Windows 2000 Server

Step-by-Step Guide to Setting up a Certificate Authority

Introduction

This step-by-step guide will help you set up a public key Certificate Authority (CA) in a network running the Microsoft® Windows® 2000 Server operating system.

A Certificate Authority is a service that issues the certificates needed to run a public key infrastructure. The CA could be an external commercial CA, or it could be a CA run by your company. The certificates enable a user to log on using a smart card, send encrypted e-mail, code-sign documents, and more. Since a CA is an important trust point in an organization, most organizations will have their own CA.

Microsoft Windows 2000 provides two types of CAs, determined by which policy modules are selected during installation—an *enterprise* CA or a *stand-alone* CA. Within these classes, there can be two types of CAs—a *root* or a *subordinate*. The policy modules define the actions that a CA can take when it receives a certificate request. Note that by changing the policy modules, it is possible to change the functionality of the system. A customer can write a policy module and customize the CA's behavior using the Microsoft Platform Software Development Kit (SDK) http://www.microsoft.com/msdownload/platformsdk/sdkupdate/.

Typically, you should install an enterprise CA if you will be issuing certificates to users or computers inside an organization that is part of a Windows 2000 domain. You should install a stand-alone CA if you will be issuing certificates to users or computers outside of a Windows 2000 domain. An enterprise CA requires that all users requesting certificates have an entry in the Windows 2000 Server Active Directory^{TM} services, whereas a stand-alone CA does not. Also, an enterprise CA can issue certificates that are used to log on to a Windows 2000-based domain, and a stand-alone CA cannot.

CAs are organized into hierarchies with the fundamental trust point—or root CA—at the top. All other CAs in the hierarchy are subordinate CAs, and are trusted only because the root is trusted. The enterprise root CA is the trust point in the enterprise. There can be more than one enterprise root CA in a Windows 2000-based domain, and thus more than one hierarchy. It is also possible to mix and match stand-alone and enterprise CAs in a hierarchy to best suit your needs.

Enterprise CAs have a special policy module that enforces how certificates are processed and issued. The policy information used by these modules is stored centrally in a CA object in Active Directory. This means that to set up an enterprise CA, you must have a working Active Directory and DNS server.

In a stand-alone hierarchy, the stand-alone root CA is at the top. Each new stand-alone root CA starts a new hierarchy. Again, it is possible to mix and match stand-alone and enterprise CAs in a hierarchy to best suit your needs.

A stand-alone CA has a very simple policy module and does not assume that Active Directory service is available. However, if Active Directory is available, then the stand-alone CA will take advantage of it.

Certificate Authority Requirements and Prerequisites

This section describes the setup requirements for each type of CA. You must meet all these requirements before installing the CA.

Enterprise Root CA

An enterprise CA is the root of a Windows 2000-based corporate CA hierarchy. You should set up an enterprise CA if the CA will be issuing certificates to users and computers within your corporation. For security reasons, the enterprise CA is typically configured to issue certificates only to subordinate CAs.

The enterprise CA requires the following:

- Windows 2000 DNS Service installed (required by Active Directory).
- Windows 2000 Active Directory installed. Enterprise policy places information into the Active Directory.
- Enterprise administrator privileges on the DNS, Active Directory, and CA servers. This is especially important because setup modifies information in numerous places, some of which require enterprise administrator privileges.

Enterprise Subordinate CA

An enterprise subordinate is a CA that issues certificates within a corporation, but is not the most trusted CA in that corporation. (It is subordinate to another CA in the hierarchy.)

The enterprise subordinate CA requires the following:

- A parent CA. This could be an external commercial CA or a stand-alone CA.
- Windows 2000 DNS service installed (required by Active Directory).
- Windows 2000 Active Directory installed. Enterprise policy places information into Active Directory.
- Enterprise administrator privileges on the DNS, Active Directory, and CA servers.

Stand-alone Root CA

A stand-alone CA is the root of a CA trust hierarchy. You should install a stand-alone root CA if you will be issuing certificates outside of a corporation's enterprise network. A root CA typically issues certificates to subordinate CAs only. For example, you want to issue certificates to your customers so they can access your Web site, and it is not feasible to give each one an account in your directory. Another example is if you intend to lock your root CA in a vault with no network access for security reasons, and want to allow only a few trusted people to access this server.

The stand-alone root CA requires administrator privileges on the local server.

Stand-alone Subordinate CA

A stand-alone subordinate CA is one that operates as a solitary certificate server, or exists in a CA trust hierarchy. You should set up a stand-alone subordinate CA when you will be issuing certificates to entities outside a corporation.

The stand-alone subordinate CA requires the following:

- An association with a CA that will process the subordinate CA's certificate requests. Again, this could be an external, commercial CA.
- Administrative privileges on the local server.

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 One and Two".

The common infrastructure documents specify a particular hardware and software configuration. If you are not using the common infrastructure, you need to take that into account when using this document. All names used throughout this guide are based on that set of instructions.

The most current information about hardware requirements and compatibility for servers, clients, and peripherals is available at the Windows 2000 Product Compatibility site.

Certificate Authority Setup

For the purposes of this step-by-step guide, you must be logged on as an enterprise administrator.

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
2. The **Active Directory Users and Computers** snap-in opens up. In the left pane, under **Reskit.com**, click the **Users** folder.
3. Double-click the **Enterprise Admins** group.
4. In the **Enterprise Admins Properties** dialog, click the **Members** tab, and then click the **Add** button.
5. In the **Select Users, Contacts, or Computers** dialog, click **Mike Nash**, and then click the **Add** button. Click **OK**.
   Mike Nash is now an enterprise administrator with the necessary permissions to set up Certificate Authority in a Windows 2000-based network.
6. Close the **Active Directory Users and Computers** window.

You now need to log on as an enterprise administrator; using our example, log on as Mike Nash.

Note You will also need to log on as an enterprise administrator when setting up the enterprise intermediary and enterprise-issuing certificate computers.

To set up the CA

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components** to start the **Windows Components Wizard**.
4. Select the **Certificate Services** check box and then click **Next**.
5. If you intend to use the Web components of the Certificate Services, ensure that the IIS check box is selected.
6. The wizard prompts you to specify the type of Certification Authority you want to install. Setup attempts to guess which option is selected in order to make installation simpler.
   - If no Active Directory is detected, the two enterprise options are disabled.
   - If an Active Directory is detected, the **Enterprise root CA** option is selected if there are no CAs already registered in the Active Directory.
   - If there are CAs registered in the Active Directory, the **Enterprise subordinate CA** option is selected.

   If you will be issuing certificates to entities in your organization, or if you need to have seamless integration with the Active Directory or to enable smart card logon, select an enterprise CA. Select one of the following:

   - **Enterprise root CA**—This is if you do not have any CAs in your directory, or if you need a second enterprise root CA. The root CA will be registered in the directory, and all computers in your enterprise using that directory will automatically trust the root CA. It is good security practice to limit the root CA to issuing certificates to subordinate CAs only, or to issuing only a few special purpose certificates. This means you want to install an enterprise subordinate after you finish installing the root. However, you can choose only the root CA.
   - **Enterprise subordinate CA**—This is if you have already installed an enterprise root CA. Typically, you will have multiple enterprise-subordinate CAs. Each of these CAs either serves different communities of users or provides different types of certificates. If there is more than one subordinate, it is possible to revoke the subordinate's certificate in case of disaster, and not have to reissue all certificates in the organization.

   If you will be issuing certificates to entities outside your enterprise and do not want to use Active Directory or other Windows 2000 public key infrastructure (PKI) features, then you want a stand-alone CA. Select one of the following:

   - **Stand-alone CA**—This is if you do not already have a stand-alone CA, or if you need a second root for a purpose different than the first.
   - **Stand-alone subordinate CA**—This is if this CA will be a member of an existing CA hierarchy. The parent CA in the hierarchy can be a stand-alone CA, an enterprise CA, or an external commercial CA.
7. If you need to change the default cryptographic settings, select the **Advanced Options** check box. (Select **Advanced Options** only if you know how to change cryptographic settings). Click **Next**.
8. If you selected **Advanced Options**, the wizard prompts you to specify the cryptographic service provider to use. (If you did not select **Advanced Options**, proceed to step 9.)

   In this dialog box, you can change the cryptographic settings, such as the Cryptographic Service Provider (CSP), hash algorithm, and other advanced options. In general, you will not need to modify the default settings. Users who need to modify these settings must be very familiar with cryptography, Certificate Server, and the CAPI 2.0 architecture.

   The list of CSPs will vary depending on the software and hardware that has been installed on the server. The **Key length** specifies the length of the public and private key pair. A value of **Default** in this box generates a key pair whose default length is determined by the selected provider. Microsoft recommends that you use a long key length, such as 1024 or 2048, for a root CA or an enterprise CA. (Note that a long key length is computationally more expensive, and may not be accepted by all hardware devices. For example, some smart cards may not accept certificates issued by a CA that has a 4096 bit key, due to space limitations on the card.)

   The **Use existing keys** option allows you to use keys that were generated previously or to reuse keys from a previously installed CA. When installing a CA, you should almost never reuse keys. The exception to this is when you are restoring a CA after a catastrophic failure. You will then *import* a set of existing keys and install a new CA that uses those keys. In addition, if you are restoring a CA after a failure, you must select the **Use the associated certificate** check box. This ensures that the new CA has a certificate that is identical to the old CA. If you do not check this box, a new certificate will be generated that makes the new CA different from the old CA.

   Note The private key is always stored locally on the server, except in the case where a cryptographic hardware device is used. In such a case, the private key is stored in the device. The public key is placed in the certificate, and in the case of an enterprise CA, the certificate is published in Active Directory.
9. The wizard prompts you to supply identifying information appropriate for your site and organization.
10. Note that the CA name (or common name) is critical because it is used to identify the CA object created in the Directory. The **Valid for** time can only be set for a root CA. Set the root CA **Valid for** time to a reasonable value: the actual duration is a tradeoff between security and administrative overhead. Keep in mind that each time a root certificate expires, an administrator has to update all trust relationships, and administrative steps need to be taken to move the CA to a new certificate. A time period of two or more years is usually sufficient. When you are finished entering the information, click **Next**.

11. A dialog box defines the locations of the certificate database, configuration information, and the location where the Certificate Revocation List (CRL) is stored. The Enterprise CA will always store its information, including the CRL, in the directory. It is recommended that you select the **Shared folder** check box. This option specifies the location of a folder where configuration information for the CA will be stored. You should make this folder a UNC path and have all your CAs point to the same folder. Then the administration tools can use this folder for determining CA configuration if the Active Directory is not available. If you have an Active Directory, this folder is optional. If you do not have an Active Directory, this folder is required.

    If you are installing a CA in the same location as a previously installed CA, the **Preserve existing certificate database** option will be enabled. Check this option if you wish your new CA to use this database; otherwise, the database will be deleted.

    When you have specified the storage locations for your information, click **Next**.
12. If IIS is running, a message will prompt you to stop the service. Click **OK** to stop IIS. You must stop IIS to install the Web components. If you do not have IIS installed, you will not see this message.
13. If you are installing a subordinate CA, the wizard next prompts you for information about how you will request the certificate. Click **Browse** to locate an online CA, or select **Save the request to a file** if you will be making a request destined for a commercial CA or a CA that is not accessible from the network. (If you create a file, you must take the file to a CA for processing. The CA provides you with a certificate, which you install using the MMC snap-in.) Click **Next**.
14. If you saved a certificate request to a file, a dialog box called **Microsoft Certificate Services** will display. Click **OK** to finish the installation. Click **Finish** to close the wizard.

When the installation is complete, take the Certificate Request file you created to your CA for processing. If you are using a Microsoft Certificate Service to process this file, you can refer to the Step-by-Step Guide to Certificate Service Web Pages for details about processing the request.

When you have your new certificate, you can use the Certificate Authority MMC snap-in to install the certificate and enable your CA.

Verify Certificate Server Installation

Whether you created an enterprise CA or a stand-alone CA, you can quickly check to see if your installation was successful.

The simplest way is to open a command window, and type **net start** to see if the Certificate Service is running.

- For an enterprise CA, open the Certificate snap-in. Click **Start**, point to **Programs**, point to **Administrative Tools**, select **Certificate Authority**, and request a certificate.
- For a stand-alone CA, you can request a new certificate using Microsoft Internet Explorer 5 by connecting to the URL http://*Localhost*/CertSrv. Replace *localhost* with the name of the server. See the Step-by-Step Guide to Certificate Service Web Pages for details.

Removing Certificate Services

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components**, and the **Windows Components** wizard appears.
4. Clear the **Certificate Services** check box, and click **Next**.

Installing a Subordinate CA Certificate from a File

This section is to be used only by people who created a certificate request file during installation of a subordinate CA.

Before you begin this section, take the certificate request file to your CA for processing. Your CA will provide you with a certificate for this file. If you are submitting this file to a Microsoft Certificate Service, refer to the Step-by-Step Guide to Certificate Service Web Pages for detailed instructions on how to submit the request file.

This section uses the Certificate Services snap-in. Refer to the Step-by-Step Guide to Advanced Certificate Management http://www.microsoft.com/TechNet/prodtechnol/windows2000serv/deploy/confeat/advcert.asp for more details.

1. Open the **Certificate Services** snap-in.
2. Right-click the CA you want to install.
3. Click **Install CA Certificate**. The **Install CA Certificate** wizard appears.
4. Follow the wizard, and select the file containing the certificate provided by your CA.
5. Click **Finish** to complete the setup.

Your CA is now installed and ready for verification.

Notes

Stand-Alone Policy Behavior

Certificate Server stand-alone policy behavior has changed. In the past, the default policy module immediately processed requests and issued the certificate. The new stand-alone policy makes the request pending until an administrator manually approves the request. This new behavior affects the stand-alone CAs only. Enterprise policy still processes the request immediately.

Installing Web Pages on a Remote Server

If the CA is an enterprise CA, the Certificate Services Web pages must be installed on the same computer as the CA. The CA needs to authenticate the client to ensure that it can request only the certificates that the client has permission to request. If the Web pages are on a different computer from the Web server, then the CA cannot authenticate the user.

Installing the CA and Web Server

The CA must be installed after the Web server to ensure that the Web pages are installed. If the CA is installed first, it still functions, but you may not be able to access the Web pages. You can enable the Web pages by running the command:

```
certutil -vroot
```

Upgrading Certificate Server 1.0

When you upgrade from Windows NT Server 4.0 to Windows 2000, the Certificate Services executable and dynamic-link library (DLL) files must be updated. Note that it is important to run the Dbcnvt.exe utility to convert the old version 1.0 database to the new format before the CA processes any new requests. Upgrades are not supported for any configuration that uses a version 1.0 database that has been modified.

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/prodtechnol/windows2000serv/howto/depprof1.asp

Part 2: Installing a Windows 2000 Professional Workstation and Connecting it to a Domain
http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/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/prodtechnol/windows2000serv/reskit/deploy/sdgintro.asp

Exploring Security Services http://www.microsoft.com/windows2000/technologies/security/default.asp

---

Send feedback to Microsoft