Active Directory

Step-by-Step Guide to Mapping Certificates to User Accounts

Introduction

The Windows® 2000 operating system provides a rich administrative model for managing user accounts. In a corporate environment with relatively few threats, the user account/password model works very well. However, the Internet is a potentially hostile environment, more prone to user ID/password attacks. Certificate mapping provides an elegant solution to this situation by using public-key technology, a safeguard that is much more resistant to attack than password-based systems. In Windows 2000, it is possible to map a certificate that has been issued to a user to the user's account. A server application can then use public-key technology to authenticate the user through this certificate. If the user is authenticated, the user's account is logged on. The result is the same as if the user had provided a user ID and password; yet the process is much more secure.

Traditionally, computer systems have used a centralized accounts database to manage users, their privileges, and their access controls. This technique has worked well, and is generally well-understood. However, as systems become more distributed—with hundreds of thousands to millions of users—this form of centralized control often becomes difficult to manage. The problems range from trying to verify an account against a database located across the Internet, to administering a lengthy list of users.

Public key certificates have the potential to help simplify these problems. Certificates can be widely distributed, issued by numerous parties, and verified by examining the certificate without referring to a centralized database. However, existing operating systems and administration tools can only deal with accounts, not certificates. The simple solution that maintains the advantages of both certificates and user accounts is to create an association—or *mapping*—between a certificate and a user account. This allows the operating system to continue using accounts while the larger system and the user use certificates.

In this model, a user presents a certificate, and the system looks at the mapping to determine which user account should be logged on. This should not be confused with smart card logons. Windows® 2000 supports smart card logon, and that mapping is implicit. For more information, see the Windows 2000 guide on smart card logon http://www.microsoft.com/windows2000/library/howitworks/security/sclogonwp.asp .

Mapping a certificate to a Windows 2000 user is done either through the Windows 2000 Active Directory™ service, or with rules defined in Internet Information Service (IIS). This guide helps you map public key certificates to a specific Windows 2000-based user account. The certificate can then be used to authenticate the user with a computer running Windows 2000 and IIS.

Requirements and Prerequisites

This step-by-step guide assumes that you have run the procedures in Step-by-Step Guide to a 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 need to make the appropriate changes to this document. The most current information about hardware requirements and compatibility for servers, clients, and peripherals is available at the Windows 2000 Product Compatibility Search page http://www.microsoft.com/windows2000/upgrade/compat/search/default.asp .

This guide assumes you have already completed:

- Step by Step Guide to Managing the Active Directory http://www.microsoft.com/technet/win2000/managad.asp
- Step by Step Guide to Setting up a Certificate Authority http://www.microsoft.com/technet/win2000/casetup.asp
- 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:

- You have installed Windows 2000 Professional operating system on a computer in a Windows 2000 domain.
- Windows 2000 Certification Authority (CA) is running in the domain.
- Windows 2000 operating systems running in the domain.
- A trusted certificate authority.
- A user certificate service or certificates issued by a trusted CA.
- Windows 2000 Active Directory service.
- Internet Information Services (IIS).
- Administrative permissions for the person mapping the CA to user accounts.

Types of Mapping

In most cases, a certificate is mapped to a user account in one of two ways: a single certificate is mapped to a single user account (one-to-one mapping), or multiple certificates are mapped to one user account (many-to-one mapping).

User Principal Name Mapping

User principal name mapping is a special case of one-to-one mapping. User principal name mapping is only available through the Active Directory. Enterprise certificate authorities (CAs) place an entry, called a UPN, into each certificate. The UPN looks very much like an e-mail name. The UPN is unique within a Windows 2000-based domain. The UPN is used to find the user's account in the Active Directory, and that account is logged on. UPN mappings are implicit in Windows 2000, and this is the method used by smart card logon. (See the next section below "Active Directory Mapping" for more details.)

One-to-One Mapping

One-to-one mapping involves mapping a single user certificate to a single Windows 2000 user account. For example, assume you want to provide a Web page to your employees that will allow them to view and modify their deductions, manage their health care, and other benefits. You want this page to work over the Internet and remain secure. As a solution, you decide to use Windows 2000, certificates, and certificate mapping. You can either issue certificates to each of your employees from your own certificate service, or you can have your employees obtain certificates from a CA approved by your company. You then take these user certificates and map them to the employees' Windows 2000 user accounts. This allows users to connect to the Web page, using the Secure Sockets Layer (SSL) from anywhere by providing their client certificate. Users log on using their user account and normal access controls can be applied.

Many-to-One Mapping

Many-to-one mapping involves mapping many certificates to a single user account. For example, assume you have a partnership with an agency that provides temporary workers for your job openings. You would like to allow the agency personnel to view Web pages describing current job openings that are otherwise accessible only to company employees. The agency has its own CA that it uses to issue a certificate to its employees. After installing the agency CA's root certificate as a trusted root in your enterprise, you can set a rule that maps all certificates issued by that CA to map to a single Windows 2000 account. You then set access rights so that this

account can access the Web page. Typically, you give the user account the same name as the agency.

When temporary employees from the agency connect to the agency's Web server and provide their certificates, they are mapped to the same account and can access the Web page. However, they cannot view other pages since the account does not have permissions to anything else. This saves administrative expense because the agency can now issue certificates and manage its users without requiring further intervention on your part.

Where Mapping Occurs

With IIS in Windows 2000, the certificate mapping can occur in one of two places: IIS or Active Directory.

IIS

When IIS does the mapping, the certificate is compared to a list of rules that IIS maintains in its metabase. IIS finds a rule that matches the indicated Windows 2000 account. IIS mapping is configured for each Web server and is useful if you need very few mappings or a different mapping on each Web server. Most people will prefer to use Active Directory mapping because it requires less administration.

Active Directory

In Active Directory mapping, when the IIS server receives a certificate from the user, it passes it on to Active Directory, which maps it to a Windows 2000 user account. The IIS server then logs this account on.

Active directory mapping is most useful when the account mappings are the same on all IIS servers. Administration is simplified because the mapping is done in only one place.

Mapping in Active Directory can happen in one of two ways. The administrator can explicitly map a certificate to a user's account. This certificate can come from any source--as long as the root CA for that certificate is trusted for client authentication.

UPN mapping can also be used. A UPN is automatically put into a certificate issued by an enterprise CA. If a certificate is passed to Active Directory for mapping, it is first examined for UPN mapping. If UPN mapping is not possible, the mapping set by the administrator is used.

UPNs are in the form of *userid@domain*. If the certificate contains a UPN, the domain is within the hierarchy of the directory, and the CA that issued the certificate is trusted to put UPNs in the certificate, then the user's account is retrieved from the directory and logged on. All these conditions must be true before the user's account is retrieved. If any of these conditions is false, the directory is searched for a mapping set by the administrator.

Requesting the User Certificate

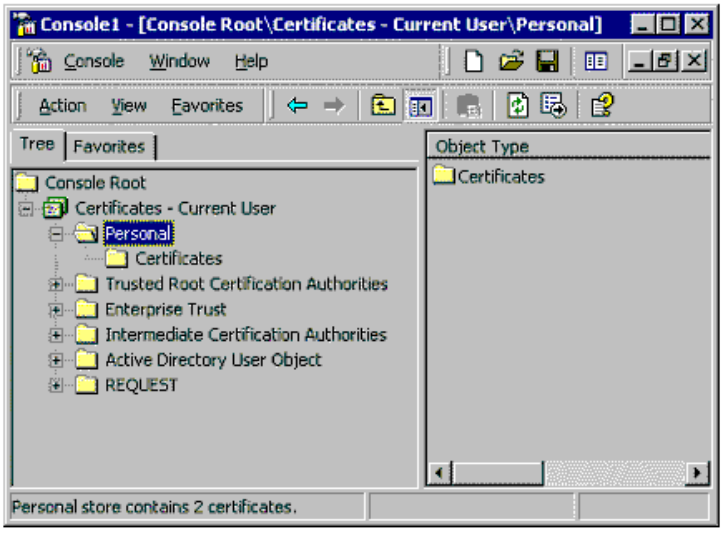
For this guide you will need to request a user certificate. If you wish to use UPN mapping, you should get a certificate from an enterprise CA in your domain. However, for all other mapping methods, you should use a certificate from a CA that is not in your enterprise. This ensures that UPN mapping is not occurring when you test the mapping at the end of this guide. For more details, see the guides entitled Administering Certificate Services and Certificate Services Web Pages. A brief description is provided below.

You can request a certificate in one of two ways:

- Use Internet Explorer to connect to a Web enrollment page. An enrollment page is provided with Windows 2000 Certificate Services and is installed on the same computer as the Certificate Service. To use these to request a certificate, connect to http://*servername*/CertSrv, and follow the directions. If you are using an enterprise CA, these pages require authentication, and you must select a template type to request a valid template. Typically, this will be a user template. You can also use Internet Explorer to request a certificate form a third-party commercial CA. Trusted root certificates are included in Windows 2000 for a number of these commercial CAs.
- Use the Certificates management snap-in to request a certificate from Microsoft Certification Authority. These procedures are described next.

To use the Certificates management console to request a certificate

1. To open the Microsoft Management Console (MMC), click **Start**, click **Run**, type **mmc** in the Open box, and click **OK**.
2. On the **Console menu**, click **Add/Remove Snap-in**. In the dialog box, click the **Add** button. In the next dialog box that pops up, click **Certificates**, and then click **Add**.
3. Select **My user account** and click **Finish**.
4. Click **Close** to close the **Add/Remove Snap-in** dialog box and then click **OK**.
5. In the **Certificates** console, expand the **Certificates** node.
6. Right-click the **Personal** folder, point to **All Tasks**, and click **Request New Certificate** as in Figure 1 below.



If your browser does not support inline frames, click here to view on a separate page.

Figure 1 MMC with Certificates snap-in

7. The Certificate Request Wizard launches. Click **Next**.
8. In the **Certificate tem**plates list, select **User**. Click **Next**.
9. Type a **Friendly name** and **Description** into the text boxes. Click **Next**.
10. Click **Finish**. A message box appears telling you the certificate request was successful. Click **Install Certificate**, and then click **OK**.
11. To view the newly issued certificate, click the **Certificates** folder under **Personal**. The new certificate is listed in the right pane. Double-click it to view certificate details.

Exporting the Certificate

Once you have the certificate, you need to export it for use in later steps.

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 that 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 (for this exercise, you can simply accept the default). 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. 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.

Installing CA Certificates

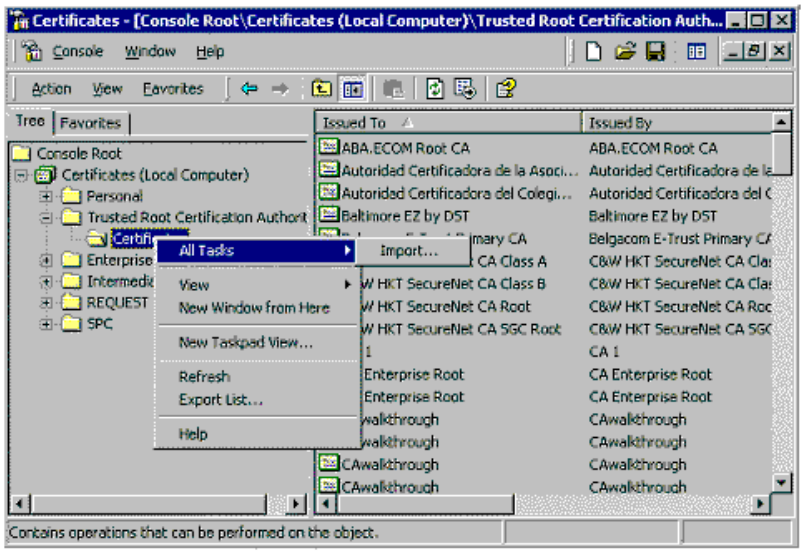
If you are using an enterprise CA in your domain, you can skip this section because the root certificate is trusted by your system.

Windows 2000 has a number of pre-installed CA 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 CA 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 open the Microsoft Management Console (MMC), click **Start**, click **Run**, type **mmc** in the Open box, and click **OK**.
2. On the **Console menu**, click **Add/Remove Snap-in**. In the dialog box, click **Add**. In the next dialog box that appears, click **Certificates**, and then click **Add**.
3. Click **Computer account**, then click **Next**.
4. Click **Local computer**, 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** as in Figure 2 below.



If your browser does not support inline frames, click here to view on a separate page.

Figure 2 Import Certificate

8. The Certificate Import Wizard launches. Click **Next**.
9. Click the **Browse** button to select the CA certificate you would like to import. After you've selected the file, click **Next**.
10. Click 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**.
11. 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.

Preparing IIS for Mapping

Active Directory Mapping

Note Skip this section if you do not want to use Active Directory mapping.

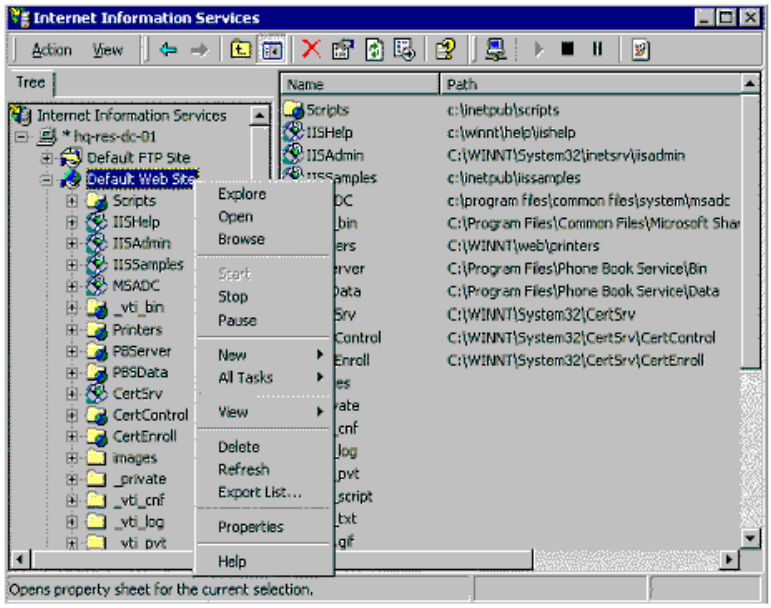
To configure Active Directory mapping

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, then click **Internet Services Manager**. Right-click the server name in which IIS is running (in our example, **HQ-RES-DC-01**), and click **Properties**.
2. On the **Internet Information Service** tab, click **Edit** in the **Master Properties** section.
3. On the Directory Security tab, check the **Enable the Windows directory service mapper** check box. This option tells IIS that when you set a Web site to do mapping, it should really do Active Directory mapping. If this setting is unchecked, IIS does the mapping. Click **Apply**, and then click **OK**.

Configuring SSL

The next step is to configure a site to use SSL. You must do this for both Active Directory and IIS mapping.

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.
2. Expand the domain node. Select **Default Web Site**, and right-click on it. Click **Properties** on the submenu as in Figure 3 below.



If your browser does not support inline frames, click here to view on a separate page.

Figure 3 IIS Manager

3. The **Default Web Site Properties** dialog box starts. Click the **Directory Security** tab.

   Notice that the **Edit** button under **Secure communications** is unavailable. This is the case until you request a Web server certificate.
4. Click the **Server Certificate** button.
5. The **Web Server Certificate Wizard** starts. Click **Next**.
6. Select the **Create a New certificate** option,and click **Next**.You will see a different dialog box if IIS already has a certificate.
7. Select the **Send the request immediately to an online certification authority** option. (This assumes that you have an enterprise CA in your domain that is configured to issue Web certificates. See the Step-by-Step Guide to Setting Up a Certificate Authority http://www.microsoft.com/technet/win2000/casetup.asp for details on setting up an enterprise CA.) Click **Next**.
8. In the **Name and Security Settings** dialog box, accept the default options. Click **Next**.
9. On the next page, enter your information, and click **Next**.
10. Type your server name in the **Common name** text box. It can be either the DNS name, the NetBIOS name, or the word LOCALHOST. Enter your choice, and click **Next**.
11. On the next page, enter your information, and click **Next**.
12. If you have an enterprise CA in your domain from which you are allowed to request Web server certificates, you will see it listed here. (If there is no CA, if the CA is not configured to issue Web server certificates, or if you do not have permission to request a Web server certificate, this list will be empty. You must have a CA available to complete this section.) Select the CA you want to use, and click **Next**.
13. The Certificate Request Submission page comes up. Click **Next**.
14. Click **Finish**. The server now has a server certificate.
15. You will notice **Edit** under **Secure communication** is now enabled (see Figure 4 below); click **Edit.**

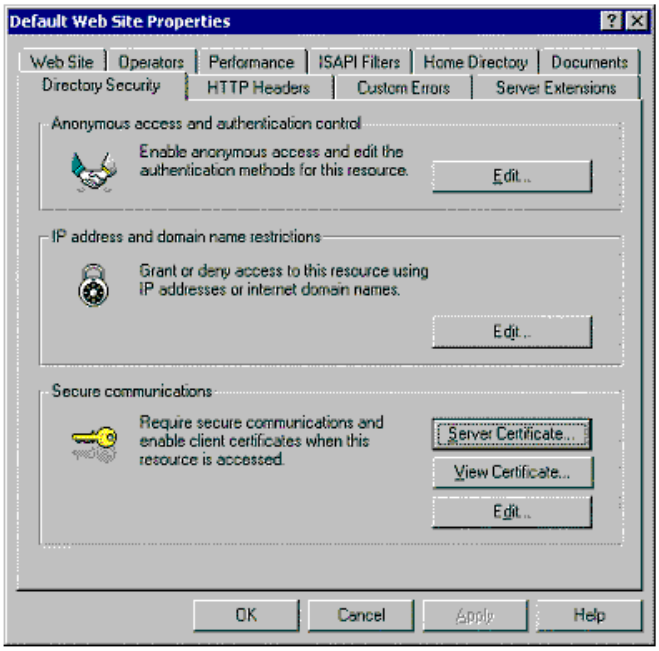


Figure 4 Secure Communications Dialog

16. Use the **Secure communications** dialog box, as in Figure 5 below, to configure the site to do SSL and account mapping. You must check the **Enable client certificate mapping** for both IIS and Active Directory mapping. Select either **Accept client certificates** or **Ignore client certificates**. The **Accept client certificates** setting requires negotiation of client certificate authentication with the browser. If it fails, it falls back to one of the standard authentication protocols. If you select **Ignore client certificates**, you must also check the **Require secure channel (SSL)** check box. No fallback is allowed to another authentication method. Requiring secure channel means that the Web site will not be viewable through HTTP, only through HTTPS. You should not check the **Enable certificate trust list** for this guide. Click **OK**. Click **Apply**, and then click **OK**.

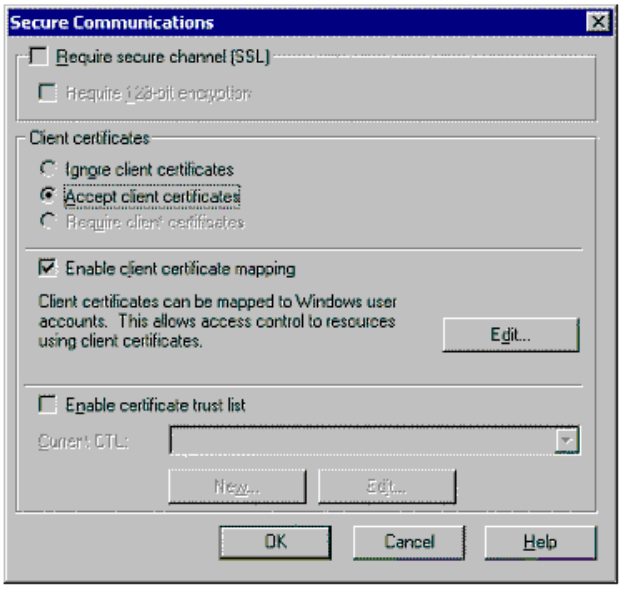


Figure 5 Configure Site.

Mapping User Accounts

If you want to do IIS mapping, first turn off Active Directory mapping. IIS is now ready to do certificate mapping.

To turn off Active Directory mapping

1. On the **Start** menu, point to **Programs**, point to **Administrative Tools**, then click **Internet Services Manager**. Right-click the server name in which IIS is running (in our example, **HQ-RES-DC-01**), and click **Properties**.
2. On the **Internet Information Service** tab, click **Edit** in the **Master Properties** section.
3. On the Directory Security tab, clear the **Enable the Windows directory service mapper** check box. This option tells IIS to do the mapping. Click **Apply** and then click **OK**.

One-to-One Mapping

This section covers one-to-one mapping, first in the Active Directory and then with IIS.

Using the Active Directory for One-to-One Mapping

If you have set IIS to do directory mapping by following the instructions above, IIS automatically does UPN mapping for certificates from a trusted enterprise CA. You can proceed directly to the section, Testing the Mapping below to see UPN mapping. The default administrator account does not have a UPN and does not map. You must create a new account and use its certificate to see UPN mapping.

To configure Active Directory one-to-one mapping

1. Click Start, click Programs, click Administrative Tools, and click Active Directory Users and Computers.
2. Expand the domain name node (**HQ-RES-DC-01**), and click the **Users** folder. In the right pane, right-click the **Administrator** account and click **Name Mappings**.
3. On the **X.509 Certificates** tab, click the **Add** button. Select the user certificate from the .cer file saved in the **Exporting a certificate** section.
4. The **Use Issuer for alternate security identity** will be selected and appear gray by default because you need to use this for both one-to-one mapping and many-to-one mapping. Select the **Use Subject for alternate security identity** option to do one-to-one mapping. By unchecking this option, you will be doing many-to-one mapping. Click **OK**.
5. Go to the section, Testing the Mapping, to verify that this works.

Using IIS for One-to-One Mapping

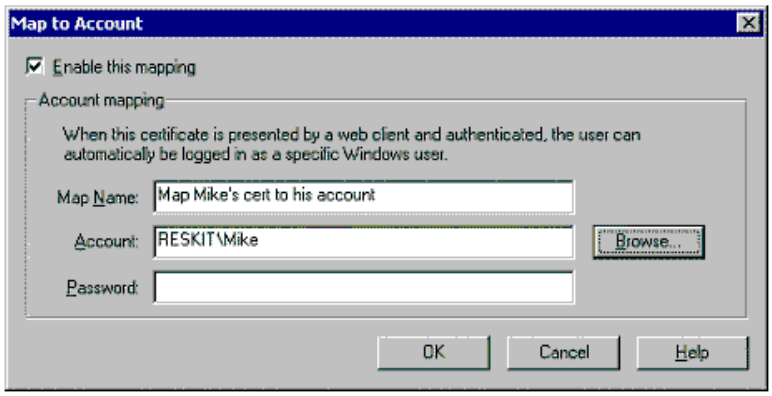
Instead of using Active Directory as in the previous section, you can use IIS to do all the mappings. To configure IIS one-to-one mapping, first ensure that Active Directory mapping is turned off (return to the master property page and unchecking **Active Directory mapping**).

To turn off Active Directory mapping

1. On the **Start** menu, point to **Programs**, point to **Administrative Tools**, then click **Internet Services Manager**. Right-click the server name in which IIS is running (in our example, **HQ-RES-DC-01**), and click **Properties**.
2. On the **Internet Information Service** tab, click the **Edit** button in the **Master Properties** section.
3. On the Directory Security tab, clear the **Enable the Windows directory service mapper** check box. This option tells IIS to do the mapping. Click **Apply**, and then click **OK**.

To configure IIS one-to-one mapping

1. Click Start, click Programs, point to Administrative Tools, and then click Internet Services Manager.
2. Expand the computer name node (in our example, **HQ-RES-DC-01**). Right-click the **Default Web Site** folder, and click **Properties** on the submenu.
3. Click the **Directory Security** tab on the **Default Web Site Properties** dialog box.
4. Click **Edit** in the **Secure communications** section.
5. In the **Secure Communications** dialog box, verify that the **Enable client certificate mapping** option is selected, and click **Edit**.
6. On the **Account Mappings** page, click the **1-to-1 tab**, and click **Add**.
7. Select the user's certificate from the list, and click **Open**. For IIS, this certificate must be base64-encoded and cannot be a binary certificate. Although Windows 2000 works with both types, IIS can only process base64-encoded files,.



If your browser does not support inline frames, click here to view on a separate page.

Figure 6 Map to Account dialog

8. The **Map to Account** dialog opens. Click **Browse** to select the **Administrator** account (see Figure 6 above). Enter the password and click **OK**.
9. Click **Apply** and/or click **OK**, as appropriate, in the remaining dialog boxes to save the information and to close them.

IIS one-to-one mapping is now configured. You can go to the section Testing the Mapping at the end of this paper to see this mapping work.

Many-To-One Mapping

In the previous two sections, you used one-to-one mapping. You will now configure many-to-one mapping in which many users (certificates) are mapped to a single Windows 2000 user account.

Using the Active Directory for Many-to-One Mapping

Remember to enable Active Directory mapping if you disabled it in the previous section:

1. Click **Start**, click **Programs**, click **Administrative Tools**, and click **Active Directory Users and Computers**.
2. Expand the domain name node (in our example, **HQ-RES-DC-01**), and click the **Users** folder. In the right pane, right-click the **Administrator** account, and click **Name Mappings** on the submenu.
3. On the **X.509 Certificates** tab, click **Add**.
4. Click the certificate you'd like to add, and click **Open**.
5. Clear the **Use Subject for alternate security identity** check box, and click **OK**.
6. A message tells you that you won't be able to use the subject for alternate security identity. Click **Yes**.
7. Your new mapping information now displays. Click **Apply**, and then click **OK**.

You have now configured Active Directory to map all certificates from the issuing CA to the Administrator account.

Using IIS for Many-to-One Mapping

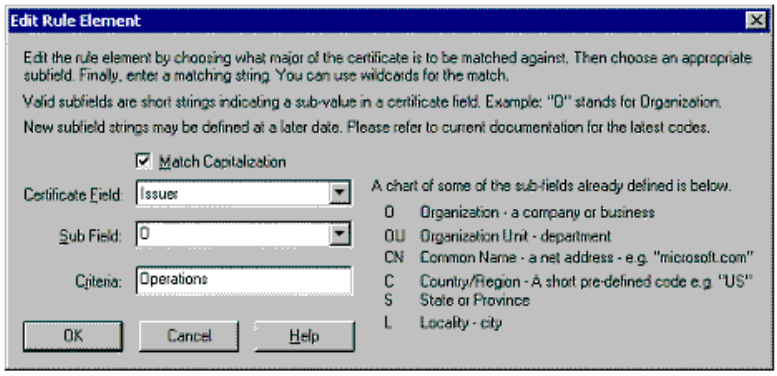
To configure IIS many-to-one mapping, you must first turn Active Directory mapping off.

To turn off directory mapping

1. Open the **Active Directory Users and Computers** snap-in.
2. Expand the domain node (in our example, **HQ-RES-DC-01**), and click **Users**. In the right pane, right-click **Administrators**, and click **Name Mappings** on the submenu.
3. On the **X.509 Certificates** tab, click **Remove**. Click **Apply**, and then click **OK**.
4. Click **Start**, point to **Programs**, point to **Administrative Tools**, then click **Internet Services Manager**. Right-click the server name in which IIS is running (in our example, **HQ-RES-DC-01**) and click **Properties**.
5. On the **Internet Information Service** tab, click the **Edit** button in the **Master Properties** section.
6. On the Directory Security tab, clear the **Enable the Windows directory service mapper** check box. This tells IIS to do the mapping. Click **Apply**, and then click **OK**.

To configure IIS many-to-one mapping

1. In the **Internet Services Manager** snap-in, expand the computer name node. Then right-click **Default Web Site**, and click **Properties** on the submenu.
2. Click the **Directory Security** tab, and in the **Secure Communications** section, click **Edit**.
3. In the **Secure Communications** dialog box, select the **Enable client certificate mapping** option, and then click the **Edit** button.
4. In the **Account Mappings** dialog box, click the **Many-to-1** tab. Click **Add**.
5. Enter a description if you wish. Click **Next**.
6. In the **Rules** dialog box, click **New**.
7. You can enter as many fields as you wish to this rule. However, for this guide, use only one. Specify that the organization (O) in the **Issuer** name is equal to **Operations** as in Figure 7 below. This means that all certificates issued to this organization will be mapped. Enter this information into your dialog box. Replace the **Criteria** with the value in your certificate. Click **OK**.



If your browser does not support inline frames, click here to view on a separate page.

Figure 7 Edit Rule

8. Click **Next**.
9. Click the **Browse** button to select the administrator's account. Click **Finish** and close all dialog boxes.

IIS is now configured to do many-to-one mapping. You can go to the Testing the Mapping section to see this in action.

Testing the Mapping

This section allows you to test the mappings that you have made.

Setting Up a Web Page

Typically, all the default Web pages installed with Windows 2000 are set for any user to access the pages. To see certificate mapping in action, you must create a page that can be accessed only if mapping is occurring. The following procedure creates a file and configures the access rights so that only a mapped user can access it. This file is used to verify that mapping is occurring.

Creating a Restricted File

First, create a file that can only be accessed by the Administrator account. This can by any type of file: .htm, .asp, .gif, .jpeg, .doc, and so on. For this test, use a .gif file.

1. Click **Start**, click **Programs**, click **Accessories**, and click **Windows Explorer**.
2. Navigate to the **Inetpub\Wwwroot** directory.
3. Copy the file **win2000.gif** and rename it **Admin.gif**.
4. Right-click the **Admin.gif** file, and select **Properties**.
5. Click the **Security** tab.
6. Uncheck the **Allow inheritable permissions from parent to propogate to this object** option at the bottom of the dialog box.
7. Remove all users and groups from the list by selecting each group and clicking **Remove**.
8. Addthe Administrator account back by clicking **Add** and selecting **Administrators**. Select **Full control**.
9. Click **Apply**, and click **OK**.

This file can now be accessed by the Administrator account only.

Turning Off Authentication

When IIS accesses a file, it impersonates a user so that the system uses the authenticated user's access rights. You need to ensure that the authentication happened using certificate mapping, rather than some other method.

To configure IIS so that no other form of authentication is possible for this file

1. Click **Start**, click **Programs**, point to **Administrative Tools**, and then click **Internet Services Manager**.
2. Click the **Default Web Site** folder.
3. In the right pane, right-click on the file **Admin.gif**.
4. Click **Properties**.
5. Click the **File Security** tab.
6. Click **Edit** under **Anonymous access and authentication control**.
7. Uncheck all options). (You can leave **Anonymous access** selected if you want.)

Return to Internet Explorer, and try to access the page. If you succeed, the user has been authenticated using the mapping.

Connecting a Web Page

The next step is to connect to this file and verify that the mapping is working.

To connect to the file

1. Log on as a user whose account has been mapped to a certificate.
2. From the **Start** menu, select **Run** and type **https://*servername*/admin.gif** where *servername* is the name of the Web server. If you are testing this on the Web server, use **LOCALHOST** instead of the server name. Click **OK**.

   Internet Explorer may display a warning that you are about to use SSL. Click **OK**.
3. You will receive a Security Alert if you used LOCALHOST to connect. Internet Explorer is warning you that the server certificate does not match the name that you typed. Click **Yes** to continue.
4. You should next see a selection of certificates. Select the certificate that you used in the mapping, and click **OK**. You should be doing this test from the computer on which you installed the certificate originally. Each certificate has a corresponding private key that is stored only on the computer on which you made the original user certificate request.

If the mapping worked you should see the .gif file.

If you see an error, there are a number of possible reasons:

- An access denied message indicates that you are successfully authenticating but that you do not have permissions to access the file. Check the permission on the file to see which account your certificate maps to.
- A certificate-revoked message usually indicates that the certificate has been revoked or that IIS was unable to retrieve a certificate revocation list (CRL). You may need to install the CRL.
- A message that the certificate is not trusted or is invalid usually means you have not installed the roots into the computer's trusted root store on the Web server. A common mistake is to install the roots into the user's trusted

Related Links

Step-by-Step Guide to a Common Infrastructure for Windows 2000 Server Deployment:

Part 1: Installing a Windows 2000 Server as a Domain Controller http://www.microsoft.com/technet/win2000/depprof1.asp

Part 2: Installing a Windows 2000 Professional Workstation and Connecting it to a Domain http://www.microsoft.com/technet/win2000/depprof2.asp

Windows 2000 Server Online Help http://windows.microsoft.com/windows2000/en/server/help/

Windows 2000 Planning and Deployment Guide http://www.microsoft.com/technet/win2000/dguide/home.asp

Exploring Security Services http://www.microsoft.com/windows2000/guide/server/features/securitysvcs.asp

Windows 2000/NT Forum http://computingcentral.msn.com/topics/windowsnt

---