How the Active Directory Installation Wizard Works

In this section

- Active Directory Installation Wizard Architecture
- Active Directory Installation Methods
- Active Directory Installation Wizard Prerequisites
- Active Directory Installation Wizard User Interface
- Active Directory Installation Wizard Directory Configuration Process
- Active Directory Removal
- Related Information

This section details the architecture of the Active Directory Installation Wizard, methods for invoking the wizard, and the directory configuration process. This section also details the removal of Active Directory from a domain controller.

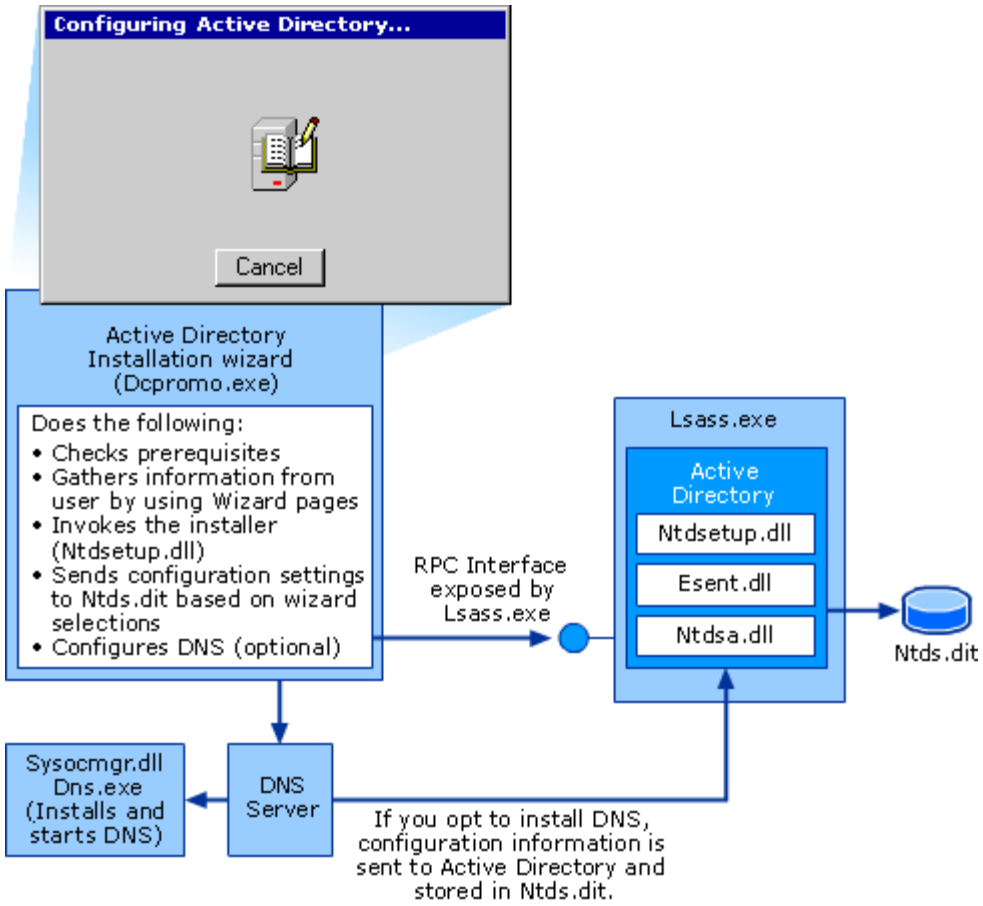
You can use the Active Directory Installation Wizard to install Active Directory on a computer, making that computer a domain controller. Before installing Active Directory to create the first domain controller in a forest, ensure that your network is online and functioning properly and that you have designed your Domain Name System (DNS) namespace and have a plan for installing and configuring DNS.

Back to Top

Active Directory Installation Wizard Architecture

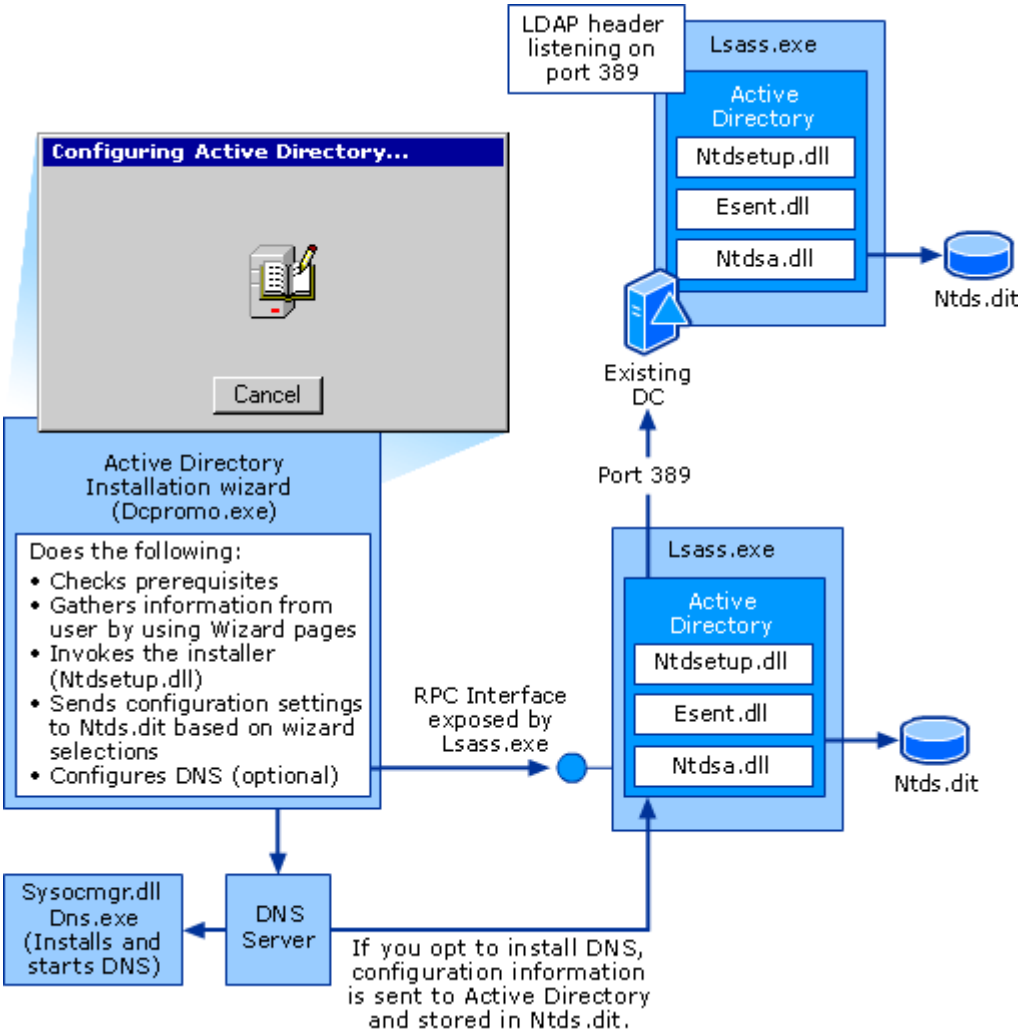
The Active Directory Installation Wizard (Dcpromo.exe) architecture verifies that certain prerequisites are met prior to an Active Directory installation, gathers information specific to your operating environment, and configures Active Directory. It works differently depending on the installation scenario you choose and the installation method you are using. The following figures illustrate how the Active Directory Installation Wizard works when creating the first domain controller in a forest, an additional domain controller in an existing domain, and the installation process when installing Active Directory from media, which is a new feature in Windows Server 2003 Active Directory.

Active Directory Installation on the First Domain Controller in a Forest



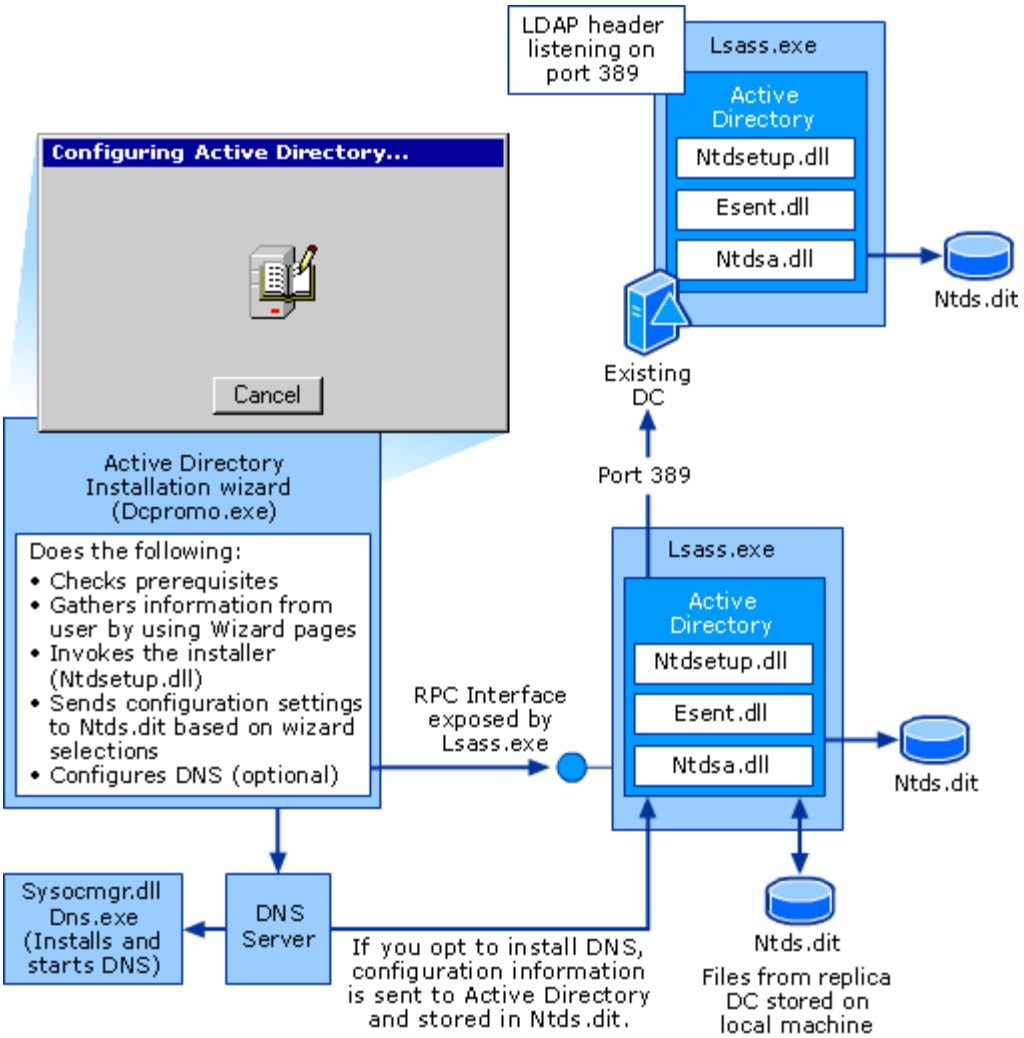
When you install Active Directory on a computer that is the first domain controller in a forest, the Active Directory Installation Wizard checks prerequisites and gathers information from you through the wizard user interface. It invokes the Active Directory installer (Ntdsetup.dll) through a remote procedure call (RPC) interface, exposed by the Lsass.exe security subsystem, to install the first domain controller in the forest. As the installer works, directory information is written to the Ntds.dit file by Esent.dll. If you select the option to install DNS, the Active Directory Installation Wizard contacts the DNS Server service, which in turn accesses Sysocmgr.exe and Dns.exe, the components that install and start DNS. After the Active Directory installation is complete and the computer restarts, the DNS Server service configures the Active Directory–integrated DNS zones and sends the DNS configuration information back to Active Directory.

Active Directory Installation on an Additional Domain Controller in an Existing Domain



When you install an additional domain controller in an existing forest, the Active Directory Installation Wizard checks prerequisites, gathers information from you through the wizard user interface, and invokes the Active Directory installer (Ntdsetup.dll) through an RPC interface exposed by the Lsass.exe security subsystem. The installer contacts an existing domain controller. The existing domain controller replicates all domain, forest, and directory partition information back to the new domain controller. As the installer works, directory information is written to the Ntds.dit file by Esent.dll. If you select the option to install DNS, the Active Directory Installation Wizard contacts the DNS Server service, which in turn accesses Sysocmgr.exe and Dns.exe, the components that install and start DNS. After the Active Directory installation is complete and the computer restarts, the DNS Server service configures the Active Directory–integrated DNS zones and sends the DNS configuration information back to Active Directory.

Active Directory Installation from Media



When you install Active Directory on an additional domain controller from backup media, the Active Directory Installation Wizard checks prerequisites, gathers information from you through the wizard user interface, and invokes the Active Directory installer (Ntdsetup.dll) through an RPC interface exposed by the Lsass.exe security subsystem. As the installer works, directory information is written to the Ntds.dit file by Esent.dll. When you install from backup media, all domain information is backed up from a domain controller in the same domain and restored to the local machine. The installer accesses the restored files to configure the directory service. A domain controller is contacted over the network to replicate any changes that have been made since the backup media was created. The result is less information being sent over the network and a faster Active Directory installation. If you select the option to install DNS, the Active Directory Installation Wizard contacts the DNS Server service, which in turn accesses Sysocmgr.exe and Dns.exe, the components that install and start DNS. After the Active Directory installation is complete and the computer restarts, the DNS Server service configures the Active Directory–integrated DNS zones and sends the DNS configuration information back to Active Directory.

The architectural components in each of the preceding diagrams are explained in the following table.

Active Directory Installation Wizard Architectural Components

Component	Description
Dcpromo.exe	The Active Directory Installation Wizard.
Lsass.exe	The LSA security subsystem, which provides services to both the kernel mode and the user mode for validating access to objects, checking user privileges, and generating audit messages.
Ntdsetup.dll	The Active Directory installer.
Esent.dll	Extensible storage engine (ESE). Communicates directly with individual records in the directory data store on the basis of the object's relative distinguished name attribute.
Ntdsa.dll	The directory service module that supports the Windows Server 2003 replication protocol and Lightweight Directory Access Protocol (LDAP), and manages partitions of data.

Ntds.dit	Directory database or data store. Requires NTFS formatting and is manipulated only by the ESE database engine. Encryption of the Ntds.dit file or related log files, their parent folders, or storage drive is not recommended and not supported.
Schema.ini	Contains the information necessary for creating the default directory objects and the default security for the Ntds.dit, as well as the Active Directory display specifiers.
Dns.exe	The executable from which the DNS Server service is run.
Sysocmgr.exe	The System Optional Component Installation Manager interprets INF files and installs optional components such as the DNS Server service.

Back to Top

Active Directory Installation Methods

You can install Active Directory using any of the following four methods:

- Install from the command line
- Install from the Configure Your Server Wizard
- Install unattended by using an answer file
- Install from media

Installing from the Command Line

You can initiate an Active Directory installation from the command line any time after Windows Server 2003 has been installed. To install Active Directory by using the command line, in the Run dialog box, type **dcpromo** and click **OK**.

Installing from the Configure Your Server Wizard

You can install Active Directory at any time by using the Configure Your Server Wizard. The Manage Your Server dialog box automatically appears when you restart the server after installing Windows Server 2003. To invoke the Configure Your Server Wizard, select **Add or remove a role**. Select the **Domain Controller (Active Directory)** role in the Configure Your Server Wizard, and then click **Next**. The Active Directory Installation Wizard starts.

Installing Unattended by Using an Answer File

You can run the Active Directory Installation Wizard without having to be present to answer the questions by using an answer file. An answer file is a text file that you populate with the parameters that the wizard needs to install Active Directory. You can use an answer file to install Windows Server 2003 and include the options necessary to subsequently install Active Directory. Alternatively, you can create an answer file that contains only the options necessary for installing Active Directory. These parameters include the domain controller type (additional domain controller for an existing domain or a new domain controller for a new domain), the configuration of the domain that is being created (new forest, new tree root, or new child) and Active Directory forest and domain functional levels.

The answer file options for installing Active Directory are in the DCInstall section of the Unattend.txt file. You can find instructions for creating an answer file for an Active Directory installation in the Deploy.cab file in the Support\Tools folder on the Windows Server 2003 product CD. Inside the Deploy.cab file, open Ref.chm to access the Unattend.txt file. In the left pane, expand **Unattend.txt**, and click **DCInstall**. In Windows 98, Windows 2000, and Windows Server 2003, use Windows Explorer to extract this document. In Windows 95 and earlier, or from MS-DOS, use the **Extract** command to open the file. You can rename the Unattend.txt file and save it in any location. The Unattend.txt file also contains sample answer files. After creating the answer file, append the **/answer** switch to the **dcpromo** command when installing Active Directory from the command line.

You can run this answer file after Windows Server 2003 setup is complete and after you have logged on to the system.

Installing from Media

When you install from media, you can pre-populate Active Directory with system state backup data from an existing Windows Server 2003–based domain controller that belongs to the same domain in which this server will become an additional domain controller. This backup can be stored on a local CD, DVD, or hard disk partition. Then, the system state backup must be restored locally on the server you are installing Active Directory on. When the data is restored, proceed with the Active Directory installation.

To install Active Directory from media, append the **/adv** switch to the **dcpromo** command when installing from the command line to enable install from media options in the Active Directory Installation Wizard.

When you select the option to copy domain information from backup files, you must identify the location of the files. If the domain controller from which you restore the system state data is a global catalog server, you have the option make this new domain controller a global catalog server. Once you have selected an option, the wizard proceeds with the installation.

The install from media feature in Windows Server 2003 reduces the time required to install directory information by reducing the amount of data that is replicated over the network. Installing from media is most beneficial in environments with very large domains or for installing new domain controllers that are connected by a slow network link. If the computer on which Active Directory is being installed is located in close proximity to another domain controller and the network connections are optimal, installing from media will only be slightly faster than copying the information over the network.

When you install Active Directory on Windows 2000 Server, the computer has to populate its entire directory service with directory information replicated from another domain controller, which requires time for the replication to occur across the network.

Back to Top

Active Directory Installation Wizard Prerequisites

The Active Directory Installation Wizard confirms several configuration and security parameters before it begins collecting information from you. The following prerequisites must be met before an Active Directory installation proceeds:

- An installation or removal operation of Active Directory must not already be in progress.
- Command line parameters must be correct if you are installing from media or using an answer file.
- You must be logged on to the local computer as a member of the Administrators group. If the credentials provided at logon are insufficient, you cannot continue.
- Certificate Services must not be installed on the computer. Changing the computer name or domain membership of a certification authority (CA) invalidates the certificates that are issued from that CA. Uninstall Certificate Services and reinstall after the Active Directory installation is complete.
- The computer must be running in normal mode. If the computer is running in safe mode, an error message advises you to restart in normal mode.
- If you have previously removed Active Directory from the computer, and you are attempting a new Active Directory installation, you must restart the computer before the new installation proceeds.
- The computer must be running Windows 2000 Server, Windows Server 2003 Standard Server, Windows Server 2003 Enterprise Server, or Windows Server 2003 Datacenter Server.
- At least one logical disk drive must be formatted with the NTFS file system. You can only install the SYSVOL shared folder on a drive that is formatted with NTFS and we also recommend installing the Active Directory database on an NTFS formatted drive.
- There must be sufficient free disk space on the computer. The Active Directory Installation Wizard requires at least 20 MB of free disk space on the computer or it does not proceed. For more information about the disk space requirements for installing Active Directory, see "What is the Active Directory Installation Wizard?."
- If the computer's name has been changed, you must restart it after the name change for the wizard to proceed. The wizard also checks to see that the computer name conforms to DNS naming requirements.
- If Terminal Server is running on the computer, a warning indicates that installing Active Directory on a computer running Terminal Server changes the local security policy, allowing only administrators to log on to the computer. You can cancel the wizard and remove Terminal Server.

After all installation prerequisites are met, the Active Directory Installation Wizard continues with the user interface portion of the installation process.

Back to Top

Active Directory Installation Wizard User Interface

Use the user interface portion of the wizard to select the type of domain controller you want to create and to

gather specific information about your environment for the proper configuration of that domain controller.

Verifying Client Operating System Compatibility

Domain controllers running Windows Server 2003 have improved security settings that might affect clients that are running older versions of Windows. Server message block (SMB) packet signing and secure channel signing are security policies that are enabled by default on domain controllers running Windows Server 2003.

Clients running Windows NT 4.0 with Service Pack 2 or earlier, and clients running Windows 95 without the Directory Service Client Pack, do not support SMB packet signing and cannot authenticate to a domain controller running Windows Server 2003.

Clients running Windows NT 4.0 with Service Pack 3 or earlier do not support secure channel signing. These clients cannot establish communications with a Windows Server 2003–based domain controller. To ensure successful communication, upgrade these clients to a later version of the Windows operating system or service pack. However, if you cannot upgrade your clients, you must disable secure channel signing on all domain controllers running Windows Server 2003 so that the traffic passing through the secure channel does not need to be signed or encrypted.

Note

- Secure channel signing does not affect Windows 95 clients.

Choosing Additional Domain Controller or Member Server

When you upgrade an existing Windows NT 4.0 backup domain controller (BDC) to Windows Server 2003, the Active Directory Installation Wizard executes immediately when the operating system upgrade is complete and gives you the following options:

- Install Active Directory, creating an additional domain controller in the domain.
- Convert the BDC to a member server joined to the domain.

Important

- You must upgrade and install Active Directory on the Windows NT 4.0 primary domain controller (PDC) in a domain before you can install Active Directory on a Windows NT 4.0 BDC.

Copying Domain Information

If you are creating an additional domain controller in an existing domain and you are installing Active Directory by using the install from media installation method, the Copying Domain Information page appears in the wizard. This wizard page, rather than the /adv switch used with the dcpromo command, determines how the Active Directory installation is performed. This wizard page presents you with the following options for copying domain information:

- Over the network from a domain controller
- From these restored backup files

The **Over the network from a domain controller** option simply performs the standard Active Directory installation without using any backup media. If you want to install from media, you must select **From these restored backup files**. Copying the restored information from local media is the recommended option and will result in a faster Active Directory installation.

Providing the System Key

If you are installing from media and system key protection was enabled on the domain controller from which you created the system state backup, the Active Directory Installation Wizard looks for the system key in the restored Active Directory files and prompts you accordingly:

- If the system key was stored on the domain controller's hard disk, the system key is stored in the backup files and available to the wizard and you are not prompted for it.
- If a system key password was set on the domain controller, then the same password is set on the system key in the backup files and the wizard prompts you for the password.
- If the system key for the domain controller was stored on a floppy disk, then the system key is not present in the backup files. The wizard prompts you for the floppy disk that contains the system key.

Configuring the Global Catalog

If you are installing from media by using the system state backup of a global catalog server, you will be asked if you want to configure the new domain controller as a global catalog server as well.

You can designate a domain controller as a global catalog server at any time by using the Active Directory Sites

and Services console. Therefore, you do not need to specify whether a domain controller will be a global catalog server during the Active Directory installation. However, if a global catalog server is required in the site in which you are installing the domain controller, designating the domain controller as a global catalog server during the Active Directory installation eliminates the additional configuration step.

Contacting an Active Directory Domain Controller

If you upgrade a Windows NT 4.0 BDC to Windows Server 2003 and then install Active Directory, the domain controller must be able to contact an Active Directory domain controller for the domain of which it was previously a member. If this is the first Windows NT 4.0 BDC being upgraded, the PDC must have already been upgraded and the BDC must be able to contact it. If this is an additional BDC, it must be able to contact either the PDC or another domain controller from its domain. If the BDC successfully contacts an Active Directory domain controller for the domain, the wizard proceeds without any notification.

If the domain controller is not able to successfully contact an Active Directory domain controller, but is able to contact a non-directory service (pre-Windows 2000) domain controller, it might be for one the following reasons:

- The primary domain controller (PDC) for the domain of which the BDC was a member has not been upgraded to Windows Server 2003.
- Network configuration or connectivity problems are preventing a domain controller from being contacted.

If the BDC cannot contact the PDC for any of the above reasons, the Cannot Contact an Active Directory Domain Controller wizard page will advise you of the issue. You can either stop to investigate and correct the problem before continuing, or choose the option to make the BDC a member server in the Active Directory domain.

Providing Network Credentials

To create a new domain controller in an existing forest, the Active Directory Installation Wizard requires that you provide valid network credentials in the form of a user name, password, and domain name. The wizard accepts the user name in the form of a logon user identifier – for example, johnSmith – or in the form of domain\user name. We do not recommend using a user principal name (UPN) formed as johnSmith@*domainName.*

- To create an additional domain controller for an existing domain, you must provide credentials for a member of either the Enterprise Admins group or the Domain Admins group for the domain to which you are adding the additional domain controller.
- To create a child domain in an existing domain tree, you must provide credentials for either a member of the Enterprise Admins group or an account that has been delegated the authority to create the new child domain by a member of the Enterprise Admins group.
- To create a new tree-root domain, you must you must provide credentials for either a member of the Enterprise Admins group or an account that has been delegated the authority to create the new tree-root domain by a member of the Enterprise Admins group.

Note

- Network credentials are not required to create a new forest. The Active Directory Installation Wizard skips this step and immediately prompts you to enter a valid DNS name. All other configurations require you to provide network credentials before entering a valid DNS name.

Providing a New Domain Name

To create a domain controller in a new domain, you must provide a DNS name for the new domain. Acceptable naming conventions for domain names include the letters A through Z, numerals 0 through 9, and a hyphen (-). A dot (.) separates the discrete parts of a domain name, commonly known as labels. Each domain label cannot be longer than 63 bytes. Fully qualified domain names cannot:

- Have a single label.

Note

- DNS names that do not contain a dot (.) cannot be registered on the internet and require additional configuration to be dynamically registered by DNS clients.
- Contain embedded spaces.
- Be solely numeric.

To create a new child domain, you must provide the full DNS name of a parent domain. The wizard verifies that the parent domain exists. If the wizard does not recognize the DNS name of the parent domain, an error message states that the specified domain could not be contacted and that you should verify that the DNS name is typed correctly. If the DNS name of the parent domain is correct, there might be a problem with your DNS configuration.

The Active Directory Installation Wizard uses the domain controller Locator to verify that the DNS name is unique

in the forest.

Generating a NetBIOS Domain Name

The Active Directory Installation Wizard generates a NetBIOS name from a valid DNS domain name, except when upgrading a Windows NT 4.0 PDC. When you upgrade a PDC running Windows NT 4.0, the NetBIOS name by default is the previous NetBIOS name of the domain and you cannot select a new name.

NetBIOS-created names have a 15-character limit. If your existing Windows NT 4.0 domain name is 15 characters in length, and your new domain name is more than 15 characters, the NetBIOS name truncates at the 15-character limit. If your domain name is truncated this way, a new NetBIOS name is created that is identical to your previous Windows NT 4.0 domain name, and domain creation fails. Domain creation also fails if your previous NetBIOS name contains embedded spaces; however, the Active Directory Installation Wizard ignores leading and trailing spaces.

In all other installation scenarios, the Active Directory Installation Wizard prompts you to either change or accept the NetBIOS name that is derived from the domain name. The wizard then uses the domain controller Locator to verify that the NetBIOS name that you have accepted is unique on the network.

Using DNS Registration Diagnostics

If you are installing Active Directory to create the first domain controller in a new forest, DNS must be installed on your computer. If you are installing an additional domain controller in an existing domain, DNS must be configured properly on your network. If DNS is not installed on the computer, the wizard prompts you to configure the DNS client and does not proceed until the configuration is complete. After the wizard verifies that the DNS client is installed, it proceeds with the Active Directory installation. During the Active Directory installation, DNS diagnostic tests verify that your DNS configuration supports Active Directory. The tests validate the full DNS name, verify that the appropriate DNS SRV resource records exist, and report the most common DNS misconfiguration scenarios.

For more information about DNS SRV resource records, see "How DNS Support for Active Directory Works."

When you install Active Directory on the first domain controller in a new domain, the Active Directory Installation Wizard performs a DNS query for the DNS name of the Active Directory domain specified in the wizard. The DNS query ensures that network hosts and services can locate the domain controller hosting the Active Directory domain. The wizard queries the DNS servers configured for its network connection for the start of authority (SOA) resource record for the zone that contains the DNS name of the Active Directory domain. After the SOA resource record is received and the name of the primary server is extracted from the response, the new domain controller queries DNS for the address (A) resource record for the primary DNS server name. After the new domain controller determines the IP address of the primary DNS server, it sends a dynamic update request to determine whether or not the DNS server exists and is capable of accepting DNS dynamic updates.

When you install Active Directory on an additional domain controller in an existing domain, a DNS server running on the network is assumed and a search for an authoritative DNS server is not performed.

The results of these diagnostic tests are displayed on the DNS Registration Diagnostics page of the Active Directory Installation Wizard. If the wizard detects a problem with the DNS configuration, it provides details about the problem. You can use the information provided on this page to repair the problem and run the wizard again.

If DNS is not installed on the computer, you are given the option to install it now or after the Active Directory installation has completed. If you choose to install DNS during the Active Directory installation, a DNS server is installed locally and configured with a primary DNS zone that matches the name of the new Active Directory domain. The wizard configures DNS to accept dynamic updates and to modify the computer's IP configuration so that the domain controller points to its local DNS server as the preferred DNS server.

Verifying Active Directory Forest and Domain Functional Levels

Windows Server 2003 forest and domain functional levels provide a system for safely enabling new Windows Server 2003 features. Before you can install Active Directory, the Active Directory Installation Wizard ensures that the domain or forest can support the domain controller.

For example, if the forest functional level is Windows Server 2003, you cannot create a new domain on a Windows 2000–based server. Similarly, if the domain functional level is Windows Server 2003, you cannot install Active Directory on a Windows 2000–based server to create an additional domain controller in an existing domain. The system also prevents restoring a domain controller with information from a domain controller that has an incompatible functional level.

When upgrading a PDC running Windows NT 4.0 and configuring it as the first domain controller in a new forest, the Active Directory Installation Wizard prompts you to raise the forest functional level to Windows Server 2003 interim, because it is assumed that the forest does not contain Windows 2000 domain controllers. The Windows Server 2003 interim forest functional level allows only Windows Server 2003–based and Windows NT 4.0–based domain controllers to co-exist in a forest.

After all Windows NT 4.0 PDCs and BDCs are upgraded to Windows Server 2003, the forest functional level can be

raised to Windows Server 2003.

When you upgrade from Windows 2000 to Windows Server 2003, the Active Directory Installation Wizard does not prompt you to raise the forest functional level. After an upgrade or clean installation of a Windows Server 2003–based domain controller, the default domain functional is Windows 2000 mixed and the default forest functional level is Windows 2000. These functional levels allow for the existence of domain controllers running Windows Server 2003, Windows 2000 or Windows NT 4.0. Functional levels can be raised manually when conditions in the domain or forest are appropriate.

For more information about functional levels, see "Active Directory Functional Levels Technical Reference."

Selecting a Location for Database and Log Folders

The Active Directory Installation Wizard displays the default location for the Active Directory database (Ntds.dit), and log files and enables you to specify an alternative location or accept the location provided.

During Windows Server 2003 installation, the Ntds.dit Active Directory database template is placed in a default location, the %*systemroot*%\System32 directory. In this location, the Ntds.dit database template does not function as the directory database; it exists as a template that is used to create the user's Active Directory database files when Active Directory is installed. The Ntds.dit template enables you to install Active Directory without using the Windows Server 2003 product CD.

We recommend that you install the Ntds.dit database template on an NTFS volume. For optimal domain controller performance, select separate physical hard disks for the Ntds.dit database template and the Active Directory log files.

Selecting a Location for the Shared System Volume

The Active Directory Installation Wizard displays the default location for the system volume (SYSVOL) and enables you to specify an alternative location or accept the location provided. An NTFS volume is required for the SYSVOL shared folder.

For optimal performance on domain controllers that are accessed by more than 1,000 users, place the log files on one physical hard disk and keep the SYSVOL shared folder and the Ntds.dit database together on a separate physical hard disk.

Assigning Permissions to User and Group Objects

When you create a domain controller for a new domain, the Active Directory Installation Wizard prompts you to select default permissions for user and group objects. It provides you with the following two options:

- **Permissions compatible with pre-Windows 2000 Server operating systems**
- **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**

Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems is the default selection and adds the Everyone security identifier (SID) and the Anonymous Logon SID to the Pre-Windows 2000 Compatible Access local group. The Pre-Windows 2000 Compatible Access local group has access to the user and group object attributes that existed in Windows NT 4.0 and that are required by certain applications to function with Active Directory.

If you include the Everyone SID in an ACL or group membership in Windows 2000 or earlier operating systems, you allow authenticated users, guest users, and anyone with an anonymous logon to gain access to many resources. In Windows Server 2003, the Everyone SID no longer allows access to anonymous users. This change was made to disallow inappropriate access to resources by anonymous users and to avoid granting accidental access to anonymous users.

Note

- The Everyone SID contains an access token for every user account in the forest, including the Guest account. The Anonymous Logon SID contains only an access token for anonymous users. Select the **Permissions Compatible with pre-Windows 2000 servers** option to populate the Pre-Windows 2000 Compatible Access group with both SIDs.

In Windows Server 2003, the Anonymous Logon SID was created for backward compatibility with any pre-Windows 2000 application requiring less strict permissions than those granted by Windows 2000–based and Windows Server 2003–based domain controllers. For example, if you have Windows NT 4.0–based Remote Access service servers that are running on Windows NT 3.*x* or Windows NT 4.0–based computers, or if these applications are running on Windows 2000 or Windows Server 2003 computers that are located in a Windows NT domain, choose the **Permissions compatible with pre-Windows 2000 servers** option to add the Anonymous Logon SID to the pre-Windows 2000 Compatible Access local group so that the user and group object attributes that existed in Windows NT 4.0 can be accessed.

Choose Permissions compatible only with Windows 2000 or Windows Server 2003 only if all of your

server-based applications are running on Windows 2000–based or Windows Server 2003–based servers that are members of Windows 2000 or Windows Server 2003 domains. This option prevents the Pre-Windows 2000 Compatible Access group from being populated. This group remains empty when high-security is required in pure Windows 2000 and Windows Server 2003 environments.

Providing an Administrator Password

When you upgrade a Windows NT 4.0 BDC and select the member server option to make the computer a member server in the new Active Directory domain, you are electing to place the computer in a new role as a member server in the new Active Directory domain. As part of this process, all users and groups that were previously created on the computer are deleted and all built-in groups are recreated. After this conversion process completes, the previous Windows NT 4.0 administrator account is no longer valid, and a new password is necessary to access the new administrator account. You must assign a new server administrator password that will have access to the newly created groups.

Providing a Directory Services Restore Mode Administrative Password

On every new domain controller, whether it has been upgraded from a Windows NT 4.0–based domain controller or it was made a domain controller after a clean installation of Windows Server 2003, the Active Directory Installation Wizard prompts you for an Administrator account password that is to be used for authenticating to the Security Accounts Manager (SAM) database when the computer is started in Directory Services Restore Mode.

Starting a domain controller in Directory Services Restore Mode causes the domain controller to temporarily operate as a stand-alone server. When operating in this mode, the SAM database uses a minimal set of user and group definitions stored in the registry.

Summary

The Active Directory Installation Wizard enables you to review and confirm the configuration options you selected and enables you to move back through the wizard and make corrections. After you verify your Active Directory configuration settings, click **Next** to complete the interactive portion of the Active Directory Installation Wizard and begin the directory service configuration.

Back to Top

Active Directory Installation Wizard Directory Configuration Process

After gathering all necessary information from the user, the Active Directory Installation Wizard begins the configuration of the directory.

Creating the SYSVOL Shared Folder

When you create a domain, the Active Directory Installation Wizard also creates the SYSVOL folder, which contains the shared system volume, SYSVOL. SYSVOL provides a default location for files that must be shared throughout an Active Directory domain. SYSVOL creation requires an NTFS volume. Active Directory does not function if the SYSVOL folder is not properly configured and shared. When it is created, the SYSVOL folder is shared automatically by the Net Logon service.

The SYSVOL folder also includes the NETLOGON shared folder. The NETLOGON shared folder includes system policies and user-based logon and logoff scripts for network clients that do not run Windows 2000 or Windows Server 2003. On servers that are upgraded from Windows NT 4.0, files that were located in the original NETLOGON shared folder (\\%systemroot%\SYSTEM32\REPL\Import\Scripts) are moved to the \\<DomainName>\SYSVOL\<FullyQualifiedDomainName>\Scripts folder in the SYSVOL tree.

The SYSVOL folder also includes:

- File system junctions.
- User logon, logoff, startup, and shutdown scripts.
- Windows 2000 and Windows Server 2003 Group Policy objects.
- File Replication service (FRS) staging directories and files.

  FRS replicates the SYSVOL shared folder. After Active Directory is installed and the domain controller is restarted, FRS actually creates the system volume objects in the system volume directory and enables replication of the SYSVOL shared folder on the domain controller. The new domain controller advertises itself in DNS as a domain controller only after SYSVOL is replicated to all domain controllers in the forest.

Creating Directory Partitions

The Active Directory Installation Wizard copies the Ntds.dit Active Directory database template from its location in the *%systemroot%*\System32 directory to the destination specified in the wizard and configures the local server to host the directory service. This process includes the creation of the directory partitions and the default domain security principals.

The Ntds.dit Active Directory database template includes a default copy of the schema, and the schema.ini file, which specifies the default structure of the configuration and domain directory partitions. The Ntds.dit template is used in the following manner:

- When you install Active Directory on a computer that is going to be the root of a forest, the Active Directory Installation Wizard uses the default copy of the schema and the information in the schema.ini file to create the new Active Directory database.
- When you install the first domain controller in a new domain that is not the root of the forest, the wizard synchronizes the schema and configuration directory partitions with the schema and configuration directory partitions of the forest root. From the Ntds.dit template, only the information in the schema.ini file that specifies the structure of the domain directory partition is used.

The following directory partitions are created as default partitions on the first domain controller in a forest, and they are updated through replication on every subsequent domain controller that is created in the forest:

- The schema directory partition is created as cn=schema,cn=configuration,dc=*forestRootDomain*. The schema.ini file is used to create default directory objects, and display specifiers, which are the containers of objects that describe how your Active Directory Users and Computers administrative console appears. Schema.ini implements default security on the directory database.
- The configuration directory partition is created as cn=configuration,dc=*forestRootDomain*.
- The domain directory partition is created as dc=*domainName* and contains the security principals for the domain.

  If you install a new domain controller from a backup of an existing domain controller by using **dcpromo /adv**, the domain directory partition is restored from the backup media onto the new domain controller.
- Two DNS application directory partitions below the forest root domain are automatically created by the DNS Server service when the computer restarts after the Active Directory Installation Wizard has finished. One application directory partition is created for the forest, ForestDnsZones, and one for the domain, DomainDnsZones. You can use the DNS administrative tool or the dnscmd.exe command-line tool, located in the \Support\Tools directory on the Windows Server 2003 product CD, to use these application directory partitions for DNS zone storage.

  Note
  - If you are installing an additional domain controller in an existing forest, the domain controller holding the domain naming operations master role must be online, available, and running Windows Server 2003 for these application directory partitions to be created. If the domain naming master is unavailable or is running Windows 2000, the DNS Server service will attempt to create the application directory partitions again at a later time.

  When you install Active Directory from media, it appears as if the application directory partitions are restored from the backup media during Active Directory installation, even though the application directory partitions that were present on the backup media are deleted. However, if the new domain controller is configured as a DNS server, DNS recreates the DNS application directory partitions after the Active Directory installation.

Replicating Directory Partitions

When you create a new domain in an existing forest, the schema and configuration directory partitions are updated on the new domain controller through replication from a source domain controller and a new domain directory partition containing all of the default domain objects is created.

Note
- All data replicated during the installation of Active Directory is compressed. After you have completed the wizard and the domain controller is restarted, the Knowledge Consistency Checker (KCC) reconfigures compression according to site boundaries.

When you install an additional domain controller in an existing domain, all three directory partitions are updated through replication from a source domain controller. Because of the large amount of data that must be synchronized when you install an additional domain controller, you might opt to delay full replication until the computer is restarted. To stop the replication process, click the **Finish Replication Later** button when it appears. Clicking the **Finish Replication Later** button causes only critical information, such as the schema directory partition, the configuration directory partition, and some objects from the domain directory partition, to replicate.

After these critical items replicate and the computer restarts, replication continues as part of the normal replication activity of the domain controller. The domain controller does not advertise itself as such until replication completes.

The computer on which you install Active Directory uses the domain controller Locator to find a domain controller in the parent domain (for a new child domain) or in its own domain (for an additional domain controller in an existing domain) to act as the source domain controller for replication. The computer queries the source domain controller for the distinguished names of the Configuration container and the Schema container by posting an LDAP query that is based on the NULL distinguished name, which retrieves the root attributes of the Active Directory tree. The source domain controller replicates the schema directory partition and configuration directory partition (in that order), referenced only by their distinguished names. After the directory partitions have been replicated to the computer on which you are installing Active Directory, the GUIDs of the containers are established from the replicated data, although the directory partitions continue to be referenced solely by the distinguished name string for the duration of the installation process.

Failure to fully replicate any of the directory partitions results in the failure to install Active Directory. To ensure complete synchronization, there is a critical point in the replication process beyond which the process cannot be terminated: Prior to replication of the attributes from the domain directory partition, you can cancel the installation process. After the domain directory partition is replicated, you cannot cancel the installation process.

Creating the Domain

Regardless of the type of domain that you create, the Active Directory Installation Wizard performs the following operations during the installation process:

- Sets the computer Domain Name System (DNS) root domain name to the name of the new domain by using this format:

  <computerName>.<domainName><forestRootDomainName>

- Determines whether the server is joined to a domain. If the computer is a member server of a domain and if you are logged on as an administrator, the wizard removes the computer from the domain and reuses the account. If you are not logged on as an administrator, the wizard alerts you that an administrator must remove the computer account for the server from the domain.
- Creates a computer account in the Domain Controllers container in the new domain. The account is added to the Domain Controllers global group in the Users container. This account allows the computer to authenticate to other domain controllers.
- Applies the password you have provided for the administrator account that will be used when you start the domain controller in Directory Services Restore Mode.
- Creates a cross-reference object in the Configuration container. When the configuration directory partition is replicated to the new domain controller, a cross-reference object is created on the domain naming master and is then replicated throughout the forest. This object is used by LDAP to locate resources in other domains.
- Modifies the Local Security Authority (LSA) membership policy to distinguish the computer as a domain controller.
- Removes the **Start** menu shortcut to the local security settings and adds two new shortcuts to the following Group Policy security setting nodes:
  - Domain security settings for all users and computers.
  - Security settings that are specifically targeted at domain controllers.

Creating a Forest Root Domain

The following operations occur when you create the forest root domain:

- Creation of the Schema container and the Configuration container.
- Assignment of the PDC emulator, RID master, domain naming master, schema master, and infrastructure master roles to the domain controller.

Note

- Creating a new forest does not affect any existing domain and, therefore, does not use a source domain controller during the installation of Active Directory.

Creating a New Child Domain

The following operations occur when you create a child domain in an existing domain tree:

- Verification of the name that you provide as a valid child domain name.

- Location of a source domain controller in the parent domain.
- Synchronization of the system time of the child domain with the system time of the source domain controller.
- Creation of parent-child trust objects in the System folder on both the parent domain and the child domain. These objects (class **trustedDomain**) identify two-way transitive trust relationships between the child domain and the parent domain.
- Replication of the Schema container and the Configuration container from the source domain controller in the parent domain.
- Assignment of the PDC emulator, RID master, and infrastructure master roles to the domain controller.

Creating a New Tree-Root Domain in an Existing Forest

When you create a new tree-root domain, its creation depends on other domains in the forest. The Active Directory Installation Wizard creates various new accounts, trust relationships, and cross-reference objects to incorporate the new tree-root domain into the forest.

The following operations occur when you create a new tree-root domain in an existing forest:

- Location of a source domain controller in the forest root domain.
- Synchronization of domain system time with the system time of the source domain controller.
- Creation of a tree-root trust relationship between the tree root domain and the forest root domain, and creation of a trust object (class **trustedDomain**) in both domains. The tree-root trust relationship is two-way and transitive.
- Assignment of the PDC emulator, RID master, and infrastructure master roles to the domain controller.

Creating an Additional Domain Controller in an Existing Domain

To add an additional domain controller to an existing domain, install Active Directory on a Windows Server 2003-based member server. The same verification and configuration processes occur as during the creation of a new domain. There are no specific namespace or TCP/IP checks and there are no operations master roles assigned.

However, if any of the following operations fail, the installation of Active Directory cannot proceed.

- Joining the computer to the domain. If the additional domain controller is already a member of a domain prior to the Active Directory installation, the computer is removed from the previous domain and rejoined to the new domain for which it is a new domain controller. Changing the join state might change the computer name as well. If the Active Directory Installation Wizard changes the join state of the computer and the Active Directory installation fails elsewhere in the wizard, you must restart the computer before attempting the installation again.
- Forced synchronization from the source server to the RID master, which ensures that a relative identifier pool is quickly provided to the new domain controller. The RID master does not have to be available during the installation of Active Directory, but it must be available at some point after the installation to transfer relative identifiers to the new domain controller.

After these operations succeed, the replication process begins.

Setting Services to Start Automatically

During your Active Directory installation, the following services are configured to start automatically:

- The RPC Locator, which enables distributed applications to use the Microsoft RPC name service. The RPC Locator manages the RPC name service database. For more information about the RPC Locator, see the Software Development Kit (SDK) on MSDN.
- The Net Logon service, which runs the Locator algorithm. Net Logon also is responsible for creating a secure channel between clients and domain controllers during the logon process, registering service (SRV) resource records in DNS, and supporting the Windows NT 4.0 replication protocol (LMRepl).
- The Key Distribution Center (KDC) service, which runs on a physically secure server and maintains a database with account information for all security principals in its realm — the Kerberos v5 authentication protocol equivalent of a Windows Server 2003 domain.
- IsmServ (Intersite Messaging [ISM] service), which is used for mail-based replication between sites and for calculating the least expensive routes between sites. Active Directory includes support for replication between sites by using Simple Mail Transfer Protocol (SMTP) over the IP transport. SMTP support is provided by the SMTP service, which is a component of Internet Information Services (IIS). The set of transports that are used for communication between sites must be extensible; therefore, each transport is defined in a separate add-in dynamic link library (DLL). These add-in DLLs are loaded into the ISM service, which runs on

all domain controllers that are candidates for performing communication between sites. The ISM service directs send requests and receive requests to the appropriate transport add-in DLLs, which then route the messages to the ISM service on the destination computer.

- TrkSvr (Distributed Link Tracking Server service), which runs on each domain controller in a domain. This service enables client applications to track linked documents that have been moved to a location on another NTFS volume in the same domain, in another domain, or in a workgroup. The Distributed Link Tracking Server service helps resolve shortcuts and OLE links to NTFS-resident files that have undergone a name change, a path change, or both.
- W32time (Windows Time service), which synchronizes clocks between clients and servers that run Windows Server 2003. Time synchronization is automatic. For more information about the Windows Time service, see "How Windows Time Service Works."

Setting Security

During the installation of Active Directory, security is enabled on directory service and file replication directories for access control, and actions allowed on domain objects are set through Group Policy.

Access Control

Default access control lists are configured on file and directory objects. Access control lists are also configured for the following registry keys and file system objects, including all child objects:

- HKEY_LOCAL_MACHINE\SOFTWARE
- HKEY_LOCAL_MACHINE\SYSTEM
- HKEY_USERS\DEFAULT
- PROGRAM FILES
- %WINDIR%

For more information about access control, see "How Security Descriptors and Access Control Lists Work."

Group Policy

Group Policy is replicated from only the first domain controller in a domain to all additional domain controllers. In the case of the first domain controller, the following security templates in the %Windir%\Inf directory are used to configure default Group Policy:

- DCFirst.inf is used to define the default Password, Lockout, and Kerberos Group Policy settings for the default Domain Group Policy object.
- DefltDC.inf is used to define the Audit and User Rights Group Policy settings for the default Domain Controllers Group Policy object.
- DCUp.inf is used to define Windows Server 2003–specific settings during the upgrade of a Windows NT 4.0–based domain controller.

Note

- To verify that Group Policy has replicated and been properly configured and applied, look in the Application log in Event Viewer for event ID 1704. If event ID 1704 is present, policy propagation succeeded.

Domains and domain controllers have default security policies. The domain controller security policy has precedence over the domain security policy. For example, if you want to grant the Add Workstation to Domain privilege to a user, you modify the default domain controller security policy rather than the default domain security policy.

For more information about Group Policy, see "Core Group Policy Technical Reference."

Security Accounts Manager (SAM) Database

When a Windows NT 4.0 PDC is upgraded to Windows 2000 or Windows Server 2003, the Active Directory Installation Wizard initializes immediately at the end of setup. When Active Directory is installed, local accounts located in the Windows NT 4.0 registry-based SAM database are migrated to Active Directory as domain accounts. The existing SAM is deleted, and a new, smaller registry-based SAM is created and used for starting the new domain controller in Directory Services Restore Mode for system repair. In Directory Services Restore Mode, the operating system is running without Active Directory and all user validation occurs through the SAM database in the registry.

Note

- When you upgrade a Windows NT 4.0 PDC to a Windows 2000–based or Windows Server 2003–based domain

controller, the previous SAM database is deleted to prevent password attacks.

If Active Directory is removed from the server, the new SAM is available for local user and group accounts on the member server. The computer SID does not change during the installation or removal of Active Directory.

Site Determination

The Active Directory Installation Wizard determines the site to add the new domain controller. It first checks the existing site of the source domain controller to find the subnet of the computer that you are installing. If the subnet is not found, you can add the computer to an existing site. You can create a new site for this domain controller after the Active Directory installation is complete. You can then move the domain controller from the installation site to the new site.

Important

- To automatically place the domain controller in the correct site, all domain controllers in the forest must have the correct site and subnet information before installing Active Directory.

During site determination, the wizard attempts to use the domain controller Locator to find the site you specified or the site in which the computer is currently located. DNS checks the site name to test that it is a valid label. A valid DNS label must contain at least one non-numeric character to distinguish it from an IP address. If the domain controller Locator does not return a site for the computer (that is, the computer's subnet is not associated with a site), the site of the source domain controller is used as the site for the new domain controller.

When you are installing the first domain in a new forest, the default site, Default-First-Site-Name, is used.

Note

- When you are performing an unattended installation, you can specify a site with the SiteName parameter in the answer file. For more information about unattended installation of Active Directory, see "Active Directory Installation Methods" earlier in this subject.

After the correct site is determined, the wizard verifies that a site object exists in Active Directory for that site and that a server object exists for the additional domain controller. If a server object does not exist, one is created. If the server object exists, the associated NTDS Settings object is deleted and then recreated for the new domain controller. An NTDS Settings object is created for each domain controller in the forest. If the NTDS Settings object already exists, the wizard performs as if this domain controller is being reinstalled.

Note

- The NTDS Settings object is always created on a remote server (the source domain controller) for an additional domain controller. For a new domain, the NTDS Settings object is created on the computer that has the domain naming master role. During replication of the Configuration container, the NTDS Settings object is replicated to all domain controllers.

Back to Top

Active Directory Removal

The Active Directory Installation Wizard also removes Active Directory. When you start the wizard on a domain controller, the computer is identified as a server that contains Active Directory, and the wizard prompts you for the information that is required to remove Active Directory.

When you remove Active Directory, you remove all short cuts that were added when Active Directory was installed, and you restore the local policy shortcut. You also restore the shortcut on the **Administrative Tools** menu that provides access to the local security settings for the member server or for the standalone server.

If the Active Directory Installation Wizard recognizes that the computer is a global catalog server, it advises you so that you can make sure that other global catalog servers are accessible to users. The wizard then asks you to indicate whether the domain controller you are decommissioning is the last domain controller in the domain.

Providing Administrative Credentials to Remove Active Directory

To remove Active Directory, you must provide the following administrative credentials:

- To remove Active Directory from a domain controller that is the last domain controller in a child domain, you must provide credentials for a member of the Enterprise Admins group.
- To remove Active Directory from a domain controller that is the last domain controller in a tree-root domain, you must provide credentials for or be logged on as a member of the Enterprise Admins group.
- To remove Active Directory from a domain controller that is the last domain controller in the forest, you do not have to provide credentials. However, you must log on to the domain as an administrator or as a

member of the Domain Admins group.

- To remove Active Directory from a domain controller that is not the last domain controller in the domain, you do not have to provide credentials. However, you must be logged on as a member of either the Domain Admins group or the Enterprise Admins group.

In many cases, removing Active Directory requires Enterprise Admins credentials. The authority to create or remove a domain can be delegated, in which case the credentials of the delegated user suffice.

Removing Active Directory from an Additional Domain Controller or the Last Domain Controller

When you remove Active Directory from either an additional domain controller or from the last domain controller in the domain, the Active Directory Installation Wizard performs the following operations:

- Replication of changes to the configuration directory partition and the schema directory partition. For an additional domain controller, it replicates changes to the configuration, schema, and domain directory partitions.
- Transfer of any operations master roles that the domain controller is holding to another domain controller. While it is possible to allow the Active Directory Installation Wizard to do this, it is not recommended that you rely on the wizard to perform this action. Controlling where operations masters are placed ensures that you can locate and administer each operations master role as necessary.
- Removal of the system volume objects from the directory database; the system volume objects from the NtFrs database; and deletion of the SYSVOL directory hierarchy. NtFrs requests that the Net Logon service remove the share from the system volume.
- Removal of the NTDS Settings object and cross-reference objects.
- Update of DNS to remove the Locator records. (When the NTDS Settings object is deleted, the Directory System Agent (DSA) notifies the Net Logon service, and the Net Logon service removes the records).
- Creation of the local SAM database in the same manner as during a new installation, including creation of the local administrator account and setting the password.
- Modification of the LSA membership policy to distinguish whether the computer is a standalone server or a member server.
- Stop of the Net Logon service and other services. The same services that were started during the installation of Active Directory procedure are stopped. Services that relate only to the directory service are configured to not start automatically.

Removing Active Directory from an Additional Domain Controller

When you remove an additional domain controller, The Active Directory Installation Wizard:

- Locates a source domain controller in the same domain where the additional domain controller account exists and replicates changes to it.
- Sets the computer account type to member server and moves the computer account for the additional server from the Domain Controllers container to the Computers container.

Removing Active Directory from the Last Domain Controller

When you remove the last domain controller in the domain, The Active Directory Installation Wizard:

- Verifies that no child domains exist.
- Locates a source domain controller in the parent domain and replicates changes to it.
- Removes Active Directory objects specific to this domain from the forest. The wizard contacts the domain naming master and removes the NTDS Settings and cross-reference objects.
- Removes trust objects on the parent server. The trustedDomain objects in the System folder are deleted.
- Places the server in a workgroup called "Workgroup."

If the NTDS Settings object is not removed successfully from Active Directory (for example, if a server fails during the removal of Active Directory), remove the object manually by using ntdsutil.exe.

Removing Active Directory from a Domain Controller that Hosts an Application Directory Partition

In Windows Server 2003, non-domain data that is not of global interest can be stored on and replicated between designated domain controllers located in different domains throughout the forest by using application directory partitions. For example, you can store data that is specific to a single application in an application directory partition.

When you are removing a domain controller on which an application directory partition is present, the Active Directory Installation Wizard blocks the removal of that domain controller if it determines that the domain controller hosts the last copy of the application directory partition in the forest. If the removal of Active Directory is blocked, a dialog box lists the application directory partitions existing on the machine. Click **Next** to remove the application directory partitions from the domain controller and continue with the removal of Active Directory.

If at least one other replica of the application directory partition is located in the domain, the wizard skips the dialog box mentioned above and proceeds with the removal of Active Directory. Any changes to the application directory partition are replicated to another replica before it is destroyed.

Provide a New Administrator Password

When Active Directory is removed from a computer, all users and groups that were created on the computer are deleted and all built-in groups are recreated. You must assign a new server administrator password that will have access to the newly created groups.

Back to Top

Related Information

The following resources contain additional information that is relevant to this section.

- DNS Support for Active Directory Technical Reference
- Active Directory Functional Levels Technical Reference
- Core Group Policy Technical Reference