

How to enable or disable DNS updates in Windows 2000 and in Windows Server 2003

This article was previously published under Q246804

Important This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, click the following article number to view the article in the Microsoft Knowledge Base:

Article ID	: 246804
Last Review	: August 8, 2006
Revision	: 4.2

[256986](http://support.microsoft.com/kb/256986/) (<http://support.microsoft.com/kb/256986/>) Description of the Microsoft Windows Registry

On This Page

↓ [SUMMARY](#)

↓ [INTRODUCTION](#)

↓ [DHCP Client service](#)

↓ [Forward and reverse for all adaptors](#)

↓ [Reverse for all adaptors](#)

↓ [Advanced TCP/IP properties controls per adaptor](#)

↓ [Forward and reverse per adaptor](#)

↓ [Reverse per adaptor](#)

↓ [Other settings](#)

↓ [DNS Server service](#)

↓ [The Net Logon service](#)

↓ [All registrations](#)

↓ [Net Logon service A registrations](#)

↓ [Remote access client](#)

↓ [How to disable DNS updates in Windows Server 2003](#)

SUMMARY

Microsoft Windows 2000 supports Domain Name System (DNS) updates per RFC 2136. By default, this behavior is enabled for Windows 2000 DNS clients.

Depending on the configuration and services that are running on a particular computer, different components perform DNS updates. There is no centralized way, such as a tool or registry keys, to manage the DNS update behavior of all components. This article describes each component and how to modify that particular component's behavior.

The article also discusses how to disable DNS updates in Microsoft Windows Server 2003. By default, client computers that are running Windows Server 2003 have DNS updates enabled.

INTRODUCTION

The following components perform DNS updates:

- **Dynamic Host Configuration Protocol (DHCP) Client service**
These updates apply to all Windows 2000-based computers.
- **DNS Server service**
These updates apply to Windows 2000-based DNS servers only.
- **Net Logon service**
This updates apply to Windows 2000-based domain controllers only.
- **Remote access client**
These updates apply to Windows 2000-based remote access clients only.

Note After you change one of these components by modifying the registry keys that are listed in this article, you must stop and restart the affected services. Sometimes, you must restart the computer. These instances are noted.

DHCP Client service

Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

The DHCP Client service performs DNS updates for network adaptors regardless of whether the adaptor is configured by using DHCP or by using manual or static methods. This section describes how to enable and disable the following lookups registrations:

- Forward and reverse for all adaptors
- Reverse for all adaptors
- Advanced TCP/IP properties controls per adaptor
- Forward and reverse per adaptor
- Reverse per adaptor
- Other settings

Forward and reverse for all adaptors

To disable both forward (A resource record) and reverse (PTR resource record) registrations that are performed for all adaptors by the DHCP Client service, use the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableDynamicUpdate

Range: 0 - 1

Default value: 0

Note When this registry value is set to **1**, the **Register this connection's addresses in DNS** check box that is located on the **DNS** tab of each network interface's **TCP/IP advanced properties**, will not be affected. If the check box was checked before the policy was enabled, it will still be checked after the policy is enabled. The registry setting made by this policy is a global setting that affects all interfaces, not an adaptor-specific setting. This global setting is not revealed in Data type REG_DWORD.

This key disables DNS update registration for all adaptors on this computer. With DNS update, DNS client computers automatically register and update their resource records whenever address changes occur.

Value	Meaning
0	Enables DNS update registration
1	Disables DNS update registration

Note For DNS updates to operate on any adaptor, DNS update must be enabled at the system level and at the adaptor level. To disable DNS update for a particular adaptor, add the DisableDynamicUpdate value to an interface name registry subkey and set its value to **1**. To disable DNS updates on all adaptors in a computer, add the DisableDynamicUpdate value to the following subkey, and then set its value to **1**:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Note When this registry value is set to 1, the **Register this connection's addresses in DNS** check box will not reflect the changes made to this registry key. (This check box is located on the **DNS** tab of each network interface's **TCP/IP advanced properties**.) If the check box was selected before the registry change, it will stay selected after this registry change. This registry setting is not an adaptor-specific setting, but a global setting that affects all interfaces. This global setting is not revealed in the user interface.

Windows 2000 does not add this entry to the registry. You can add it by editing the registry or by using a program that edits the registry.

To make the changes to this value effective, you must restart Windows 2000.

Reverse for all adaptors

When you want forward lookup (A resource record) registrations but not reverse lookups (PTR resource record) registrations, use the following registry subkey to disable registrations of PTR resource records:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableReverseAddressRegistration
```

Data type: REG_DWORD

Range: 0 - 1

Default value: 0

This key disables DNS update registration of PTR resource records by this DNS client. PTR resource records associate an address with a computer name. This entry is designed for enterprises where the primary DNS server that is authoritative for the reverse lookup zone cannot, or is configured not to, perform DNS updates. It reduces unnecessary network traffic and prevents event log errors that record unsuccessful tries to register PTR resource records.

Value	Meaning
0	Register PTR resource records
1	Do not register PTR resource records

Note Windows 2000 does not add this entry to the registry. You can add it by editing the registry or by using a program that edits the registry.

To make the changes to this value effective, you must restart Windows 2000.

Advanced TCP/IP properties controls per adaptor

DNS registrations that are performed by each adaptor can be changed by using the following adaptor-specific advanced TCP/IP settings on the **DNS** tab:

- **DNS suffix for this connection**
- **Register this connection's addresses in DNS**
- **Use this connection's DNS suffix in DNS registration**

The **Register this connection's addresses in DNS** default setting registers A and PTR resource records for the first IP address that is configured on this adaptor. Clear this check box to keep the DHCP Client service from registering both A and PTR resource records for this adaptor.

By default, the **Use this connection's DNS suffix in DNS registration** setting is cleared. Each computer has a primary DNS suffix. Use the **ipconfig /all** command to view this suffix.

Additionally, each adaptor can also have a separate DNS suffix that is configured for itself. An adaptor-specific DNS suffix can be configured manually or by using DHCP option 15 as part of the DHCP lease process.

For additional information about DNS options, click the following article number to view the article in the Microsoft Knowledge Base:

[121005](http://support.microsoft.com/kb/121005/) (http://support.microsoft.com/kb/121005/) DHCP options supported by clients

Select this check box to enable the DHCP Client service to register A and PTR resource records for the *PrimaryDnsSuffix*, host name and for the following fully qualified domain name (FQDN):

```
hostname.dns_suffix_for_this_adaptor
```

Forward and reverse per adaptor

To disable A and PTR resource record registrations that are performed for a specific adaptor by the DHCP Client service use the following registry subkey:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\  
name>\DisableDynamicUpdate
```

Data type: REG_DWORD
Range: 0 - 1
Default value: 0

This disables DNS update registration on this adaptor. With DNS update, DNS client computers automatically register a update their resource records whenever address changes occur.

Value	Meaning
0	Enables DNS update registration
1	Disables DNS update registration

Note For DNS updates to operate on any adaptor, it must be enabled at the system level and at the adaptor level. To disable DNS updates for a particular adaptor, add the DisableDynamicUpdate value to an interface name registry subkey and then set its value to 1. To disable DNS updates on all adaptors in a computer, add the DisableDynamicUpdate value to the following registry subkey, and then set its value to 1:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

Windows 2000 does not add this entry to the registry. You can add it by editing the registry or by using a program that edits the registry.

To make the changes to this value effective, you must restart Windows 2000.

Reverse per adaptor

There is no mechanism to disable PTR resource record registrations on a per-adaptor basis.

Other settings

This section lists other parameters that are used by the DHCP Client service as they relate to DNS updates.

By default, DNS records are re-registered dynamically and periodically every 24 hours by Windows 2000 Professional and every hour by Windows 2000 Server and by Windows 2000 Advanced Server. You can use the following registry subkey to modify the update interval:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DefaultRegistrationRefreshInterval
```

Data type: REG_DWORD
Range: 0x0 - 0xFFFFFFFF seconds
Default value: 0x15180 (86,400 seconds = 24 hours) for Windows 2000 Professional
Default value: 0xE10 (3,600 seconds = 1 hour) for Windows 2000 Server and Windows Advanced Server
Scope: Affects all adaptors

This specifies the time interval between DNS update registration updates. By default, on a computer that is running Windows XP or Windows Server 2003, the DefaultRegistrationRefreshInterval key value is 1 day. This is true regardless whether the computer is a client or a server.

Windows 2000 does not add this entry to the registry. You can add it by editing the registry or by using a program that edits the registry.

To make the changes to this value effective, you must restart Windows 2000.

The default Time To Live (TTL) value used for dynamic registrations is 20 minutes. You can use the following registry subkey to modify the TTL value:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DefaultRegistrationTTL
```

Data type: REG_DWORD
 Range: 0x0 - 0xFFFFFFFF seconds
 Default value: 0x4B0 (1,200 seconds = 20 minutes)
 Scope: Affects all adaptors

This specifies the TTL of the DNS registration.

Windows 2000 does not add this entry to the registry. You can add it by editing the registry or by using a program that edits the registry.

To make the changes to this value effective, you must restart Windows 2000.

By default, only the first IP address is dynamically registered. You can use the following registry key to modify the number of IP addresses that are dynamically registered for an adaptor that is configured with more than one IP address, or is logically multihomed:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Adapters\<Interface
name>\MaxNumberOfAddressesToRegister
```

Data type: REG_DWORD
 Range: 0x0 - 0xFFFFFFFF
 Default value: 0x1
 Scope: Affects this adaptor only

This setting determines the maximum number of IP addresses that can be registered in DNS for this adaptor.

If the value of this entry is 0, IP addresses cannot be registered for this adaptor.

To make the changes to this value effective, you must restart Windows 2000.

By default, non-secure DNS registrations are tried. You can use the following registry subkey to modify this behavior:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\UpdateSecurityLevel
```

Data type: REG_DWORD
 Range: 0x0 | 0x10 | 0x100
 Default value: 0x0
 Scope: Affects all adaptors

This determines whether the DNS client uses secure dynamic update or standard dynamic update. Windows 2000 supports both dynamic updates and secure dynamic updates. With secure dynamic updates, the authoritative name server accepts updates only from authorized clients and servers.

Value	Meaning

0 (0x0)	Send secure dynamic updates only when non-secure dynamic updates are refused.
16 (0x10)	Send only non-secure dynamic updates.
256 (0x100)	Send only secure dynamic updates.

Windows 2000 does not add this entry to the registry. You can add it by editing the registry or by using a program that edits the registry.

To make the changes to this value effective, you must restart Windows 2000.

By default, the DNS client tries to replace the original registration with a record that associates the DNS name to its own address. You can use the following registry subkey to modify this behavior:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableReplaceAddressesInConflict:

Data type: REG_DWORD
 Range: 0 - 1
 Default value: 0
 Scope: Affects all adaptors

This prevents the DNS client from overwriting an existing resource record when it discovers an address conflict during dynamic update. An address conflict occurs when the DNS client discovers that an existing A resource record associate DNS name with the IP address of a different computer.

By default, the DNS client tries to replace the original registration with a record that associates the DNS name to its own address. However, you can use this entry to direct DNS back out of the registration process. An error in Event Viewer is not logged.

This entry is designed for zones that do not use secure dynamic update. It prevents unauthorized users from changing IP address registration of a client computer.

Value Meaning

0	The DNS client overwrites the existing A resource record with an A resource record for its own IP address.
1	The DNS client backs out of the registration process. No error is written to the Event Viewer log.

Windows 2000 does not add this entry to the registry. You can add it by editing the registry or by using a program that edits the registry.

To make the changes to this value effective, you must restart Windows 2000.

DNS Server service

The DNS Server service registers host name A resource records for all the adaptors that the service is listening on if the service is authoritative (SOA) for a particular name.

When a server that is running the DNS Server service has multiple adaptors, unwanted addresses can be automatically published. Common scenarios include disconnected or unused network adaptors that publish AutoNet addresses and private or perimeter network (DMZ) interfaces that publish unreachable addresses.

If the Network Load Balancing service is installed on a DNS server, both the virtual network adaptor address and the dedicated network adaptor address will be registered by the DNS Server service. The adaptors that the DNS server is listening on can be changed by using the DNS snap-in. In **Server properties**, click the **Adapters** tab.

If the list of IP addresses that the DNS server listens to and serves is different from the list of IP addresses that is published or that is registered by the DNS Server service, use the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters\PublishAddresses

Data type: REG_SZ
 Range: IP address [IP address]
 Default value: blank

This value specifies the IP addresses that you want to publish for the computer. The DNS server creates A resource records only for the addresses in this list. If this entry does not appear in the registry, or if its value is blank, the DNS server creates an A resource record for each of the computer's IP addresses.

This entry is designed for computers that have multiple IP addresses. With this entry, you can publish only a subset of available addresses. Typically, this entry is used to prevent the DNS server from returning a private network address in response to a query when the computer has a corporate network address.

DNS reads its registry entries only when it starts. You can change entries while the DNS server is running by using the DNS console. If you change entries by editing the registry, the changes are not effective until you restart the DNS serv

The DNS server does not add this entry to the registry. You can add it by editing the registry or by using a program th edits the registry.

The Net Logon service

By default, the Net Logon service registers certain SRV, CNAME, and A resource records every hour, even if some or al these records are correctly registered in DNS. The list of records that the Net Logon service tries to register is stored ir %systemroot%\System32\Config\Netlogon.dns file. This log file lists records that are required to be registered for this domain controller.

The Net Logon service does not provide a mechanism to control registrations that it performs on a per-adaptor basis. T section describes how to enable and disable the following items:

- All registrations
- Net Logon service A registrations

All registrations

To disable all registrations that are performed by the Net Logon service, use the following registry subkey. (A restart o Net Logon service is required, although a restart of the computer is preferred.)

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\UseDynamicDns
```

Data type: REG_DWORD

Range: 0 - 1

Default value: 1

This value determines whether the Net Logon service on this domain controller uses DNS updates. The Net Logon servi can use DNS updates to register DNS names that identify the domain controller. Whenever an authorized zone server requests an update, DNS updates provide automatic updates of zone data, such as DNS names, on the zone's primary server. DNS supplements the static, manual method of adding and changing zone records. The dynamic update protoc defined in RFC 2136.

Value	Meaning

0	The Net Logon service does not use DNS updates. Records specified in the Netlogon.dns file must be registered manually in DNS.
1	The Net Logon service uses DNS updates to register the names that identify this domain controller.

You might disable the Net Logon service's use of DNS updates if your DNS servers do not support DNS updates or to remove the network traffic that is associated with periodic registration of the Net Logon service's DNS records.

This entry is supported on domain controllers only. Windows 2000 does not add this entry to the registry. You can add by editing the registry or by using a program that edits the registry.

To make the changes to this value effective, delete the %systemroot%\System32\Config\netlogon.dnb file, and then restart the Net Logon service. A restart of Windows 2000 is preferred.

Net Logon service A registrations

By default, the Net Logon service on a domain controller registers SRV, domain A, and global catalog A resource record every hour. SRV records are mapped to an FQDN, and A resource records are mapped to an IP address.

Registration of domain A resource records for all adaptors by the Net Logon service and subsequent re-registration eve hour, by default, can be problematic if clients resolve the domain name to an unreachable IP address.

The following registry subkey enables or disables the registration of A resource records by the Net Logon service for a domain controller. The domain A resource records are not required by Windows 2000, but they are registered for the benefit of Lightweight Directory Access Protocol (LDAP) implementations that do not support SRV records.

This RegisterDnsARecords registry value disables all A resource record registrations that are performed by the Net Logon service. These records include the gc._msdcs.DnsForestName records. Registration of gc._msdcs.DnsForestName records is required and must be performed manually if the RegisterDnsARecords registry value is set to disabled.

For additional information about registering these A resource records, click the following article number to view the article in the Microsoft Knowledge Base:

[258213](http://support.microsoft.com/kb/258213/) (http://support.microsoft.com/kb/258213/) Registration of gc._msdcs.<DnsForestName> records in DNS is required

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\RegisterDnsARecords

Data type: REG_DWORD

Range: 0 - 1

Default value: 1

This value determines whether this domain controller registers DNS A (IP address) records for the domain. If this domain controller is a global catalog resource, this entry also determines whether the domain controller registers global catalog DNS A resource records.

Value	Meaning
0	Does not register DNS A resource records. LDAP implementations that do not support SRV records will not be able to locate the LDAP server on this domain controller.
1	Registers DNS A resource records.

Note This entry is used only when it appears in the registry of a domain controller. You might set this value to 0 if DNS does not complete its updates because it cannot update A resource records. DNS stops updating when an update try does not succeed.

Windows 2000 does not add this entry to the registry. You can add it by editing the registry or by using a program that edits the registry.

To make the changes to this value effective, you must restart the Net Logon service. A restart of Windows 2000 is preferred.

Remote access client

To configure individual Remote Access Service connection settings, use Advanced TCP/IP properties, as in the "Per adapter - advanced TCP/IP properties controls" section.

How to disable DNS updates in Windows Server 2003

By default, client computers that are running Windows Server 2003 have DNS updates enabled. To disable DNS updates for all network interfaces, follow these steps:

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Type **DisableDynamicUpdate**, and then press ENTER two times.
5. In the **Edit DWORD Value** dialog box, type **1** in the **Value data** box, and then click **OK**.

Note By default, the DNS update is enabled (0).

6. Quit Registry Editor.

To disable DNS updates for a particular interface, follow these steps:

1. Click **Start**, click **Run**, type **regedit**, and then click **OK**.
2. Locate and then click the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces*deviceID*

Note *deviceID* is the device ID of the network adaptor for the interface.

3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Type **DisableDynamicUpdate**, and then press ENTER two times.
5. In the **Edit DWORD Value** dialog box, type **1** in the **Value data** box, and then click **OK**.
6. Quit Registry Editor.

For additional information, click the following article number to view the article in the Microsoft Knowledge Base:

[816592](http://support.microsoft.com/kb/816592/) (http://support.microsoft.com/kb/816592/) How to configure DNS dynamic update in Windows Server 2003

APPLIES TO

- Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
- Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
- Microsoft Windows Server 2003, Standard Edition (32-bit x86)
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Professional Edition

Keywords: kbinf KB246804