Configure HTTPS Support for ISE SCEP Integration

Document ID: 116238

Contributed by Todd Pula and Sylvain Levesque, Cisco TAC Engineers.
Jul 31, 2013

Contents

Introduction

This document describes the steps required to configure Hypertext Transfer Protocol Secure (HTTPS) support for Secure Certificate Enrollment Protocol (SCEP) integration with the Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Microsoft's Internet Information Services (IIS) web server
- Experience in the configuration of SCEP and certificates on ISE

Components Used

The information in this document is based on these software and hardware versions:

- ISE Release 1.1.x
- Windows Server 2008 R2 Enterprise with hotfixes for ***KB2483564*** and ***KB2633200*** installed

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.

The information related to Microsoft certificate services is provided as a guide specifically for Cisco Bring Your Own Device (BYOD). Refer to Microsoft's TechNet as the definitive source of truth for Microsoft certification authority, Network Device Enrollment Service (NDES), and SCEP related server configurations.

Background Information

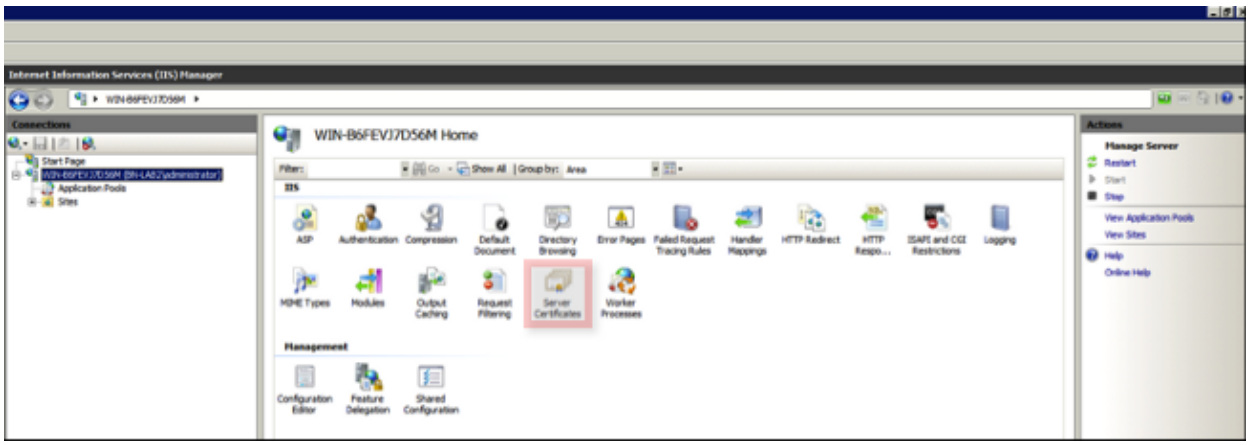
In a BYOD deployment, one of the core components is a Microsoft 2008 R2 Enterprise server that has the NDES role installed. This server is a member of the Active Directory (AD) forest. During the initial installation of NDES, Microsoft's IIS web server is automatically installed and configured to support HTTP termination of SCEP. In some BYOD deployments, customers might want to further secure the communications between ISE and NDES using HTTPS. This procedure details the steps required to request and install a Secure Socket Layer (SSL) certificate for the SCEP website.

Configure

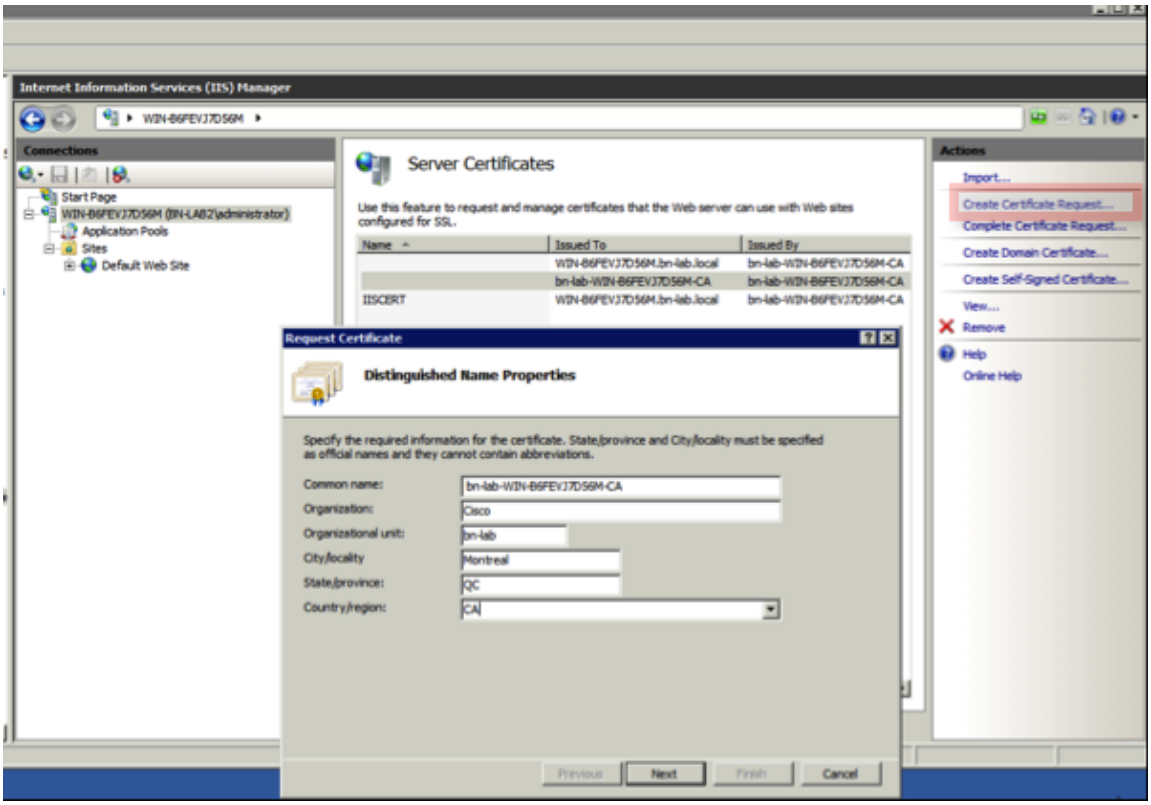
NDES Server Certificate Configuration

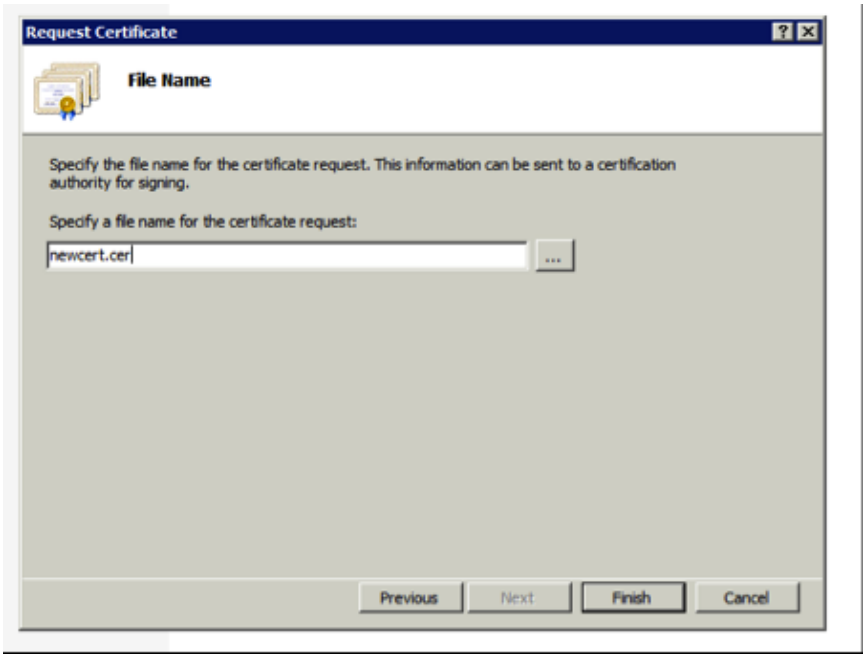
Note: You must configure a new certificate for IIS (only required when IIS is integrated with a 3rd party PKI such as Verisign or when the Certification Authority (CA) and NDES server roles are separated onto separate servers). In the install, if the NDES role is on an current Microsoft CA server, IIS uses the server identity certificate created during the CA setup. For standalone configurations such as this, skip directly to the ***NDES Server IIS Binding Configuration*** section in this document.

1. Connect to the NDES server via console or RDP.
2. Click ***Start -> Administrative Tools -> Internet Information Services (IIS) Manager***.
3. Highlight the IIS server name and click the ***Server Certificates*** icon.

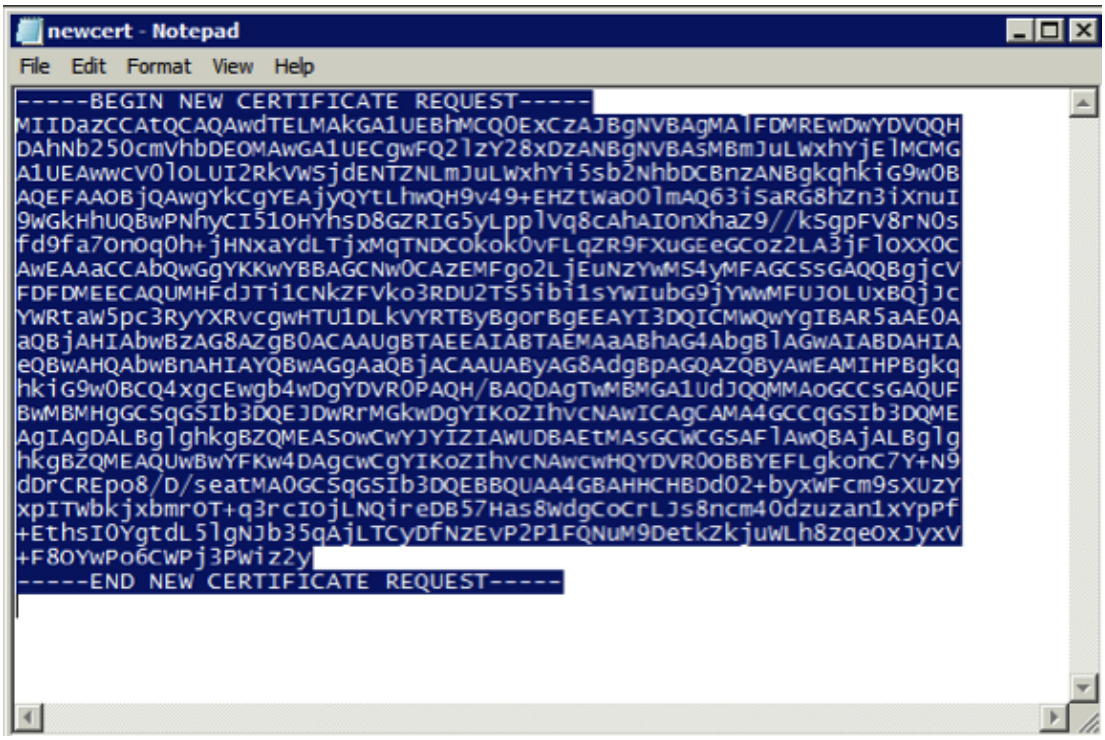


4. Click on ***Create Certificate Request***, and complete the fields.



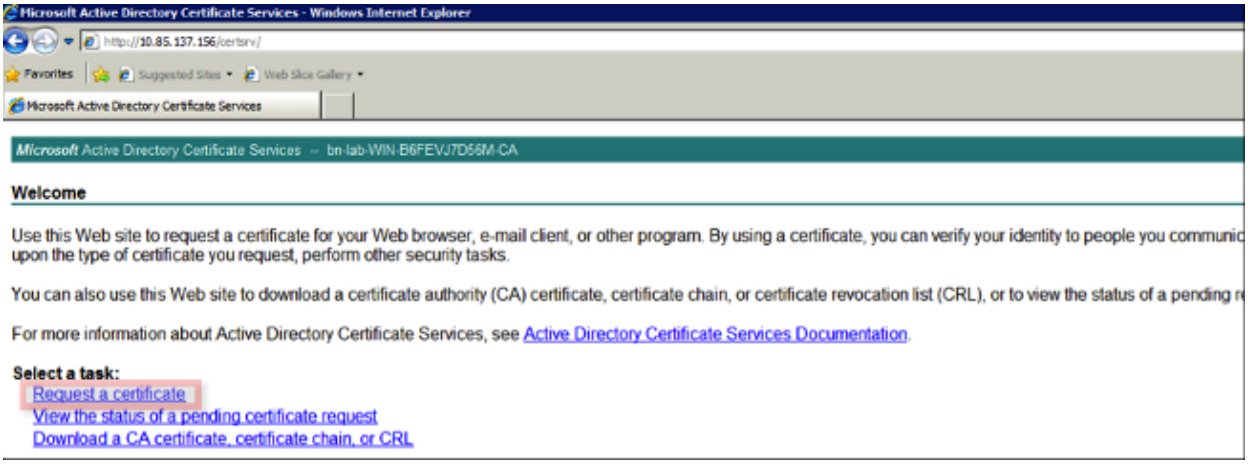


5. Open the .cer file created in the previous step with a text editor and copy the content to the clipboard.

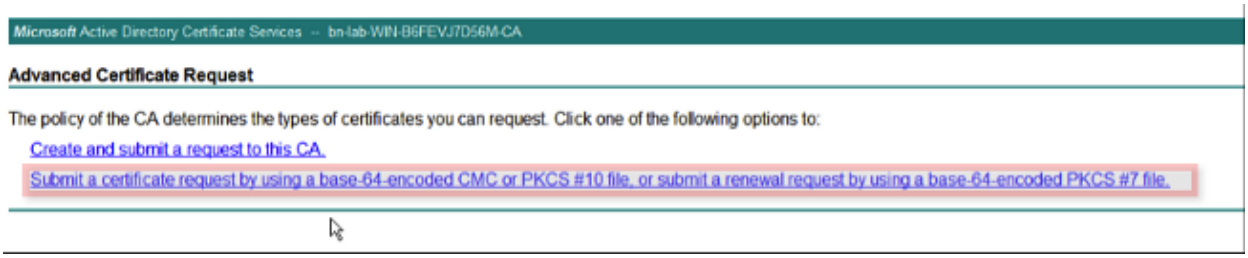


6. Access the Microsoft CA Web Enrollment website and click ***Request a Certificate***.

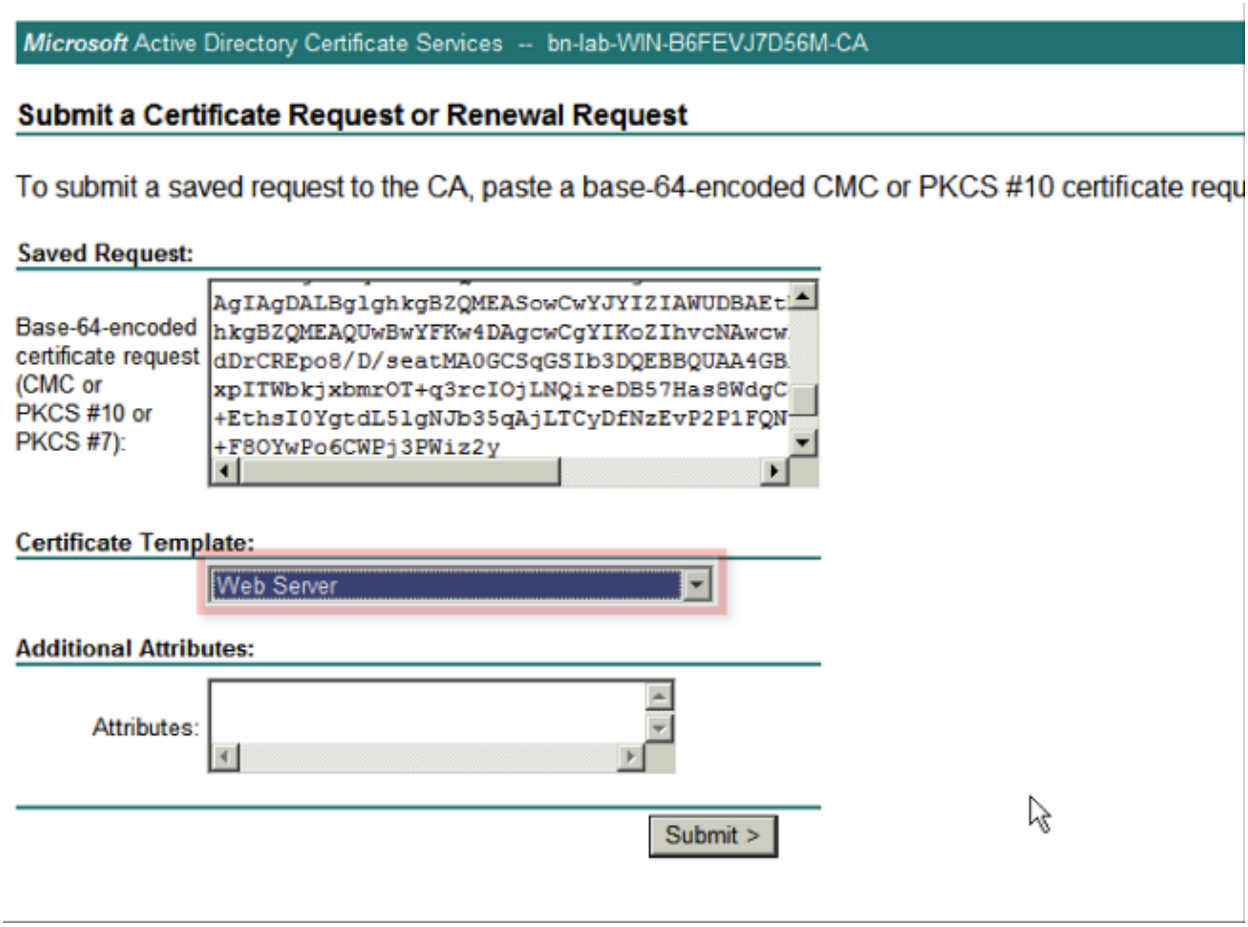
   Example URL: http://yourCAIP/certsrv



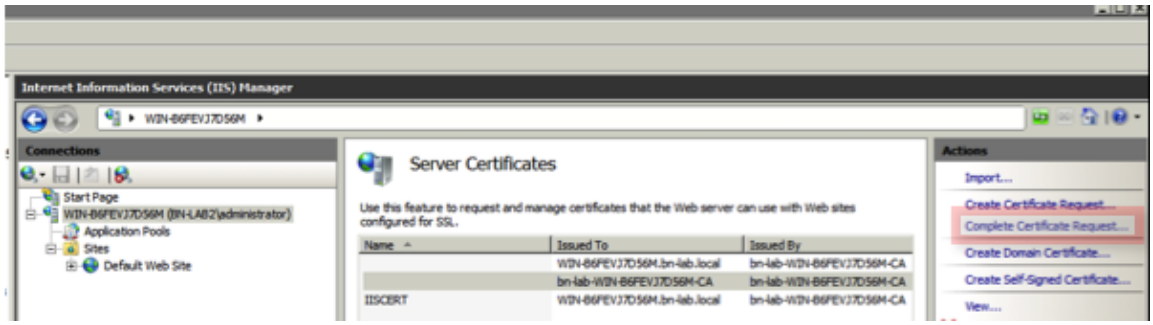
7. Click ***Submit a certificate request by using...***. Paste in the certificate content from the clipboard, and choose the ***Web Server*** template.



8. Click ***Submit*** and then save the certificate file to the desktop.

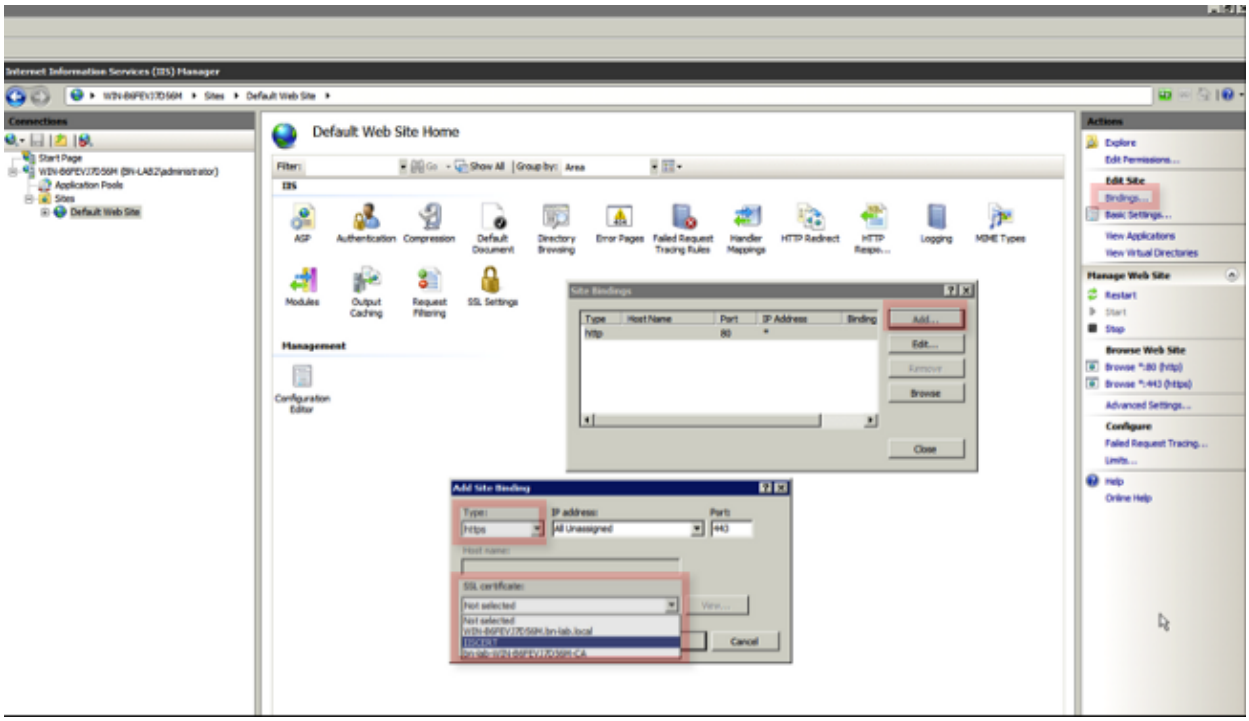


9. Return to the NDES server and open the IIS Manager utilty. Click on the server name and then click ***Complete Certificate Request*** in order to import the newly created server certificate.



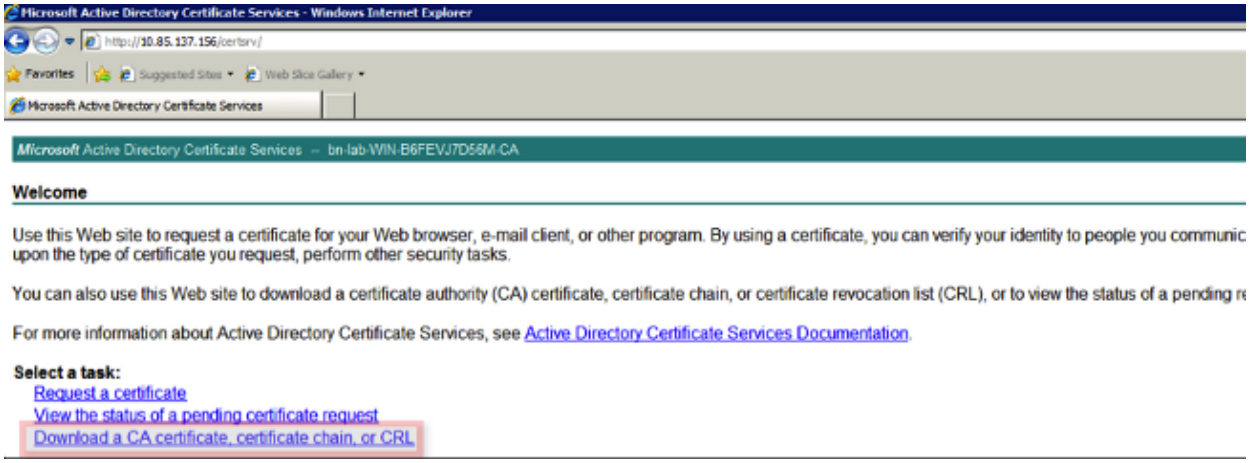
NDES Server IIS Binding Configuration

1. Expand the ***server name***, expand ***Sites***, click ***Default Web Site***.
2. Click ***Bindings*** in the upper right corner.
3. Click ***Add***, change the ***Type***to HTTPS, and choose the certificate from the drop−down list.
4. Click ***OK.***

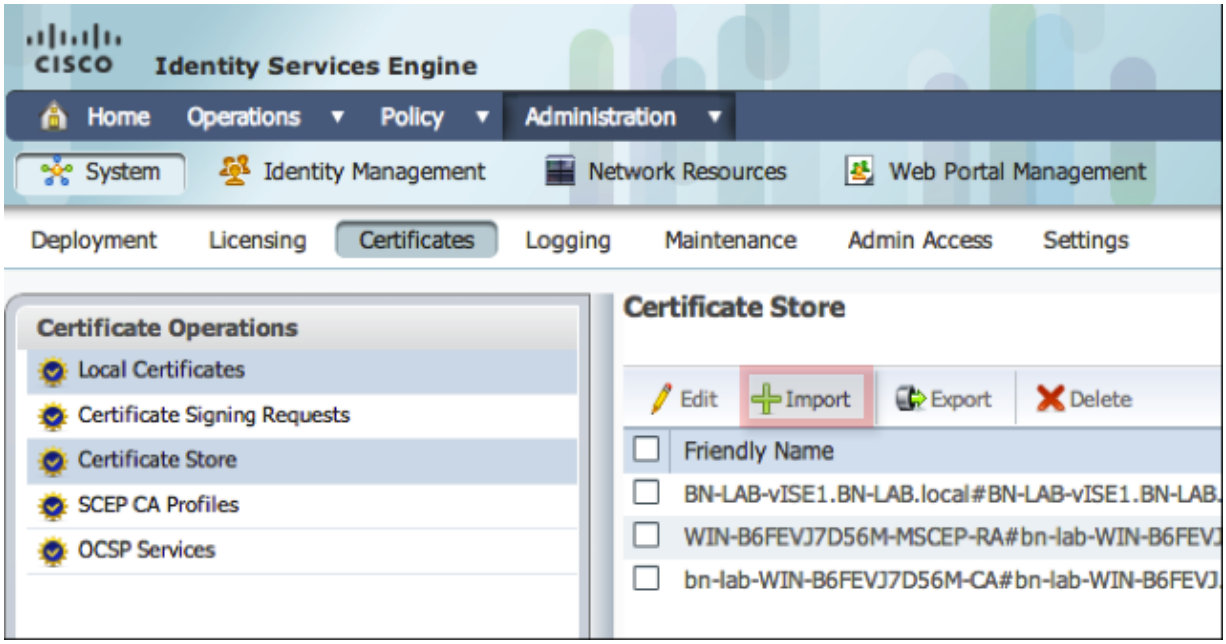


ISE Server Configuration

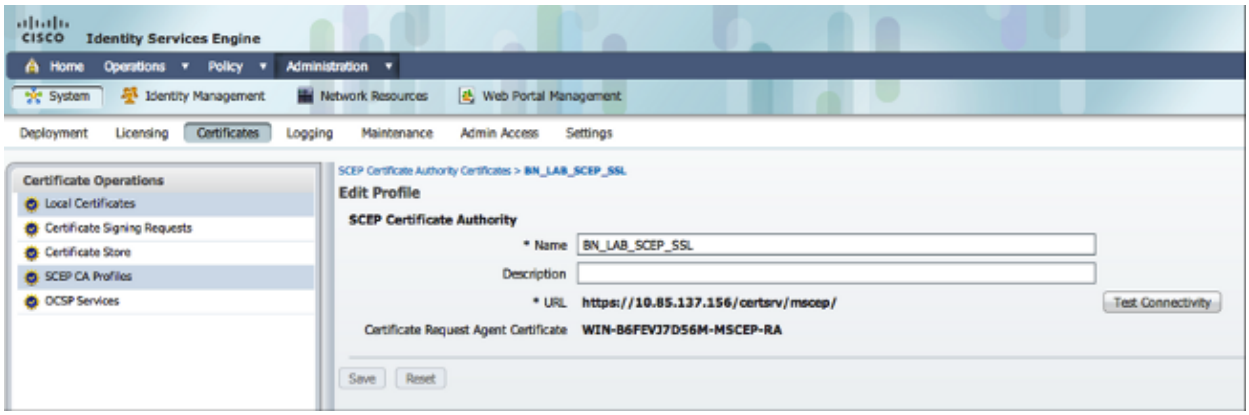
1. Connect to the Web Enrollment interface of the CA server and download the CA certificate chain.



2. From the ISE GUI, navigate to ***Administration*** **−>** ***Certificates*** **−>** ***Certificate Store*** and import the CA certificate chain into the ISE store.



3. Navigate to ***Administration*** −> ***Certificates*** −> ***SCEP CA Profiles*** and configure the URL for HTTPS. Click ***Test Connectivity*** and then click ***Save***.



Verify

Use this section to confirm that your configuration works properly.

- Navigate to ***Administration*** −> ***Certificates*** −> ***Certificate Store***and verify that the CA certificate chain and the NDES server Registration Authority (RA) certificate are present.
- Use Wireshark or TCP Dump to monitor the initial SSL exchange between the ISE admin node and the NDES server.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- Break down the BYOD network topology into logical waypoints in order to help identify debug and capture points along the path between these endpoints − ISE, NDES, and CA.
- Ensure that TCP 443 is permitted bidirectionally between the ISE and the NDES server.

- Monitor the CA and NDES server application logs for registration errors and use Google or TechNet to research those errors.
- Use the TCP Dump utility on the ISE PSN and monitor traffic to and from the NDES server. This is located under ***Operations*** > ***Diagnostic Tools*** > ***General Tools***.
- Install Wireshark on the NDES server or use SPAN on intermediary switches in order to capture SCEP traffic to and from the ISE PSN.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

Note: Refer to Important Information on Debug Commands before you use ***debug*** commands.

Related Information

- ***Configure SCEP Support for BYOD***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Jul 31, 2013 Document ID: 116238