

Introduction to the Name Resolution Policy Table NRPT

The Name Resolution Policy Table (NRPT) is a table of namespaces and corresponding settings stored in the Windows Registry that determines the DNS client's behavior when issuing queries and processing responses. Each row in the NRPT represents a rule for a portion of the namespace for which the DNS client issues queries. Before issuing name resolution queries, the DNS client will consult the NRPT to determine if any additional flags must be set in the query. Upon receiving the response, the client will again consult the NRPT to determine any special processing or policy requirements. In the absence of the NRPT, the client will operate in a normal fashion. The NRPT stores configurations and settings that are used to deploy DNS Security Extensions (DNSSEC), and also stores information related to DirectAccess, a remote access technology.

The NRPT can be configured using Group Policy or by using the Windows Registry. For more information about configuring the NRPT, see [Deploy Name Resolution Policy to Client Computers](#).

The preferred method of configuring the NRPT is with the Group Policy Management Editor. See the following example.

Group Policy Management Editor

File Action View Help



- [-] DNSSEC Policy [DC1.WOODGROVEBANK.]
 - [-] Computer Configuration
 - [-] Policies
 - + Software Settings
 - [-] Windows Settings
 - [-] Name Resolution Policy
 - [-] Scripts (Startup/Shutdown)
 - + Security Settings
 - + Policy-based QoS
 - + Administrative Templates: Po...
 - + Preferences
 - [-] User Configuration
 - + Policies
 - + Preferences

Name Resolution Policy

Overview

The Name Resolution Policy Table (NRPT) stores configuration settings for DNS security (DNSSEC). You can use this page to create or edit rules, which are used to make policies that can be applied to...

[Learn more about DNSSEC on the Web](#)

Description

Name Resolution Policy is the Group Policy object (GPO) that contains the policy information found in the Name Resolution Policy Table (NRPT).

Create Rules

To which part of the namespace does this rule apply?

Suffix:

Certification authority: (Optional)


DNSSEC | DNS Settings for Direct Access

- Enable DNSSEC in this rule
- DNSSEC settings
 - Validation:
 - Require DNS clients to check that name and address data h... by the DNS server
 - IPsec:
 - Use IPsec in communication between the DNS client and D...
 - Encryption type:

Name Resolution Policy Table

Namespace	CA	DNSSEC (V...	DNSSEC (I...	DNSSEC (I...	Direct Acce...	Dir
.secure.woo...		Yes	Yes	No encrypti...		

The properties of an NRPT rule are described in the following table:

Rule Property	Functionality/Use	Format
Namespace	Used to indicate the namespace to which the policy applies. When a query is issued, the DNS client will compare the name in the query to all of the namespaces in this column to find a match.	<ul style="list-style-type: none"> • DNS suffix (*.contoso.com) • DNS prefix (hrweb.*) • FQDN (hrweb.contoso.com) • IP address subnet for reverse lookup (157.0.0.0/8)
DNSSEC	<p>Used to indicate whether the DNS client should check for DNSSEC validation in the response.</p> <p> Hinweis</p> <p>Selecting this option will not force the DNS server to perform DNSSEC validation. That validation is triggered by the presence of a trust anchor for the zone the DNS server is querying. Setting this value to true prompts the DNS client to</p>	Binary (on or off)

check for the presence of the Authenticated Data bit in the response from the DNS server if the response has been validated, If not, the DNS client will ignore the response.

Used to indicate whether IPsec must be used to protect DNS traffic for queries belonging to the namespace.

DNS Over IPsec

Setting this value to true will cause the DNS client to set up an IPsec connection to the DNS server before issuing the DNS query.

Binary (on or off)

Used to indicate whether DNS connections over IPsec will use encryption.

IPsec Encryption Level

If DNSOverIPsec is off, this value is ignored.

- Array:
- 0 – Do not use encryption (only integrity is performed)
- 1 – Low: 3DES, AES (all)
- 2 – Medium: AES (all)
- 3 – High: AES (192, 256)

The CA (or list of CAs) that issued the DNS server certificates for

IPsec CA

DNS over IPsec connections. When using IPsec to allow the client to trust the

String – The domain name of the CA that issued the DNS server certificate. If left blank, the authorization check is not required for this name.

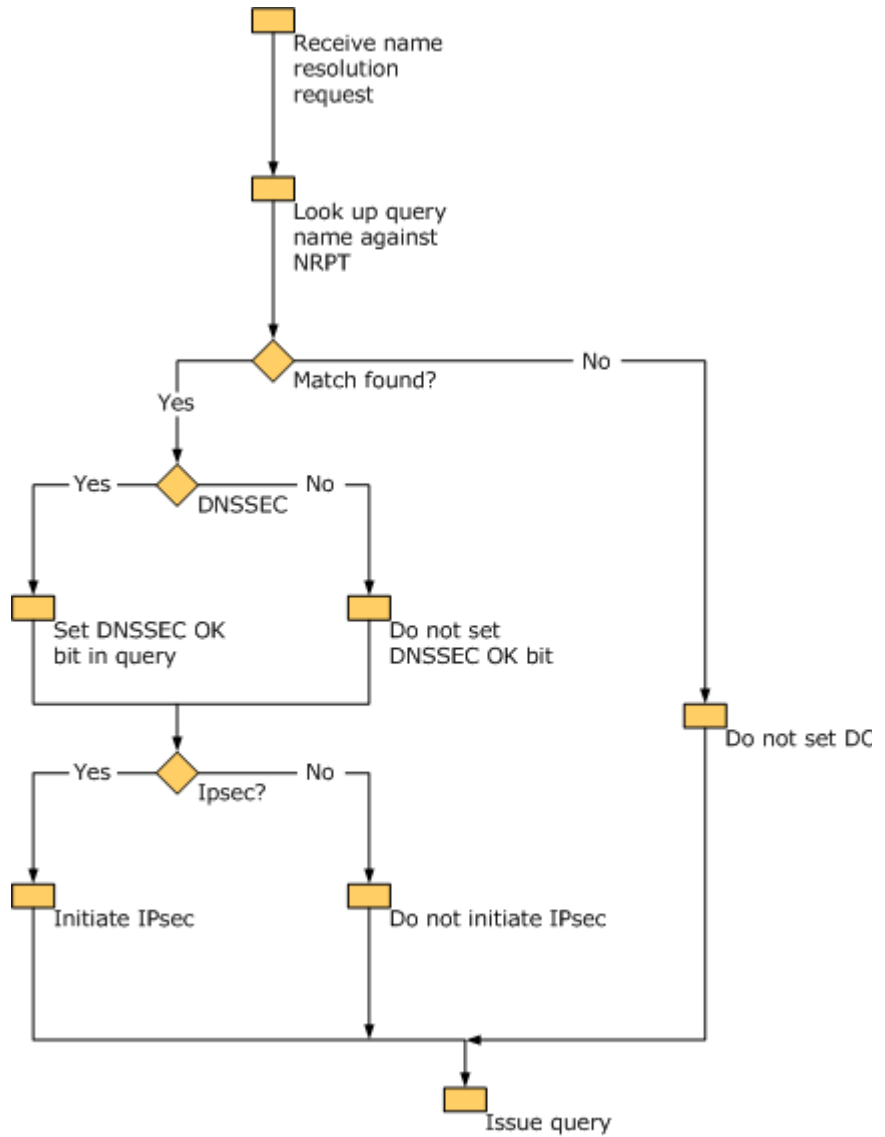
This is checked along with the presence of a DNS EKU in the server certificate.

The following flowchart shows how the DNS client uses the

DNS server, the NRPT when issuing queries.

DNS client checks for the server authorization based on the server certificates issued by this CA. If not set, all root CAs in the client computer's stores are checked.

If DNSOverIPsec is off, this value is ignored.



Siehe auch