Windows 2000 Server

Step-by-Step Guide to End User Certificate Management

Abstract

This step-by-step guide takes you through the process that end users go through to obtain and manage certificates in the Microsoft® Windows® 2000 operating system.

Introduction

This step-by-step guide takes you through the process that end users go through to obtain and manage certificates in the Microsoft® Windows® 2000 operating system.

Prerequisites

This step-by-step guide assumes that you have run the procedures in *Step-by-Step Guide to Common Infrastructure for Windows 2000 Server Deployment Parts 1* http://www.microsoft.com/technet/win2000/depprof1.asp *and 2* http://www.microsoft.com/technet/win2000/depprof2.asp.

The common infrastructure documents specify a particular hardware and software configuration. If you are not using the common infrastructure, you must take that into account when using this guide. The most current information about hardware requirements and compatibility for servers, clients, and peripherals is available at the Windows 2000 Product Compatibility Search site http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/default.asp.

End User Certificate Management also assumes you have already completed:

- Step-by-Step Guide to Setting up a Certificate Authority
- Step-by-Step Guide to Certificate Services Web Pages

If you have not completed those step-by-step guides, you must still create the following environment to be successful with the procedures described in this document:

- Windows 2000 Professional operating system is installed on a computer in a Windows 2000 domain.
- Windows 2000 Certification Authority (CA) is running in the domain.

Certificate Management in Windows 2000

This section explains how to view and manage certificates in certificate stores on a computer running Windows 2000 Professional.

Viewing Your Certificates

1. Click **Start**, point to **Settings**, and click **Control Panel**.
2. Double-click the **Users and Passwords** icon. The **Users and Passwords** dialog box appears.
3. Click the **Advanced** tab. Then, click the **Certificates** button to start the **Certificates** window (see Figure 2).

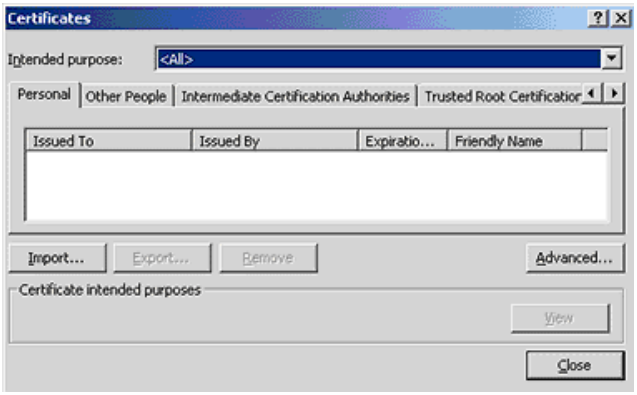

Figure 1 Certificate Listing

4. Certificates are organized into the following four categories. Each of the categories is a separate tab within the **Certificates** dialog box.
   - **Personal**. Certificates that are issued to you.
   - **Other People**. Certificates that are issued to other individuals or companies.
   - **Intermediate Certification Authorities**. An Intermediate Certification Authority issues server certificates, personal certificates, publisher certificates, or certificates for other Intermediate Certification Authorities. Intermediate Certificate Authorities issue and validate personal digital certificates. These certificates must be verified by a root certificate in the Trusted Root Certification Authorities.
   - **Trusted Root Certification Authorities**. Certificates that are issued by root certification authorities that you trust explicitly.
5. Double-click a certificate to view information about it. The **Certificate** dialog is organized into the following three tabs:
   - **General**. Default view for seeing a certificate's purposes.
   - **Details**. Displays the actual X.509 fields, extensions, and properties of a certificate. You may also click **Edit Properties** in this view. This allows you to modify the **Friendly Name** and **Description** fields. You can also specify what the certificate can be used for.
   - **Certification Path**. Displays the certification path.

Installing a Root Certificate

Windows 2000 has a number of pre-installed root certificates for various commercial certification authorities. If you choose to use a commercial CA that is not pre-installed, you must install the CA root certificate to enable trust of any certificates issued by that CA. Installation of the CA root certificate may vary depending on the particular CA. This example shows you how to install the root certificate for the enterprise root certification authority.

Root certificates for Windows 2000 Certification Authority services in the same domain as the client are installed automatically.

To install a root certificate obtained from a third party

1. First, create a **Certificates** management console to manage the certificates for the computer on which you are working. To do this, click **Run** on the **Start** menu, and type **mmc** in the **Run** text box.
2. On the **Console menu**, click **Add/Remove Snap-in**. In the dialog, click the **Add** button. In the next dialog, click **Certificates**, and then click **Add**.
3. In the **Certificates snap-in** dialog, select **Computer account**, and then click **Next**.
4. Select the **Local computer** radio button. Then click **Finish**. Click **Close**, and then click **OK**. The **Certificates** directory now displays in the left pane of the console.
5. On the console menu, click **Save As**. In the **File name** text box, type **Certificates**, and then click **Save**.
6. In the console, expand the **Certificates** node. Then expand **Trusted Root Certification Authority**.
7. Right-click the **Certificates** folder, point to **All Tasks**, and then click **Import**.
8. The Certificate Import Wizard launches. Click **Next**.
9. Click the **Browse** button to locate and select the CA certificate you would like to import.
10. After you've selected the file, click **Next**.
11. Now, select the **Place all certificates in the following store** option. By default, **Trusted Root Certification Authority** should show up in the text box as the store to which to save the imported file. If this doesn't show up by default, click **Browse** to find the store. Then, click **Next**.
12. Read the information in the **Completing the Certificate Import Wizard** window, and then click **Finish**. The CA certificate is now installed. To verify this, scroll through the list of certificates in the right pane to find the one you have just installed.

Obtaining a Client Authentication Certificate from the Certification Authority

This example shows you how to get a client authentication certificate from the Certificate Authority.

1. Open **Internet Explorer** and navigate to the Certificate Service Web pages by going to http://*CA server name*/certsrv/. Here, *CA server name* is the common name or IP address of the CA computer in your network.
2. On the **Welcome** page, select the **Request a certificate option**, and click **Next**.
3. On the **Choose Request Type** page, select the **User certificate request** option, and then click **Next**.
4. You are now on the **User Certificate – Identifying Information** page. If you would like to select a Cryptographic Service Provider (CSP), click the **More Options** button. Note that only an administrator with an understanding of CSPs should attempt this. Click **Submit**.

   A message informs you that the request is being generated.
5. Next, a page comes up informing you whether the certificate was issued to you. If it was, click the **Install this certificate** link. You will see a message letting you know when the certificate has been successfully installed.

Changing a Certificate's Intended Purposes

You may want to limit the intended purpose(s) of a certificate because certification authorities may choose to issue certificates without (a) predefined intended purpose(s). In the following procedure, you modify the intended purposes of the root certificate of the CA.

Note This example assumes you have installed the root certificate for this CA, as explained earlier.

To change a certificate's intended purpose(s)

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certificates**.
2. Click the + next to **Certificates** to expand it, and then right-click the **Trusted Root Certification Authorities** folder.
3. In the right pane, scroll down to **Microsoft Root Authority** and double-click it to open the certificate (see figure 2).

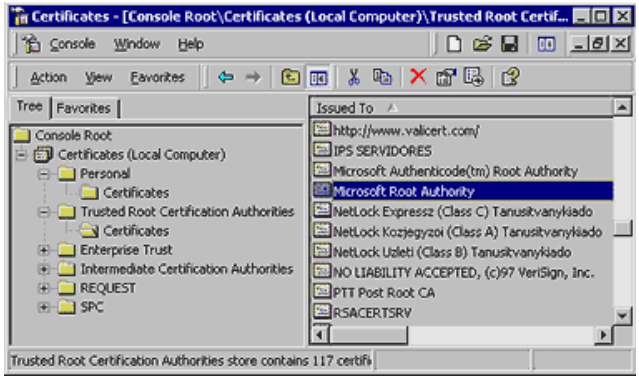

Figure 2 Microsoft Root Authority

4. The certificate information is displayed on the **General** tab.
5. Select the **Details** tab. Click **Edit Properties**.
6. The **Certificate Properties** dialog launches (see figure 7). A root certificate may contain information about its intended purpose(s). In this case, the root certificate has all purposes enabled.

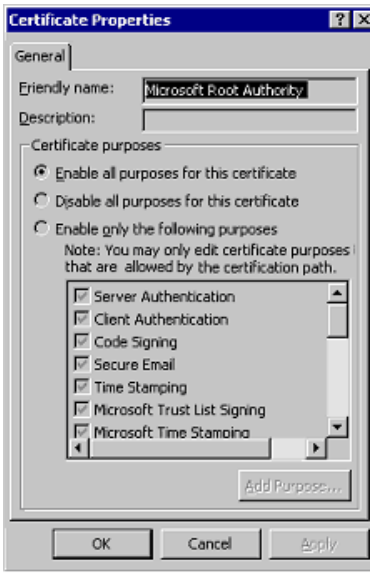

Figure 3 Certificate Properties

7. Click the **Enable only the following purposes** option.
8. Unselect all intended purposes except for **Code Signing**. Windows will only use this certificate and any certificates that this CA issues for code signing (and verification).
9. Click **Apply** to save the changes, and then click **OK** to close the dialog.

Exporting Certificates

You can back up important certificates and their corresponding private keys, or move them to another computer.

Note To enable exporting the private key with the certificate, that option must be chosen when a user requests a certificate using the Web enrollment form. For more information on this, see Step-by-Step Guide to Certificate Services Web Pages.

To export certificates

1. Right-click the certificate(s) you want to export.
2. Point to **All Tasks** on the context menu, and click **Export** to launch the **Certificate Export Wizard**. Click **Next**.
3. If the certificate you are exporting has a corresponding private key in the system, you can choose to export the private key with the certificate.

   Note You will only be able to export to a Personal Information Exchange PKCS#12 file if you want to export the private key.
4. Select the export file format. Click **Next**..
5. If the file specified is a Personal Information Exchange—PKCS #12 (*.pfx), you will be prompted for the password. Enter your password to export the file. Click **Next**.
6. Enter the name of the file you want to export. Click **Next.**
7. Verify the choices you have made in the wizard. Click **Finish** to export to the file.

Importing Certificates

You can restore certificates and the corresponding private keys from a file.

To import a file

1. Right-click the certificate store you want to import, and click **Install PFX** on the context menu.
2. The Certificate Import Wizard launches. Click **Next**.
3. In the File name text box, type the name of the certificate file that you want to import. Alternatively, you can find the file by clicking **Browse**. Click **Next**.
4. If the file specified is a Personal Information Exchange–PKCS #12 (*.pfx), you will be prompted for the password. Enter the password to import the file. Click **Next**.
5. Select where you'd like to store the certificate. Click **Next**.
6. The next wizard page contains summary information about the file that you are importing. Click **Finish** to import the file. The certificate(s) are now ready for use by the system.
