A brief Guide to Managing the Global Query Block List on 2008 R2 DNS Servers

The dynamic update feature of Domain Name System (DNS) makes it possible for all windows clients to register and dynamically update their resource (A) records with a DNS server whenever a client changes its network address or host name.

This reduces the need for manual administration of zone records. This convenience comes at a cost, however, because any authorised client can register any unused host name, even a host name that might have special significance for certain applications. This can allow a malicious user to take over a special name and divert certain types of network traffic to that user's computer.

Two commonly deployed protocols are particularly vulnerable to this type of takeover: the Web Proxy Automatic Discovery Protocol (WPAD) and the Intra-site Automatic Tunnel Addressing Protocol (ISATAP). Even if a network does not deploy these protocols, clients that are configured to use them are vulnerable to the takeover that DNS dynamic update enables. To help prevent such a takeover, the DNS server role in Windows Server 2008 includes a global query block list that can help prevent a malicious user from taking over http://wpad.contoso.com/wpad.dat

The block list feature that is provided by the DNS server role in Windows Server 2008 helps prevent the takeover of WPAD by ensuring that queries for WPAD servers always fail unless WPAD is excluded from the block list.

ISATAP provides a transition between networks that are based on IP version 4 (IPv4) and networks that are based solely on the newer IP version 6 (IPv6). ISATAP provides this transition by using a tunneling approach to carry IPv6 traffic on an IPv4 infrastructure. In other words, ISATAP encapsulates IPv6 packets with an IPv4 header, which makes it possible for the IPv6 packets to be transmitted through a single ISATAP router from one ISATAP-enabled host to another. This transmission occurs wherever the hosts are located on the network, regardless of whether the hosts are located on an IPv6-enabled subnet or on an IPv4-only network.

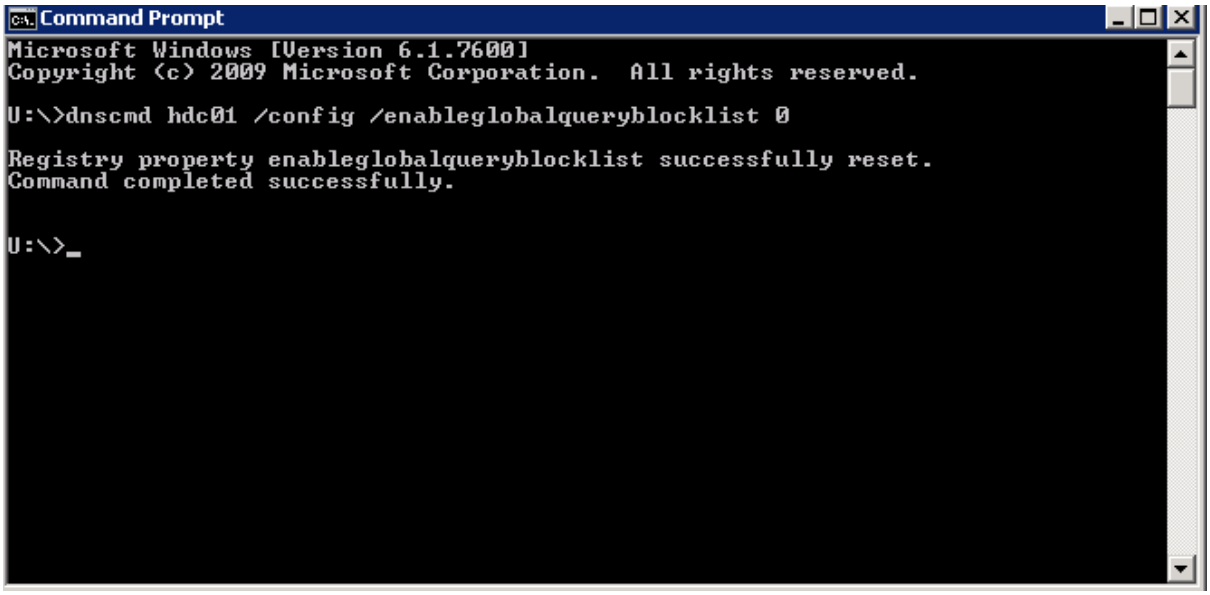
A malicious user can spoof an ISATAP router in much the same way as a malicious user can spoof a WPAD server: A malicious user can use dynamic update to register the user's own computer as a counterfeit ISATAP router and then divert traffic between ISATAP-enabled computers on the network. To prevent this, the Windows Server 2008 DNS Server service blocks name resolution of the isatap host name by default.

In its default configuration, the Windows Server 2008 DNS Server service maintains a list of names that, in effect, it ignores when it receives a query to resolve the name in any zone for which the server is authoritative. To accomplish this, the DNS Server service first checks queries against the list. Then, if the leftmost portion of the name matches an entry in the list, the DNS Server service replies to the query as though no resource record existed, even if there is a host (A or AAAA) resource record in the zone for the name. In this way, if a host (A or AAAA) resource record exists in the zone because a host has used dynamic update to register itself with a blocked name, the DNS Server service does not resolve the name.

The block list automatically applies to all zones for which the server is authoritative. For example, if the DNS server is authoritative for ctcs.co.uk and for Europe.ctcs.co.uk, it ignores queries for wpad.ctcs.co.uk as well as for wpad.europe.ctcs.co.uk.

However, the DNS Server service does not ignore queries for names in zones for which it is not authoritative. Specifically, the DNS Server service does not ignore queries that it receives through a forwarder or a stub zone or as a result of normal recursion or forwarding. If the block list causes the DNS Server service to ignore a request for a resource record that does exist in a zone, it logs an event that explains why it did so. This event is logged only once after the DNS server has been restarted to prevent the event log from being flooded by an attempted denial-of-service attack.

The command below disables the Global Query Block List



You can also chose to update the global query block list

Open a command prompt.

To open an elevated Command Prompt window, click Start, point to All Programs, click Accessories, right-click Command Prompt, and then click Run as administrator.

At the command prompt, type the following command, and then press ENTER:

Copy

```
dnscmd [<ServerName>] /config /globalqueryblocklist [<name> [<name>]...]
```