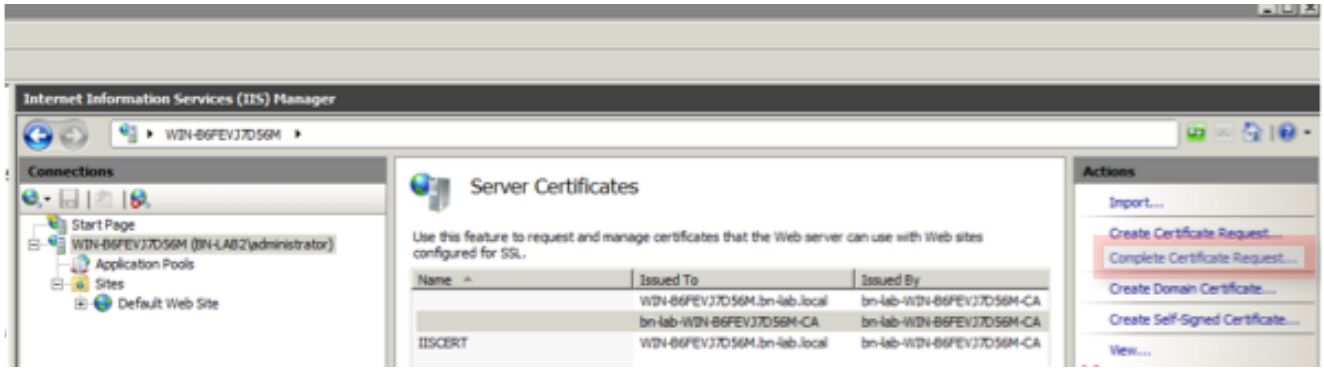
7. Klicken Sie auf **Zertifikatsanforderung senden mit...**. Fügen Sie den Zertifikatsinhalt aus der Zwischenablage ein, und wählen Sie die **Webserver**-Vorlage aus.



8. Klicken Sie auf **Senden**, und speichern Sie die Zertifikatsdatei auf dem Desktop.

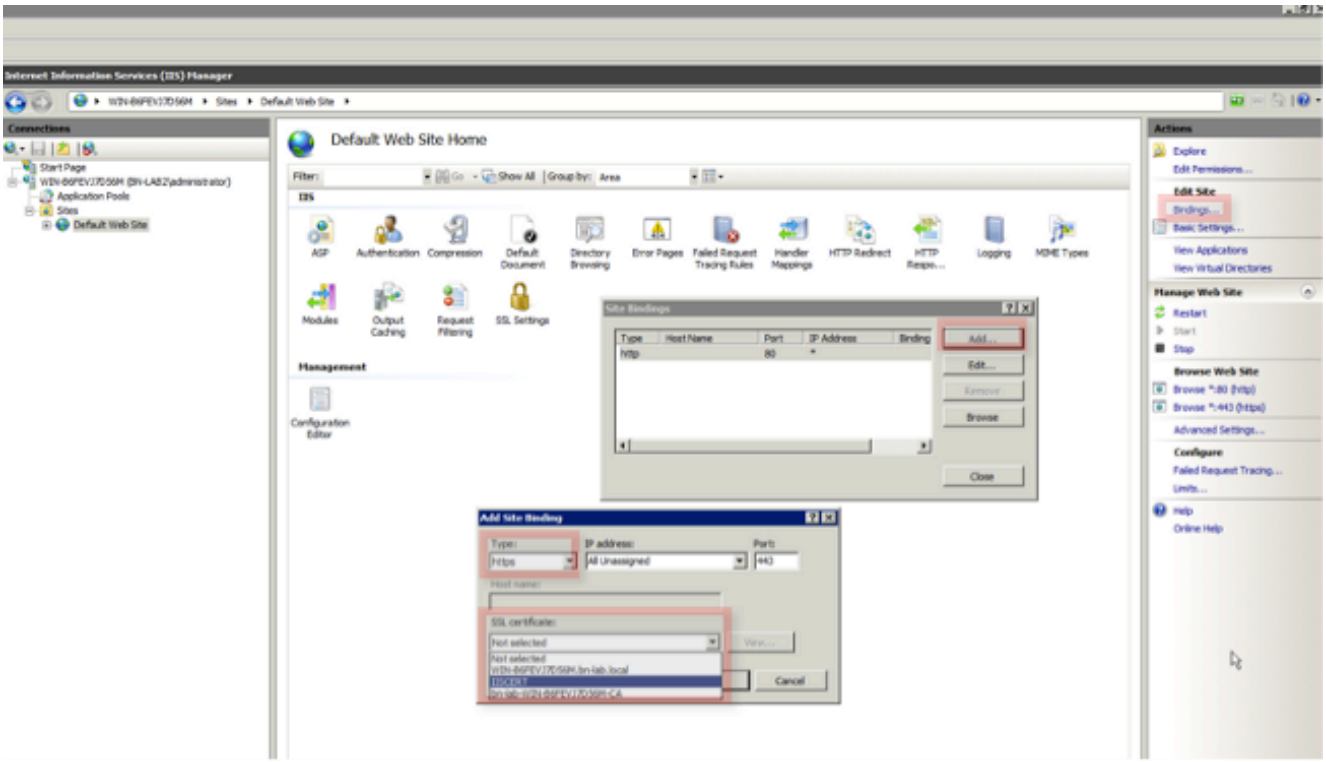


9. Kehren Sie zum NDES-Server zurück, und öffnen Sie das IIS-Manager-Dienstprogramm. Klicken Sie auf den Servernamen und anschließend auf **Zertifikatsanforderung abschließen**, um das neu erstellte Serverzertifikat zu importieren.



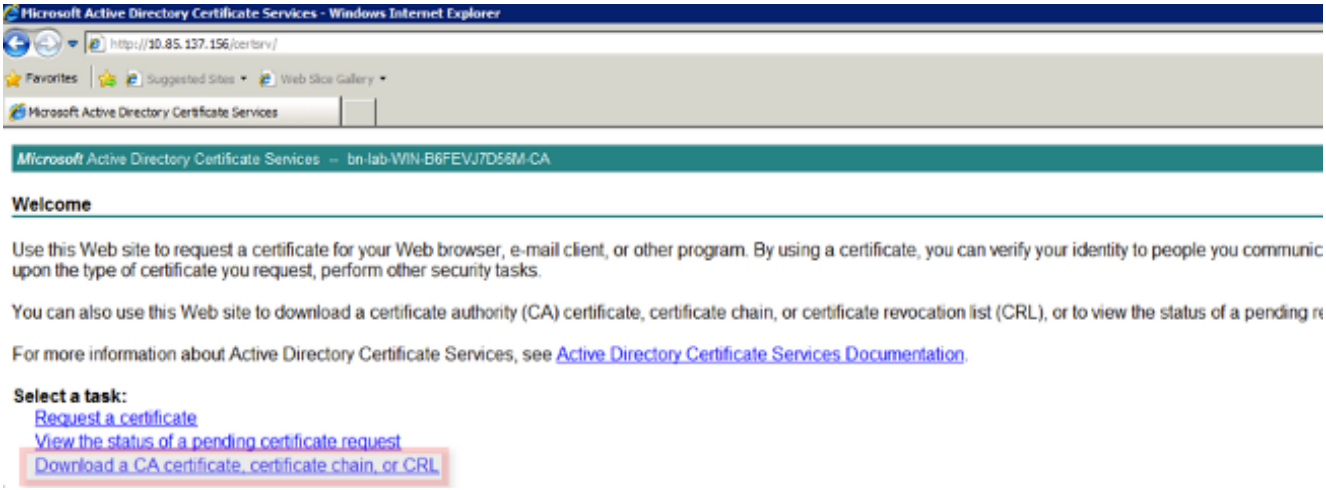
IIS-Bindungskonfiguration des NDES-Servers

1. Erweitern Sie den **Servernamen**, erweitern Sie **Sites**, und klicken Sie auf **Standardwebsite**.
2. Klicken Sie in der rechten oberen Ecke auf **Bindungen**.
3. Klicken Sie auf **Hinzufügen**, ändern Sie den Typ in HTTPS, und wählen Sie das Zertifikat aus der Dropdown-Liste aus.
4. Klicken Sie auf **OK.**

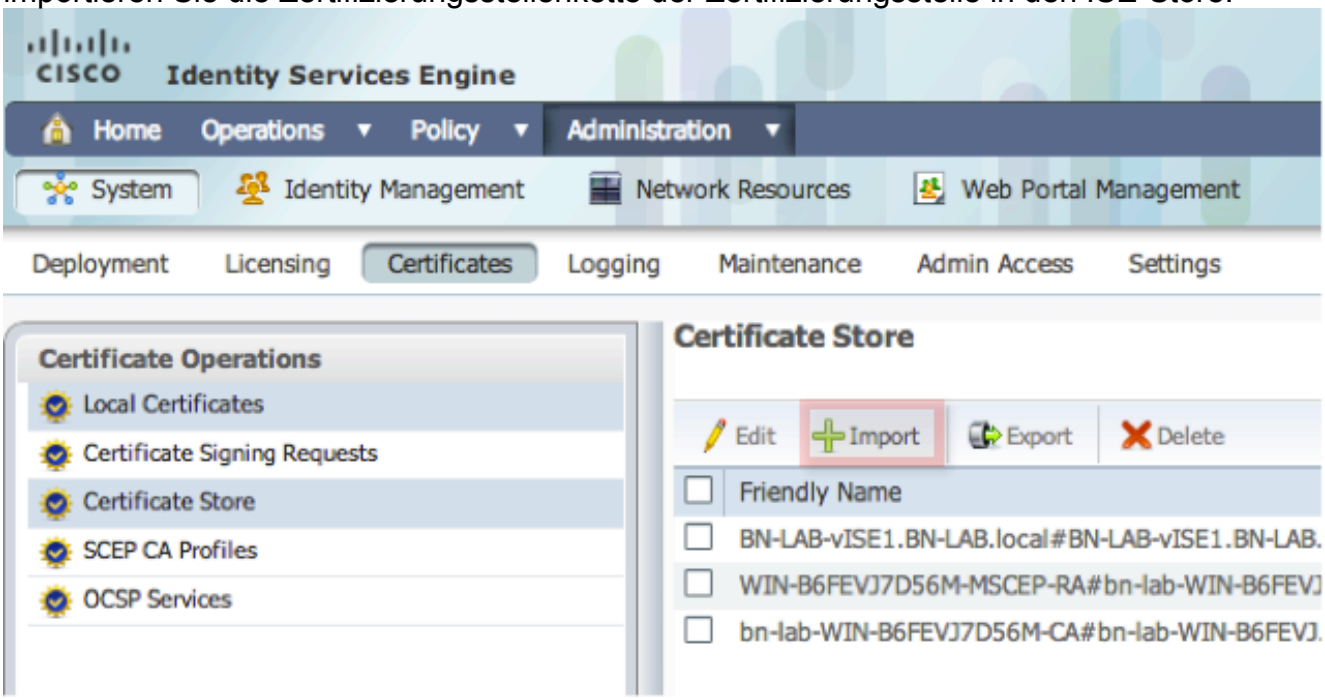


ISE-Serverkonfiguration

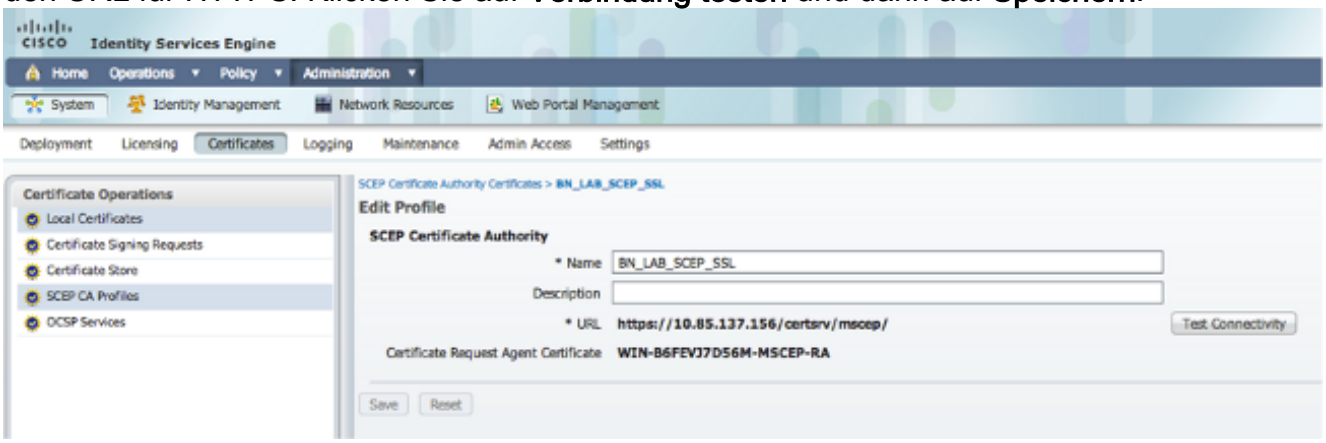
1. Stellen Sie eine Verbindung zur Web Enrollment-Schnittstelle des CA-Servers her, und laden Sie die Zertifizierungsstellenkette herunter.



2. Navigieren Sie in der ISE-GUI zu **Administration -> Certificates -> Certificate Store**, und importieren Sie die Zertifizierungsstellenkette der Zertifizierungsstelle in den ISE-Store.



3. Navigieren Sie zu **Administration -> Certificates -> SCEP CA Profiles**, und konfigurieren Sie den URL für HTTPS. Klicken Sie auf **Verbindung testen** und dann auf **Speichern**.



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- Navigieren Sie zu **Administration -> Certificates -> Certificate** Store, und überprüfen Sie, ob

die Zertifizierungsstellenkette der Zertifizierungsstelle und das Zertifikat der NDES Server Registration Authority (RA) vorhanden sind.
- Verwenden Sie Wireshark oder TCP Dump, um den ersten SSL-Austausch zwischen dem ISE-Admin-Knoten und dem NDES-Server zu überwachen.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Unterteilen Sie die BYOD-Netzwerktopologie in logische Wegpunkte, um Debug- und Erfassungspunkte entlang des Pfads zwischen diesen Endpunkten - ISE, NDES und CA - zu identifizieren.
- Stellen Sie sicher, dass TCP 443 bidirektional zwischen der ISE und dem NDES-Server zugelassen ist.
- Überwachen Sie die CA- und NDES-Serveranwendungsprotokolle auf Registrierungsfehler, und verwenden Sie Google oder TechNet, um diese Fehler zu untersuchen.
- Verwenden Sie das TCP-Dump-Dienstprogramm auf dem ISE-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 NDES-Server, oder verwenden Sie SPAN auf zwischengeschalteten Switches, um SCEP-Datenverkehr vom und zum ISE-PSN zu erfassen.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

> **Hinweis**: Bevor Sie **Debug-**Befehle verwenden, lesen Sie die wichtigen Informationen zu Debug-Befehlen.

Zugehörige Informationen

- **Konfigurieren der SCEP-Unterstützung für BYOD**
- **Technischer Support und Dokumentation - Cisco Systems**