[MS-GPNRPT-Diff]:

Group Policy: Name Resolution Policy Table (NRPT) Data Extension

---

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards ~~as well as overviews of the interaction among each of these technologies~~support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights**. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you ~~may~~can make copies of it in order to develop implementations of the technologies that are described in ~~the Open Specifications~~ this documentation and ~~may~~can distribute portions of it in your implementations ~~using~~that use these technologies or in your documentation as necessary to properly document the implementation. You ~~may~~can also distribute in your implementation, with or without modification, any ~~schema, IDL's~~schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications~~.~~ documentation.
- **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
- **Patents**. Microsoft has patents that ~~may~~might cover your implementations of the technologies described in the Open Specifications~~.~~ documentation. Neither this notice nor Microsoft's delivery of ~~the~~this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open ~~Specification may~~Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in ~~the Open Specifications~~this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks**. The names of companies and products contained in this documentation ~~may~~might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names**. The example companies, organizations, products, domain names, ~~e-mail~~email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications ~~do~~documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments~~,~~ you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available ~~standard~~standards specifications and network programming art~~,~~ and ~~assumes~~, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
8/27/2010	0.1	New	Released new document.
10/8/2010	0.1	None	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	0.1	None	No changes to the meaning, language, or formatting of the technical content.
1/7/2011	0.1	None	No changes to the meaning, language, or formatting of the technical content.
2/11/2011	0.1	None	No changes to the meaning, language, or formatting of the technical content.
3/25/2011	0.1	None	No changes to the meaning, language, or formatting of the technical content.
5/6/2011	0.1	None	No changes to the meaning, language, or formatting of the technical content.
6/17/2011	0.2	Minor	Clarified the meaning of the technical content.
9/23/2011	0.2	None	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	1.0	Major	Updated and revised the technical content.
3/30/2012	1.0	None	No changes to the meaning, language, or formatting of the technical content.
7/12/2012	1.0	None	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	2.0	Major	Updated and revised the technical content.
1/31/2013	2.0	None	No changes to the meaning, language, or formatting of the technical content.
8/8/2013	3.0	Major	Updated and revised the technical content.
11/14/2013	4.0	Major	Updated and revised the technical content.
2/13/2014	5.0	Major	Updated and revised the technical content.
5/15/2014	5.0	None	No changes to the meaning, language, or formatting of the technical content.
6/30/2015	6.0	Major	Significantly changed the technical content.
10/16/2015	6.0	~~No Change~~None	No changes to the meaning, language, or formatting of the technical content.

Table of Contents

1 Introduction 5
1.1 Glossary 5
1.2 References 7
1.2.1 Normative References 7
1.2.2 Informative References 7
1.3 Protocol Overview (Synopsis) 8
1.3.1 Background 8
1.3.2 Name Resolution Policy Table Extension Encoding Overview 8
1.4 Relationship to Other Protocols 9
1.5 Prerequisites/Preconditions 9
1.6 Applicability Statement 9
1.7 Versioning and Capability Negotiation 9
1.8 Vendor-Extensible Fields 9
1.9 Standards Assignments 9

2 Messages 10
2.1 Transport 10
2.2 Message Syntax 10
2.2.1 Global Policy Configuration Options 10
2.2.1.1 Enable DirectAccess for All Networks 10
2.2.1.2 DNS Secure Name Query Fallback 10
2.2.1.3 DirectAccess Query Order 11
2.2.2 Name Resolution Policy Messages 11
2.2.2.1 Name 11
2.2.2.2 Config Options 11
2.2.2.3 Version 12
2.2.2.4 DNSSEC Query IPsec Encryption 12
2.2.2.5 DNSSEC Query IPsec Required 13
2.2.2.6 DNSSEC Validation Required 13
2.2.2.7 IPsec CA Restriction 13
2.2.2.8 DirectAccess DNS Servers 14
2.2.2.9 DirectAccess Proxy Name 14
2.2.2.10 DirectAccess Proxy Type 14
2.2.2.11 DirectAccess Query IPsec Encryption 15
2.2.2.12 DirectAccess Query IPsec Required 15
2.2.2.13 Generic DNS Servers 15
2.2.2.14 IDN Configuration 16
2.2.2.15 Auto-Trigger VPN 16
2.2.2.16 Proxy Name 16
2.2.2.17 Proxy Type 17

3 Protocol Details 18
3.1 Administrative Plug-in Details 18
3.1.1 Abstract Data Model 18
3.1.2 Timers 18
3.1.3 Initialization 18
3.1.4 Higher-Layer Triggered Events 18
3.1.5 Processing Events and Sequencing Rules 18
3.1.6 Timer Events 19
3.1.7 Other Local Events 19

4 Protocol Examples 20
4.1 Global Policy Configuration Messages 20
4.2 Name Resolution Policy Messages 20
4.2.1 DirectAccess 20

4.2.2 DNSSEC 22
4.2.3 Both DirectAccess and DNSSEC 23
4.2.4 Generic DNS Server 24
4.2.5 IDN Configuration 25
5 Security 27
5.1 Security Considerations for Implementers 27
5.2 Index of Security Parameters 27
6 Appendix A: Product Behavior 28
7 Change Tracking 31
8 Index 32

1 Introduction

This document specifies the Name Resolution Policy Table (NRPT) Group Policy Data Extension, an extension to Group Policy: Registry Extension Encoding [MS-GPREG]. The NRPT Group Policy Data Extension provides a mechanism for an administrator to control any **Name Resolution Policy** behavior on a **client** by using Group Policy settings.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative ~~and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in [RFC2119]. Sections 1.5 and 1.9 are also normative but do not contain those terms~~. All other sections and examples in this specification are informative.

1.1 Glossary

~~The~~This document uses the following terms ~~are specific to this document~~:

Active Directory: A general-purpose network directory service. **Active Directory** also refers to the Windows implementation of a directory service. **Active Directory** stores information about a variety of objects in the network. Importantly, user accounts, computer accounts, groups, and all related credential information used by the Windows implementation of Kerberos are stored in **Active Directory**. **Active Directory** is either deployed as Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS). [MS-ADTS] describes both forms. For more information, see [MS-AUTHSOD] section 1.1.1.5.2, Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Kerberos, and **DNS**.

administrative template: A file associated with a **Group Policy Object (GPO)** that combines information on the syntax of registry-based policy settings with human-readable descriptions of the settings, as well as other information.

Advanced Encryption Standard (AES): A block cipher that supersedes the **Data Encryption Standard (DES)**. AES can be used to protect electronic data. The AES algorithm can be used to encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. AES is used in symmetric-key cryptography, meaning that the same key is used for the encryption and decryption operations. It is also a block cipher, meaning that it operates on fixed-size blocks of plaintext and ciphertext, and requires the size of the plaintext as well as the ciphertext to be an exact multiple of this block size. AES is also known as the Rijndael symmetric encryption algorithm [FIPS197].

certification authority (CA): A third party that issues public key certificates (1). Certificates serve to bind public keys to a user identity. Each user and certification authority (CA) can decide whether to trust another user or CA for a specific purpose, and whether this trust should be transitive. For more information, see [RFC3280].

client: A client, also called a client computer, is a computer that receives and applies settings of a **Group Policy Object (GPO)**, as specified in [MS-GPOL].

client computer: A computer that receives and applies settings from a **Group Policy Object (GPO)**, as specified in [MS-GPOL].

client-side extension GUID (CSE GUID): A **GUID** that enables a specific client-side extension on the Group Policy client to be associated with policy data that is stored in the logical and physical components of a **Group Policy Object (GPO)** on the Group Policy server, for that particular extension.

Data Encryption Standard (DES): A specification for encryption of computer data that uses a 56-bit key developed by IBM and adopted by the U.S. government as a standard in 1976. For more information see [FIPS46-3].

DirectAccess: A collection of different component policies, including Name Resolution Policy and IPsec, which allows seamless connectivity to corporate resources when not physically connected to the corporate network.

domain: A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set must act as a domain controller (DC) and host a member list that identifies all members of the domain, as well as optionally hosting the **Active Directory** service. The domain controller provides authentication (2) of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members. For more information, see [MS-AUTHSOD] section 1.1.1.5 and [MS-ADTS].

Domain Name System (DNS): A hierarchical, distributed database that contains mappings of domain names (1) to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database.

fully qualified domain name (FQDN): An unambiguous domain name (2) that gives an absolute location in the **Domain Name System's (DNS)** hierarchy tree, as defined in [RFC1035] section 3.1 and [RFC2181] section 11.

globally unique identifier (GUID): A term used interchangeably with universally unique identifier (UUID) in Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the value. Specifically, the use of this term does not imply or require that the algorithms described in [RFC4122] or [C706] must be used for generating the **GUID**. See also universally unique identifier (UUID).

Group Policy Object (GPO): A collection of administrator-defined specifications of the policy settings that can be applied to groups of computers in a domain. Each GPO includes two elements: an object that resides in the **Active Directory** for the domain, and a corresponding file system subdirectory that resides on the sysvol DFS share of the Group Policy server for the domain.

IPv4 address in string format: A string representation of an IPv4 address in dotted-decimal notation, as described in [RFC1123] section 2.1.

IPv6 address in string format: A string representation of an IPv6 address, as described in [RFC4291] section 2.2.

Name Resolution Policy: **Policy settings** that control how **client** name resolution is performed for a given **DNS** domain or hostname.

Name Resolution Policy Table (NRPT): The collection of Name Resolution Policy settings that apply to a given client.

NetBIOS: A particular network transport that is part of the LAN Manager protocol suite. **NetBIOS** uses a broadcast communication style that was applicable to early segmented local area networks. The LAN Manager protocols were the default in Windows NT operating system environments prior to Windows 2000 operating system. A protocol family including name resolution, datagram, and connection services. For more information, see [RFC1001] and [RFC1002].

policy setting: A statement of the possible behaviors of an element of a domain member computer's behavior that can be configured by an administrator.

Punycode: An ASCII Compatible Encoding syntax that transforms strings containing Unicode characters into strings consisting of a limited set of ASCII characters allowable for **DNS**. Used to transform internationalized domain names. For more details, see [RFC3492].

registry: A local system-defined database in which applications and system components store and retrieve configuration data. It is a hierarchical data store with lightly typed elements that are logically stored in tree format. Applications use the registry API to retrieve, modify, or delete registry data. The data stored in the registry varies according to the version of Windows.

registry policy file: A file associated with a **Group Policy Object (GPO)** that contains a set of registry-based policy settings.

tool extension GUID or administrative plug-in GUID: A GUID defined separately for each of the user policy settings and computer policy settings that associates a specific administrative tool plug-in with a set of policy settings that can be stored in a **Group Policy Object (GPO)**.

Unicode: A character encoding standard developed by the Unicode Consortium that represents almost all of the written languages of the world. The **Unicode** standard [UNICODE5.0.0/2007] provides three forms (UTF-8, UTF-16, and UTF-32) and seven schemes (UTF-8, UTF-16, UTF-16 BE, UTF-16 LE, UTF-32, UTF-32 LE, and UTF-32 BE).

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as defined in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the Errata.

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information.

[MS-GPOL] Microsoft Corporation, "Group Policy: Core Protocol".

[MS-GPREG] Microsoft Corporation, "Group Policy: Registry Extension Encoding".

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt

[RFC5280] Cooper, D., Santesson, S., Farrell, S., et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008, http://www.ietf.org/rfc/rfc5280.txt

1.2.2 Informative References

[MS-HNDS] Microsoft Corporation, "Host Name Data Structure Extension".

[RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987, http://www.ietf.org/rfc/rfc1034.txt

[RFC3490] Faltstrom, P., "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003, http://www.ietf.org/rfc/rfc3490.txt

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and Souissi, M., "DNS Extensions to Support IP version 6", RFC 3596, October 2003, http://www.ietf.org/rfc/rfc3596.txt

1.3 Protocol Overview (Synopsis)

The Name Resolution Policy Table (NRPT) Group Policy Data Extension provides a mechanism for an administrator to control Name Resolution Policy behavior of the client through Group Policy by using the Group Policy: Registry Extension Encoding [MS-GPREG].

1.3.1 Background

The Group Policy: Core Protocol (as specified in [MS-GPOL]) allows clients to discover and retrieve **policy settings** created by administrators of a **domain**. These settings are persisted within **Group Policy Objects (GPOs)** that are assigned to Policy Target accounts in the **Active Directory**. On each client, each GPO is interpreted and acted upon by software components known as client plug-ins. The client plug-ins responsible for a given GPO are specified using an attribute on the GPO. This attribute specifies a list of **globally unique identifier (GUID)** lists. The first GUID of each GUID list is referred to as a **client-side extension GUID (CSE GUID)**. Other GUIDs in the GUID list are referred to as **tool extension GUIDs**. For each GPO that is applicable to a client, the client consults the CSE GUIDs listed in the GPO to determine which client plug-in on the client ~~should~~will handle the GPO. The client then invokes the client plug-in to handle the GPO.

Registry-based settings are accessible from a GPO through the Group Policy: Registry Extension Encoding protocol [MS-GPREG], which is a client plug-in. The protocol provides mechanisms both for administrative tools to obtain metadata about registry-based settings and for clients to obtain applicable registry-based settings.

Group Policy: Registry Extension Encoding settings are specified using **registry policy files** (as specified in [MS-GPREG] section 2.2.1). An administrative tool uses the information within the **administrative template** to write out a registry policy file and associate it with a GPO. The Group Policy: Registry Extension Encoding plug-in on each client reads registry policy files specified by applicable GPOs and applies their contents to its registry.

1.3.2 Name Resolution Policy Table Extension Encoding Overview

Name Resolution Policy Table policies are configurable from a GPO through the Name Resolution Policy Table Group Policy Data Extension, which uses the {f4d8c39a-f43d-42b4-9bdf-4e48d3044ba1} tool extension GUID. The protocol provides mechanisms both for Group Policy administrators to deploy policies and for clients to obtain the applicable policies to enforce them. The Name Resolution Policy Table component has complex settings not expressible through administrative templates, and for this reason it implements a custom UI that can author registry policy files containing the encodings of the settings described in this document. Given that the Name Resolution Policy Table policies are applied to the whole machine, the NRPT Group Policy Data Extension protocol uses the Computer Policy Mode described in [MS-GPREG] section 1.3.2.

Name Resolution Policy Table policies are applied as follows:

1. An administrator invokes a Group Policy Name Resolution Policy Table administrative tool on the administrator's computer to administer a Group Policy Object (GPO) through Group Policy Protocol using the Policy Administration mode, as specified in [MS-GPOL] section 2.2.7. The administrative tool invokes a plug-in specific to Group Policy: Registry Extension Encoding so that the administrator can administer the Group Policy: Name Resolution Policy Table Data Structure transported over the Group Policy: Registry Extension Encoding data. This results in the storage and retrieval of metadata inside a GPO on a Group Policy server. This metadata describes configuration settings to be applied to the registry on a client that is affected by the GPO. The administrator views the data and updates it to add a directive to run a command when the **client computer** starts up. If they are not already present from a prior update, the CSE GUID and tool extension GUID for Computer Policy Settings for Group Policy: Registry Extension Encoding are written to the GPO.

2. A client computer affected by that GPO is started (or is connected to the network, if this happens after the client starts), and Group Policy Protocol is invoked by the client to retrieve Policy Settings from the Group Policy server. As part of the processing of Group Policy Protocol, the Group Policy: Registry Extension Encoding's CSE GUID is read from this GPO, and this instructs the client to invoke a Group Policy: Registry Extension Encoding plug-in component for Policy Application.

3. In processing the Policy Application portion of Group Policy: Registry Extension Encoding, the client parses the settings and then saves the settings in the registry on the local computer and notifies the Name Resolution Policy client component. The NRPT policies are stored in local storage.

4. The NRPT Group Policy Data Extension is invoked for policy application. To apply the policies, the Name Resolution Policy component parses its previously stored settings in local storage.

1.4 Relationship to Other Protocols

This protocol depends on the Group Policy: Registry Extension Encoding (as specified in [MS-GPREG]) to transport the Name Resolution Policy Table Group Policy Data Extension settings. The protocol also has all the dependencies inherited from Group Policy: Registry Extension Encoding.

1.5 Prerequisites/Preconditions

The prerequisites for this protocol are the same as those for the Group Policy: Registry Extension Encoding ([MS-GPREG]).

In addition, a client needs to have a system/subsystem capable of executing commands at startup/shutdown time because the Computer Policy Mode of the Group Policy: Registry Extension Encoding is used.

1.6 Applicability Statement

The NRPT Group Policy Data Extension is applicable only while transported under the Group Policy: Registry Extension Encoding and within the Group Policy: Core Protocol framework. The Group Policy: Name Resolution Policy Table Data Structure ~~should be~~is used to express the required Name Resolution Policy Table policy of the client. Settings configured under Group Policy have priority over local settings.

The NRPT Group Policy Data Extension ~~should~~is not ~~be~~ used in any other context.

1.7 Versioning and Capability Negotiation

The Group Policy: Name Resolution Policy Table Data Structure has a policy version (also called schema version), but the protocol currently defines a single version with a value of 1.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

Parameter	Value
Tool extension GUID	{f4d8c39a-f43d-42b4-9bdf-4e48d3044ba1}
Policy Base registry key	Software\Policies\Microsoft\Windows NT\DNSClient

2 Messages

2.1 Transport

The Name Resolution Policy Table Group Policy Data Extension requires Group Policy: Registry Extension Encoding. All messages are exchanged in registry policy files encoded using Group Policy: Registry Extension Encoding.

2.2 Message Syntax

2.2.1 Global Policy Configuration Options

The Global Policy Configuration Options specify name resolution behavior that applies to all entries within the NRPT.

For information about the Type values, see [MS-GPREG] section 2.2.1.

2.2.1.1 Enable DirectAccess for All Networks

Key: Software\Policies\Microsoft\Windows NT\DNSClient or System\CurrentControlSet\services\Dnscache\Parameters<1>

Value: "EnableDAForAllNetworks"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	Let Network ID determine when **DirectAccess** settings are to be used.
0x00000001	Always use DirectAccess settings regardless of location.
0x00000002	Never use DirectAccess settings regardless of location.

2.2.1.2 DNS Secure Name Query Fallback

Key: Software\Policies\Microsoft\Windows NT\DNSClient or System\CurrentControlSet\services\Dnscache\Parameters<2>

Value: "DnsSecureNameQueryFallback"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	Only use Link-Local Multicast Name Resolution (LLMNR) and **NetBIOS** if the name does not exist in **DNS**.

Value	Meaning
0x00000001	Always fall back to LLMNR and NetBIOS for any kind of name resolution error.
0x00000002	Always fall back to LLMNR and NetBIOS if the name does not exist in DNS or if the DNS servers are unreachable when on a private network.

2.2.1.3 DirectAccess Query Order

Key: Software\Policies\Microsoft\Windows NT\DNSClient or System\CurrentControlSet\services\Dnscache\Parameters<3>

Value: "DirectAccessQueryOrder"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	Resolve only IPv6 addresses.
0x00000001	Resolve both IPv4 and IPv6 addresses.

2.2.2 Name Resolution Policy Messages

The Name Resolution Policy Table consists of one or more Name Resolution Policy keys under Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig. The names for these keys can be any unique string value.

2.2.2.1 Name

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<4>

Value: "Name"

Type: REG_MULTI_SZ.

Size: Equal to the size of the **Data** field.

Data: One or more **Unicode** string names, each of which MUST be either a DNS suffix, a DNS prefix, a **fully qualified domain name (FQDN)**, an IPv4 subnet formatted as specified in [RFC1034], section 3.6.2, or an IPv6 subnet formatted as specified in [RFC3596] section 2.5.

Each DNS suffix present MUST consist of a "." character with a domain name appended. Each DNS prefix present MUST be constructed according to the "name" rule specified in [MS-HNDS] section 2.1.

2.2.2.2 Config Options

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<5>

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000002	Only DNSSEC options (that is, options defined in sections 2.2.2.4, 2.2.2.5, 2.2.2.6, and 2.2.2.7) are specified.
0x00000004	Only DirectAccess options (that is, options defined in sections 2.2.2.8, 2.2.2.9, 2.2.2.10, 2.2.2.11, and 2.2.2.12) are specified.
0x00000006	Both DNSSEC and DirectAccess options are specified.
0x00000008	Only the Generic DNS server option (that is, the option defined in section 2.2.2.13) is specified.
0x0000000A	The Generic DNS server option and the DNSSEC options are specified.
0x0000000C	The Generic DNS server option and the DirectAccess options are specified.
0x0000000E	The Generic DNS server option, DNSSEC options, and DirectAccess options are specified.
0x00000010	Only the IDN Configuration option (that is, option defined in section 2.2.2.14) is specified.
0x00000012	The IDN configuration option and DNSSEC options are specified.
0x00000014	The IDN configuration option and DirectAccess options are specified.
0x00000016	The IDN configuration option, DNSSEC options, and DirectAccess options are specified.
0x00000018	The IDN configuration option and the Generic DNS server options are specified.
0x0000001A	The IDN configuration option, Generic DNS server option, and DNSSEC options are specified.
0x0000001C	The IDN configuration option, Generic DNS server options, and DirectAccess options are specified.
0x0000001E	The IDN configuration option, Generic DNS server option, DNSSEC options, and DirectAccess options are specified.

2.2.2.3 Version

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<6>

Value: "Version"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value specifying the Name Resolution Policy version. Its value MUST be 0x00000001.

2.2.2.4 DNSSEC Query IPsec Encryption

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<7>

Value: "DNSSECQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	No encryption (integrity only) necessary when IPsec protection is used for DNSSEC queries.
0x00000001	Low security encryption, which includes **DES** or **AES** with key size of 128, 192, or 256 bits, is to be used when IPsec protection is used for DNSSEC queries.
0x00000002	Medium security encryption, which includes AES with key size of 128, 192, or 256 bits, is to be used when IPsec protection is used for DNSSEC queries.
0x00000003	High security encryption, which includes AES with key size of 192 or 256 bits, is to be used when IPsec protection is used for DNSSEC queries.

2.2.2.5 DNSSEC Query IPsec Required

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<8>

Value: "DNSSECQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	IPsec is not required for DNS queries.
0x00000001	IPsec is required for DNS queries.

2.2.2.6 DNSSEC Validation Required

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<9>

Value: "DNSSECValidationRequired"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	DNSSEC validation is not required for DNS queries.
0x00000001	DNSSEC validation is required for DNS queries.

2.2.2.7 IPsec CA Restriction

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<10>

Value: "IPSECCARestriction"

Type: REG_SZ.

Size: Equal to the size of the **Data** field.

Data: A Unicode string specifying the **Certificate Authority** in X509 format [RFC5280].

2.2.2.8 DirectAccess DNS Servers

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<11>

Value: "DirectAccessDNSServers"

Type: REG_SZ.

Size: Equal to the size of the **Data** field.

Data: A semicolon-delimited Unicode string of IP addresses or names of DNS servers used for internal name resolutions by DirectAccess clients. Each IP address item in the string MUST be either an **IPv4 address in string format** or an **IPv6 address in string format**. Each name in the string MUST be an extended hostname as specified in [MS-HNDS].

2.2.2.9 DirectAccess Proxy Name

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<12>

Value: "DirectAccessProxyName"

Type: REG_SZ.

Size: Equal to the size of the **Data** field.

Data: A Unicode string specifying the HTTP proxy name and port in the format "proxy:port" where "proxy" MUST be either an extended hostname as specified in [MS-HNDS] section 2.1, an IPv4 address in string format, or an IPv6 address in string format; "port" MUST be a decimal integer between 1 and 65535.

2.2.2.10 DirectAccess Proxy Type

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<13>

Value: "DirectAccessProxyType"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	No proxy configured.
0x00000001	Use the default proxy.

Value	Meaning
0x00000002	Use the proxy specified by the DirectAccess Proxy Name (see section 2.2.2.9).

2.2.2.11 DirectAccess Query IPsec Encryption

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<14>

Value: "DirectAccessQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	No encryption (integrity only) required for IPsec protection of DNS queries.
0x00000001	Low security, which includes DES or AES with key size of 128, 192, or 256 bits, required for IPsec protection of DNS queries.
0x00000002	Medium security, which includes AES with key size of 128, 192, or 256 bits, required for IPsec protection of DNS queries.
0x00000003	High security, which includes AES with key size of 192 or 256 bits, required for IPsec protection of DNS queries.

2.2.2.12 DirectAccess Query IPsec Required

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<15>

Value: "DirectAccessQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value, which MUST contain of one of the following values.

Value	Meaning
0x00000000	IPsec protection is not required for DNS queries.
0x00000001	IPsec protection is required for DNS queries.

2.2.2.13 Generic DNS Servers

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<16><17>

Value: "GenericDNSServers"

Type: REG_SZ

Size: Equal to the size of the **Data** field.

Data: A semicolon-delimited Unicode string of IP addresses or names of DNS servers used for name resolutions by clients in the absence of DirectAccess settings. Each IP address item in the string MUST be either an IPv4 address in string format or an IPv6 address in string format. Each name in the string MUST be an extended hostname, as specified in [MS-HNDS].

2.2.2.14 IDN Configuration

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<18><19>

Value: "IDNConfig"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value that MUST contain one of the following values.

Value	Meaning
0x00000000	The query name MUST be encoded in UTF-8 without any mapping.
0x00000001	The query name MUST be encoded in UTF-8 with mapping.
0x00000002	The query name MUST be encoded in **Punycode**.

For more information about IDN configuration, see [RFC3490].

2.2.2.15 Auto-Trigger VPN

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<20>

Note This property is optional. If it is not used, its value is set to an empty string.

Value: "VpnRequired"

Type: REG_DWORD

Size: 32 bits.

Data: This field is a 32-bit value that MUST contain one of the following values.

Value	Meaning
0x00000000	Do NOT notify VPN platform to dial VPN when sending DNS queries.
0x00000001	Notify VPN platform to dial VPN when sending DNS queries.

2.2.2.16 Proxy Name

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<21>

Note This property is optional. If it is not used, its value is set to an empty string.

Value: "ProxyName"

Type: REG_SZ

Size: Equal to the size of the **Data** field.

Data: A Unicode string specifying the HTTP proxy name and port in the format "proxy:port" where "proxy" MUST be either an extended hostname as specified in [MS-HNDS] section 2.1, an IPv4 address in string format, or an IPv6 address in string format; "port" MUST be a decimal integer between 1 and 65,535.

2.2.2.17 Proxy Type

Key: Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID} or System\CurrentControlSet\services\Dnscache\Parameters\DnsPolicyConfig\{Rule GUID}<22>

Note This property is optional. If it is not used, its value is set to an empty string.

Value: "ProxyType"

Type: REG_SZ

Size: Equal to the size of the **Data** field.

Data: This field is a 32-bit value, which MUST contain one of the following values.

Value	Meaning
0x00000000	No proxy configured.
0x00000001	Use the default proxy.
0x00000002	Use the proxy specified by the Proxy Name (section 2.2.2.16).

3 Protocol Details

3.1 Administrative Plug-in Details

The administrative plug-in mediates between the user interface (UI) and a remote data store that contains Name Resolution Policy Table Group Policy extension settings. Its purpose is to receive Name Resolution Policy Table Group Policy information from a UI and to write the same policy information to a remote data store.

The NRPT Group Policy Data Extension administrative plug-in relies on a collection of settings specified in section 2.2 and stored as a Unicode configuration file ([MS-GPREG] section 2.2) at a remote storage location using the Group Policy: Core Protocol. The administrative plug-in parses and encodes these settings as specified in section 2.2 to perform its functions.

The NRPT Group Policy Data Extension administrative plug-in reads in these settings from the remote storage location and displays them to an administrator through a UI.

An administrator can then use the UI to make further configuration changes, and the NRPT Group Policy Data Extension administrative plug-in will make corresponding changes to the name-value pairs stored in the aforementioned Unicode configuration file following the conventions of the keys specified in section 2.2.

3.1.1 Abstract Data Model

None.

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

The NRPT Group Policy Data Extension administrative plug-in is invoked when an administrator launches the user interface for editing Group Policy settings. The plug-in displays the current settings to the administrator, and when the administrator requests a change in settings, it updates the stored configuration appropriately as specified in section 2.2, after performing additional checks and actions as noted in this section.

The administrative plug-in SHOULD<23> take measures in its UI to ensure that the user cannot unknowingly set the Name Resolution Policy Table Group Policy settings to an invalid value.

3.1.5 Processing Events and Sequencing Rules

The NRPT Group Policy Data Extension administrative plug-in reads extension-specific data from the remote storage location and will then pass that information to a UI to display the current settings to an administrator.

It will also write the extension-specific configuration data to the remote storage location if the administrator makes any changes to the existing configuration.

Any additional entries in the configuration data that do not pertain to the configuration options specified in section 2.2, or that are not supported by the particular implementation, MUST be ignored by the plug-in.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

4 Protocol Examples

4.1 Global Policy Configuration Messages

The following is an example of Name Resolution Policy global options to query for both IPv4 and IPv6, always allow fallback to LLMNR and NetBIOS, and to enable Name Resolution Policy behavior only when not physically connected to the corporate network.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient

Value: "DirectAccessQueryOrder"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "DnsSecureNameQueryFallback"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "EnableDAForAllNetworks"

Type: REG_DWORD

Size: 32 bits.

Data: 00000000

4.2 Name Resolution Policy Messages

The following are examples of individual Name Resolution Policy entries specifying DNSSEC, DirectAccess, and both.

4.2.1 DirectAccess

The following is an example of a Name Resolution Policy entry to apply DirectAccess for names under the directaccess.example.com domain. The policy specifies the DNS servers to query and requires IPsec with medium encryption but no CA restriction or proxy.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID}

Value: "Version"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "Name"

Type: REG_MULTI_SZ.

Size: Equal to the size of the data field.

Data: ".directaccess.example.com"

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits.

Data: 00000004

Value: "DirectAccessDNSServers"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: "10.1.1.1;10.2.2.2"

Value: "DirectAccessProxyName"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: ""

Value: "DirectAccessProxyType"

Type: REG_DWORD

Size: 32 bits.

Data: 00000000

Value: "DirectAccessQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: 00000002

Value: "DirectAccessQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "IPSECCARestriction"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: ""

4.2.2 DNSSEC

The following is an example of a Name Resolution Policy entry to apply DNSSEC for names under the dnssec.example.com domain. The policy requires DNSSEC validation, IPsec with medium encryption, and a specific CA.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\ {Rule GUID}

Value: "Version"

Type: REG_DWORD

Size: 32 bits.

Data: 1

Value: "Name"

Type: REG_MULTI_SZ.

Size: Equal to the size of the data field.

Data: ".dnssec.example.com"

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits.

Data: 00000002

Value: "DNSSECQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: 00000002

Value: "DNSSECQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "DNSSECValidationRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "IPSECCARestriction"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: 'C=US, O="VeriSign, Inc.", OU=Class 3 Public Primary Certification Authority - G2, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network'

4.2.3 Both DirectAccess and DNSSEC

The following is an example of a Name Resolution Policy entry to apply both DirectAccess and DNSSEC for names under the both.example.com domain. For DNSSEC, the policy requires DNSSEC validation, IPsec with high encryption, and a specific CA. For DirectAccess, it specifies DNS servers for DirectAccess, requires IPsec with high encryption, and specifies a proxy.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID}

Value: "Version"

Type: REG_DWORD

Size: 32 bits.

Data: 1

Value: "Name"

Type: REG_MULTI_SZ.

Size: Equal to the size of the data field.

Data: ".both.example.com"

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits.

Data: 00000006

Value: "DirectAccessDNSServers"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: "10.1.1.1"

Value: "DirectAccessProxyName"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: "exampleproxy:80"

Value: "DirectAccessProxyType"

Type: REG_DWORD

Size: 32 bits.

Data: 00000002

Value: "DirectAccessQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: 00000003

Value: "DirectAccessQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "DNSSECQueryIPSECEncryption"

Type: REG_DWORD

Size: 32 bits.

Data: 00000003

Value: "DNSSECQueryIPSECRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "DNSSECValidationRequired"

Type: REG_DWORD

Size: 32 bits.

Data: 00000001

Value: "IPSECCARestriction"

Type: REG_SZ.

Size: Equal to the size of the data field.

Data: 'C=US, O="VeriSign, Inc.", OU=Class 3 Public Primary Certification Authority - G2, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network'

4.2.4 Generic DNS Server

The following is an example of a Name Resolution Policy entry to apply the Generic DNS server configuration for names under the example.com domain. The policy requires the use of the configured DNS server for all DNS queries.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID}

Value: "VpnRequired"

Type: REG_DWORD

Size: 32 bits

Data: 00000001

Value: "Name"

Type: REG_MULTI_SZ

Size: Equal to the size of the data field

Data: ".example.com"

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits

Data: 00000008

Value: "GenericDNSServers"

Type: Reg_SZ

Size: Equal to the size of the data field

Data: "10.1.1.1; 10.2.2.2"

Value: "ProxyName"

Type: REG_SZ

Size: Equal to the size of the data field

Data: "exampleproxy:80"

Value: "ProxyType"

Type: REG_DWORD

Size: 32 bits

Data: 00000002

4.2.5 IDN Configuration

The following is an example of a Name Resolution Policy entry to apply internationalized domain name processing for names under the idn.example.com domain. The policy requires that all names in this domain be encoded in Punycode.

Key: SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Rule GUID}

Value: "Version"

Type: REG_DWORD

Size: 32 bits.

Data: 1

Value: "Name"

Type: REG_MULTI_SZ.

Size: Equal to the size of the data field.

Data: ".dnssec.example.com"

Value: "ConfigOptions"

Type: REG_DWORD

Size: 32 bits.

Data: 000000010

Value: "IDNConfig"

Type: Reg_DWORD

Size: 32 bits

Data: 00000002

5 Security

5.1 Security Considerations for Implementers

~~Implementers SHOULD NOT~~Do not transmit passwords or other sensitive data through this protocol. The primary reason for this restriction is that the protocol provides no encryption, and therefore sensitive data transmitted through this protocol can be intercepted easily by an unauthorized user with access to the network carrying the data. For example, if a network administrator configured a Group Policy: Registry Extension Encoding setting in a GPO to instruct a computer to use a specific password when accessing a certain network resource, this protocol would send that password unencrypted to those computers. A person gaining unauthorized access, intercepting the protocol's network packets in this case, would then discover the password for that resource, which would then be unprotected from the unauthorized person.

5.2 Index of Security Parameters

None.

6 Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include released service packs.

~~Note: Some of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader.~~

- Windows 7 operating system
- Windows Server 2008 R2 operating system
- Windows 8 operating system
- Windows Server 2012 operating system
- Windows 8.1 operating system
- Windows Server 2012 R2 operating system
- Windows 10 operating system
- Windows Server 2016 ~~Technical Preview~~ operating system

Exceptions, if any, are noted below. If a service pack or Quick Fix Engineering (QFE) number appears with the product version, behavior changed in that service pack or QFE. The new behavior also applies to subsequent service packs of the product unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that the product does not follow the prescription.

<1> Section 2.2.1.1: In the presence of both keys, the System\CurrentControlSet\services\Dnscache\Parameters key is ignored.

<2> Section 2.2.1.2: In the presence of both keys, the System\CurrentControlSet\services\Dnscache\Parameters key is ignored.

<3> Section 2.2.1.3: In the presence of both keys, the System\CurrentControlSet\services\Dnscache\Parameters key is ignored.

<4> Section 2.2.2.1: The **Name** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. In the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<5> Section 2.2.2.2: The **Config Options** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<6> Section 2.2.2.3: The **Version** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<7> Section 2.2.2.4: The **DNSSEC Query IPsec Encryption** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the

presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<8> Section 2.2.2.5: The **DNSSEC Query IPsec Required** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<9> Section 2.2.2.6: The **DNSSEC Validation Required** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<10> Section 2.2.2.7: The **IPsec CA Restriction** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<11> Section 2.2.2.8: The **DirectAccess DNS Servers** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<12> Section 2.2.2.9: The **DirectAccess Proxy Name** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<13> Section 2.2.2.10: The **DirectAccess Proxy Type** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<14> Section 2.2.2.11: The **DirectAccess Query IPsec Encryption** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<15> Section 2.2.2.12: The **DirectAccess Query IPsec Required** key specification is Software\Policies\Microsoft\Windows NT\DNSClient\DnsPolicyConfig\{Name}. Note that in the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<16> Section 2.2.2.13: In the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<17> Section 2.2.2.13: This property is ignored on Windows 7 and Windows Server 2008 R2.

<18> Section 2.2.2.14: In the presence of both specified keys, Windows ignores the System\CurrentControlSet\services\Dnscache\Parameters key.

<19> Section 2.2.2.14: This property is ignored on Windows 7 and Windows Server 2008 R2.

<20> Section 2.2.2.15: This property is ignored on Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012.

<21> Section 2.2.2.16: This property is ignored on Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012.

<22> Section 2.2.2.17: This property is ignored on Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012.

<23> Section 3.1.4: Windows administrative tools verify the validity of the objects as defined in section 2.2 before writing them to the remote store through Group Policy: Registry Extension Encoding.

7 Change Tracking

No table of changes is available. The document is either new or has had no changes since its last release.

8 Index

A

Abstract data model 18
Administrative plug-in - overview 18
Applicability 9
Auto-Trigger VPN 16

C

Capability negotiation 9
Change tracking 31
Config Options message 11

D

Data model - abstract 18
DirectAccess
  DNS Servers message 14
  Proxy
    Name message 14
    Type message 14
  Query
    IPsec
      Encryption message 15
      Required message 15
    Order message 11
DNS Secure Name Query Fallback message 10
DNSSEC
  Query IPsec
    Encryption message 12
    Required message 13
  Validation Required message 13

E

Enable DirectAccess for All Networks message 10
Examples
  Global Policy Configuration messages 20
  Name Resolution Policy messages
    DirectAccess 20
    DirectAccess and DNSSEC 23
    DNSSEC 22
    generic DNS server 24
    IDN configuration 25
    overview 20

F

Fields - vendor-extensible 9

G

Generic DNS servers 15
Global Policy Configuration
  message example 20
  Options - message overview 10
Global Policy Configuration Options message 10
Glossary 5

H

Higher-layer triggered events 18

I

IDN configuration 16
Implementer - security considerations 27
Index of security parameters 27
Informative references 7
Initialization 18
Introduction 5
IPsec CA Restriction message 13

L

Local events 19

M

Message processing 18
Messages
  Global Policy Configuration Options 10
    DirectAccess Query Order 11
    DNS Secure Name Query Fallback 10
    Enable DirectAccess for All Networks 10
    overview 10
  Name Resolution Policy
    Auto-Trigger VPN 16
    Config Options 11
    DirectAccess
      DNS Servers 14
      Proxy
        Name 14
        Type 14
      Query IPsec
        Encryption 15
        Required 15
    DNSSEC
      Query IPsec
        Encryption 12
        Required 13
      Validation Required 13
    generic DNS servers 15
    IDN configuration 16
    IPsec CA Restriction 13
    Name 11
    overview 11
    Proxy Name 16
    Proxy Type 17
    Version 12
  Name Resolution Policy Messages 11
  transport 10

N

Name message 11
Name Resolution Policy
  message - overview 11
  message example
    DirectAccess 20
    DirectAccess and DNSSEC 23
    DNSSEC 22
    generic DNS server 24
    IDN configuration 25
    overview 20
  Table extension encoding - overview 8
Name Resolution Policy Messages message 11

Normative references 7

O

Overview
  background 8
  Name Resolution Policy - Table extension encoding 8
  synopsis 8
Overview (synopsis) 8

P

Parameter index - security 27
Parameters - security index 27
Preconditions 9
Prerequisites 9
Product behavior 28
Proxy Name 16
Proxy Type 17

R

References 7
  informative 7
  normative 7
Relationship to other protocols 9

S

Security
  implementer considerations 27
  parameter index 27
Sequencing rules 18
Standards assignments 9

T

Timer events 19
Timers 18
Tracking changes 31
Transport 10
Triggered events 18

V

Vendor-extensible fields 9
Version message 12
Versioning 9