Technical white paper

HP Device Manager 4.7

SCEP Tutorial with Network Device Enrollment Service

Table of contents

Overview

Simple Certificate Enrollment Protocol (SCEP) is the most popular and most tested certificate enrollment protocol that is widely available. The Network Device Enrollment Service (NDES) is a SCEP server provided by Microsoft. This document introduces how to setup a NDES environment and enroll certificates with HPDM.

This feature is available on HP ThinPro 4 and higher with an SCEP add-on installed only.

For more information about NDES, go to http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx.

NDES setup

Operating system

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008 Service Pack 2
- Windows Server 2008 with the KB959193 hotfix installed (http://support.microsoft.com/kb/959193)

Setup

If you have a valid CA, go to http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx#Setup to set up the NDES.

To set up a brand-new NDES environment:

1. Set up a Windows Server system.
2. Open **Server Manager**.
3. Add the **Active Directory Domain Services** role.
    A. Run the Active Directory Domain Services Installation Wizard (`dcpromo.exe`) to finish the setup.
4. Create an account for **SCEPSvc**.
    A. Add the SCEPSvc account to the Administrators group.
    B. Add the SCEPSvc account to the IIS_IUSRS group.

    For more details about the required account permissions, go to http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx#Permissions_Required_for_the_Network_Device_Enrollment_Service.

    C. Log in with the account and create a user profile.
5. Add the **Active Directory Certificate Services** role.
    A. Select **Certification Authority** as the role service.
6. Add **Active Directory Certificate Services – Network Device Enrollment Service** to the role service.
    A. Set the account for **SCEPsvc**.
7. Set the NDES to issue certificates automatically.
    A. Right-click **Server Manager > Roles > Active Directory Certificate Services > <Your CA>**, and then select **Properties**.
    B. Select the **Policy Module** tab.
    C. Click the **Properties** button.
    D. In the radio box, select the **automatically issue the certificate** option.
    E. Restart the Active Directory Certificate Services. The NDES is now available.

The challenge password from the request challenge password URL can issue only one certificate. In some environments, such as manufacturing, it might be desirable to reuse the same challenge password for more than one device. For instructions on setting the NDES to reuse the same challenge password, see *Reusing a password for multiple devices* at http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx#Password_and_Password_Cache.

Enrolling certificates through the NDES

Figure 1. Enrolling certificates through the NDES
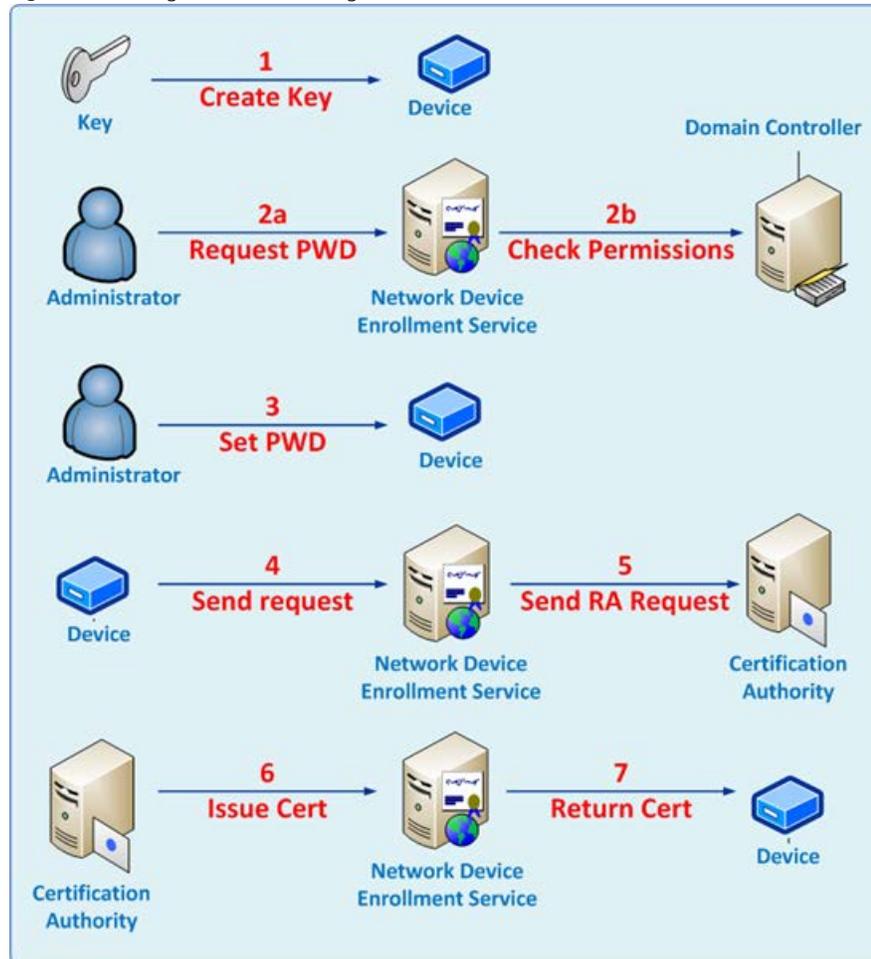
Figure 1 shows the usual steps for cerficate enrollment through the NDES. With HPDM, you only need to do step 2a (request a password) and step 3 (set a password) to finish the certificate enrollment.

Note

In the following procedure, enter your NDES address where <NDES-address> is in the URLs. Do not forget to enter the final / of the URLs.

Figure 2. Requesting a challenge password from NDES
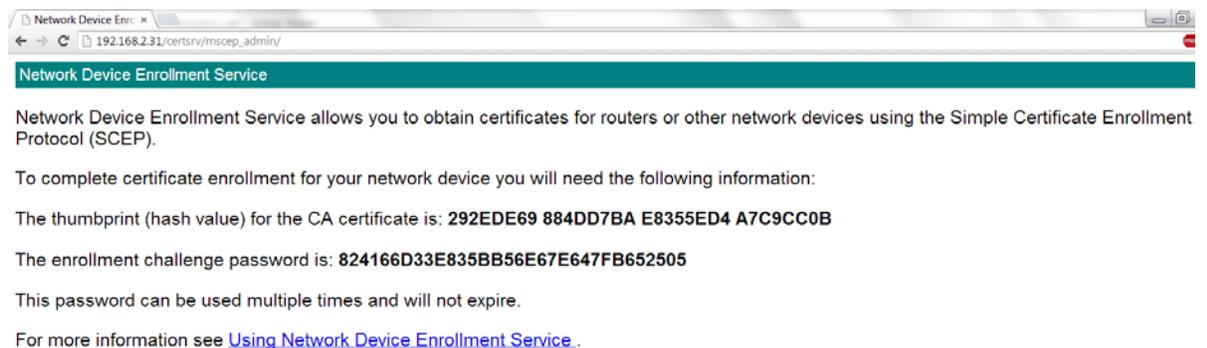
8. To request a challenge password, go to http://<NDES-address>/certsrv/mscep_admin/.

9. Enter your account name and password to finish the NTLM authentication. You will then receive the challenge password.

Figure 3. Sending an Enroll certificates with SCEP task

10. To enroll a certificate, go to http://<NDES-address>/certsrv/mscep/.

11. Enter the challenge password.

After enrollment, you can find the issued certificates in the HP ThinPro Certificate Manager.

For more information

To read more about HP Device Manager, go to hp.com/go/hpdm.

Sign up for updates

hp.com/go/getupdated