Network Device Enrollment Service (NDES)

The Network Device Enrollment Service (NDES) is the Microsoft implementation of Simple Certificate Enrollment Protocol (SCEP). SCEP is a communication protocol that makes it possible for software that is running on network devices such as routers and switches—which cannot otherwise be authenticated on the network—to enroll for X.509 certificates from a CA.

This feature applies to organizations that have PKIs with one or more Windows Server 2012–based CAs, and that want to enhance the security for their network devices. Port security, based on 802.1x, requires certificates be installed on switches and access points. Secure Shell (SSH), instead of Telnet, requires a certificate on the router, switch, or access point. NDES is the service that allows administrators to install certificates on devices using SCEP.

Adding support for NDES can enhance the flexibility and scalability of an organization's PKI. Therefore, this feature should interest PKI architects, planners, and administrators.

Before installing NDES, you must decide:

- Whether to set up a dedicated user account for the service, or use the Network Service account.
- The name of the NDES registration authority and what country/region to use. This information is included in any SCEP certificates that are issued.
- The CSP to use for the signature key that is used to encrypt communication between the CA and the registration authority.
- The CSP to use for the encryption key that is used to encrypt communication between the registration authority and the network device.
- The key length for each of these keys.

In addition, you need to create and configure the certificate templates for the certificates that are used in conjunction with NDES.

Installing NDES on a computer creates a new registration authority and deletes any preexisting registration authority certificates on the computer. Therefore, if you plan to install NDES on a computer where another registration authority has already been configured, any pending certificate requests should be processed and any unclaimed certificates should be claimed before you install NDES.

Configure the Network Device Enrollment Service

Applies To: Windows Server 2008 R2

Setting up the Network Device Enrollment Service involves the following tasks:

- Add the account that will be the registration authority to the Internet Information Services (IIS) user group.
- Set up and configure the Network Device Enrollment Service.

Membership in the **Administrators** group is the minimum required to complete this procedure. For more information, see Implement Role-Based Administration.

To add a designated registration authority to the IIS_IUSRS group

1. Open the Local Users and Groups snap-in, and double-click the **Groups** folder.
2. Click the **IIS_IUSRS** built-in group.
3. On the **Action** menu, click **Add to Group**.
4. Click **Add**, type the domain name of the account that will be the registration authority, and then click **OK**.

Membership in **Enterprise Admins** or **Domain Admins**, or equivalent, is the minimum required to complete this procedure. For more information, see Implement Role-Based Administration.

To set up and configure the Network Device Enrollment Service

1. On the server where you want to install the Network Device Enrollment Service, open Server Manager, and click **Add Roles** to start the Add Roles Wizard.
2. On the **Select Server Roles** page, select the **Active Directory Certificate Services** check box, and then click **Next** two times.
3. On the **Select Role Services** page, clear the **Certification Authority** check box, and then select the **Network Device Enrollment Service** check box.

   You are prompted to install IIS and Windows Activation Service.

4. Click **Add Required Role Services**, and then click **Next** three times.
5. On the **Specify User Account** page, click **Select User**, and type the user name and password for the account that the Network Device Enrollment Service will use to authorize certificate requests. Click **OK**, and then click **Next**.
6. On the **Specify CA** page, if this computer does not host a CA, select either the **CA name** or **Computer name** check box, click **Browse** to locate the CA that will issue the Network Device Enrollment Service certificates, and then click **Next**.
7. On the **Specify Registry Authority Information** page, type the name of the registration authority in the **RA name** box. Under **Country/region**, select the country/region you are in, and then click **Next**.
8. On the **Configure Cryptography** page, accept the default values for the signature and encryption keys or configure your own values, and then click **Next**.
9. Review the summary of configuration options, and then click **Install**.