[MS-GPFR]:
Group Policy:
Folder Redirection Protocol Extension

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.

- **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 make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.

- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.

- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft Open Specification Promise or the Community Promise. If you would prefer a written license, or if the technologies described in the Open Specifications 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 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, email addresses, logos, people, places, and events 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 specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do 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 are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
02/22/2007	0.01		MCPP Milestone 3 Initial Availability
06/01/2007	2.0	Major	Updated and revised the technical content.
07/03/2007	2.0.1	Editorial	Revised and edited the technical content.
07/20/2007	2.0.2	Editorial	Revised and edited the technical content.
08/10/2007	2.0.3	Editorial	Revised and edited the technical content.
09/28/2007	2.0.4	Editorial	Revised and edited the technical content.
10/23/2007	2.0.5	Editorial	Revised and edited the technical content.
11/30/2007	2.0.6	Editorial	Revised and edited the technical content.
01/25/2008	2.0.7	Editorial	Revised and edited the technical content.
03/14/2008	2.0.8	Editorial	Revised and edited the technical content.
05/16/2008	2.0.9	Editorial	Revised and edited the technical content.
06/20/2008	2.1	Minor	Updated the technical content.
07/25/2008	2.2	Minor	Updated the technical content.
08/29/2008	2.2.1	Editorial	Revised and edited the technical content.
10/24/2008	2.2.2	Editorial	Revised and edited the technical content.
12/05/2008	2.3	Minor	Updated the technical content.
01/16/2009	2.3.1	Editorial	Revised and edited the technical content.
02/27/2009	2.3.2	Editorial	Revised and edited the technical content.
04/10/2009	2.3.3	Editorial	Revised and edited the technical content.
05/22/2009	3.0	Major	Updated and revised the technical content.
07/02/2009	3.1	Minor	Updated the technical content.
08/14/2009	3.1.1	Editorial	Revised and edited the technical content.
09/25/2009	3.2	Minor	Updated the technical content.
11/06/2009	3.3	Minor	Updated the technical content.
12/18/2009	3.3.1	Editorial	Revised and edited the technical content.
01/29/2010	3.4	Minor	Updated the technical content.

Release: Friday, October 25, 2013

Date	Revision History	Revision Class	Comments
03/12/2010	3.4.1	Editorial	Revised and edited the technical content.
04/23/2010	3.4.2	Editorial	Revised and edited the technical content.
06/04/2010	3.4.3	Editorial	Revised and edited the technical content.
07/16/2010	3.5	Minor	Clarified the meaning of the technical content.
08/27/2010	3.5	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	3.5	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	3.5	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	3.5	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	3.5	No change	No changes to the meaning, language, or formatting of the technical content.
03/25/2011	4.0	Major	Significantly changed the technical content.
05/06/2011	5.0	Major	Significantly changed the technical content.
06/17/2011	6.0	Major	Significantly changed the technical content.
09/23/2011	7.0	Major	Significantly changed the technical content.
12/16/2011	8.0	Major	Significantly changed the technical content.
03/30/2012	8.0	No change	No changes to the meaning, language, or formatting of the technical content.
07/12/2012	8.0	No change	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	8.0	No change	No changes to the meaning, language, or formatting of the technical content.
01/31/2013	8.0	No change	No changes to the meaning, language, or formatting of the technical content.
08/08/2013	9.0	Major	Significantly changed the technical content.
11/14/2013	9.0	No change	No changes to the meaning, language, or formatting of the technical content.

Contents

Release: Friday, October 25, 2013

1   Introduction

The Group Policy: Folder Redirection Protocol Extension allows an administrator to relocate certain file system **folders**, called **user profile folders**, to different paths such as a shared network location.

Sections 1.8, 2, and 3 of this specification are normative and can contain the terms MAY, SHOULD, MUST, MUST NOT, and SHOULD NOT as defined in RFC 2119. Sections 1.5 and 1.9 are also normative but cannot contain those terms. All other sections and examples in this specification are informative.

1.1   Glossary

The following terms are defined in [MS-GLOS]:

> **access control list (ACL)**
> **client-side extension GUID (CSE GUID)**
> **curly braced GUID string**
> **Distributed File System (DFS)**
> **domain**
> **domain controller (DC)**
> **folder**
> **folder redirection**
> **globally unique identifier (GUID)**
> **Group Policy Object (GPO)**
> **Group Policy Object (GPO) path**
> **security identifier (SID)**
> **Server Message Block (SMB)**
> **share**
> **tool extension GUID**
> **Unicode**
> **Universal Naming Convention (UNC)**
> **user profile folder**

The following terms are specific to this document:

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

1.2   References

References to Microsoft Open Specifications documentation do not include a publishing year because links are to the latest version of the documents, which are updated frequently. References to other documents include a publishing year when one is available.

A reference marked "(Archived)" means that the reference document was either retired and is no longer being maintained or was replaced with a new document that provides current implementation details. We archive our documents online [Windows Protocol].

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. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[C706] The Open Group, "DCE 1.1: Remote Procedure Call", C706, August 1997, https://www2.opengroup.org/ogsys/catalog/c706

[MS-DTYP] Microsoft Corporation, "Windows Data Types".

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

[MS-SMB] Microsoft Corporation, "Server Message Block (SMB) Protocol".

[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

1.2.2   Informative References

[HOWARD] Howard, M., "Writing Secure Code", Microsoft Press, 2002, ISBN: 0735617228.

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary".

1.3   Overview

This document specifies the Group Policy: Folder Redirection Protocol Extension, which conveys an administrator's policy for redirecting user profile folders.

1.3.1   Background

The Group Policy Protocol, as specified in [MS-GPOL], allows clients to discover and retrieve policy settings created by **domain** administrators. These settings are persisted within **Group Policy Objects (GPOs)** that are assigned to policy target accounts in the Active Directory. Policy target accounts are either computer accounts or user accounts in the Active Directory. Each client uses Lightweight Directory Access Protocol (LDAP) to determine what GPOs are applicable to it by consulting the Active Directory objects corresponding to each client's computer account, and the user accounts of any users logging on to the client computer.

On each client, each GPO is interpreted and acted upon by software components known as client-side plug-ins. The client-side 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)** pairs. The first GUID of each pair is referred to as a **client-side extension GUID (CSE GUID)**. The second GUID of each pair is referred to as a **tool extension GUID**.

For each GPO that is applicable to a client, the client consults the CSE GUIDs listed in the GPO to determine what client-side plug-ins on the client should handle the GPO. The client then invokes the client-side plug-ins to handle the GPO.

A client-side plug-in uses the contents of the GPO to retrieve settings specific to its class in a manner specific to the class. Once its class-specific settings are retrieved, the client-side plug-in uses those settings to perform class-specific processing.

1.3.2   Folder Redirection Protocol Overview

The Group Policy: Folder Redirection Protocol Extension enables an administrator to redirect the location of certain file system folders, called user profile folders, to different paths such as a shared network location. When the operating system or application requests access to these redirected folders, the operating system automatically redirects the access requests to the location on a network **share** specified by the administrator.

By convention, an operating system or application may expect to read and store a user's data in a set of folders within the local file system. For example, the operating system may conventionally store image files for user "Sue" in a folder of the local file system called \Sue\Documents\My Pictures. The Group Policy: Folder Redirection Protocol Extension allows an administrator to change the location of Sue's My Pictures folder from its default local location to a UncPath such as \\CorpServer\Users\Sue\Documents, thereby making it available to Sue from any machine on the network. This also enables the administrator to manage its storage from a central location.

It is important to note that an operating system may not support redirection of all user folders. The set of folders that can be redirected (that is, user profile folders) is a function of the operating system version. The protocol provides both a Version Zero file format that assumes a constant list of user profile folders and a Version One file format that supports an extensible set of user profile folders.<1>

Two software plug-ins interact with each other through files in the **folder redirection** protocol format, stored and communicated through a remote storage location such as a network share. The plug-ins are as follows:

- Folder Redirection Administrative-Side Plug-in

- Folder Redirection Client-Side Plug-in

The Folder Redirection Administrative-Side Plug-in provides a user interface by which network administrators can establish and update folder locations for users' folders. It relies on the Group Policy Protocol, as specified in [MS-GPOL], to specify the location of the remote storage location where the folder redirection configuration data should be stored. This **GPO path** is metadata in a GPO that is stored on the **domain controller** where the Folder Redirection Protocol configuration data is stored. The plug-in uses SMB operations, as specified in [MS-SMB], to retrieve existing configuration data (in the form of files) from that location and to store updated configuration to it.

The Folder Redirection Client-Side Plug-in is a component of each client machine in the network that users log on to. It is invoked by the client implementation of the Group Policy Protocol, as specified in [MS-GPOL], on behalf of the user logging on to the operating system. The protocol provides the folder redirection protocol with the remote storage location from which the protocol should read the Folder Redirection Client-Side Plug-in configuration data. This location is constructed based on the GPO path in the GPO retrieved by the Group Policy Protocol. The client-side plug-in uses SMB operations to retrieve the current configuration data from that location. The plug-in then parses the data and configures the folder redirection subsystem of the underlying operating system to redirect the user's user profile folders to the locations specified, as described in section 1.3.4.

Note The remote storage location can be implemented using a variety of techniques such as a network share. Therefore, implementing a remote storage location does not require understanding the folder redirection protocol.

1.3.3   Folder Redirection Administrative-Side Plug-In

The Folder Redirection Administrative-Side Plug-in determines (through the Group Policy Protocol, as specified in [MS-GPOL]) the path of a file containing the Folder Redirection protocol data. Given the

path name, the plug-in retrieves the contents of the file using SMB as a transport, as specified in [MS-SMB].

An administrator uses the Folder Redirection Administrative-Side Plug-in to read the current configuration for users' folders and to modify the configuration data for any of the users' folders by way of the user interface of the plug-in. If the administrator modifies any data, the Folder Redirection Administrative-Side Plug-in writes the modified folder redirection protocol configuration data to the remote storage location, using SMB as a transport.

1.3.4 Folder Redirection Client-Side Plug-In

The Folder Redirection Client-Side Plug-in determines (by way of the Group Policy Protocol, as specified in [MS-GPOL]) the path of a file containing the folder redirection protocol data. Given the path name, the client-side plug-in retrieves the contents of the file using SMB as a transport. The client-side plug-in parses the configuration data and configures the operating system folder redirection subsystem with the directives in the protocol data.

1.4 Relationship to Other Protocols

This protocol depends on the Group Policy: Core Protocol (as specified in [MS-GPOL]) to provide a list of applicable GPOs. It also depends on the SMB Protocol, as specified in [MS-SMB], for transmitting Group Policy settings and instructions between the client and the GP server.

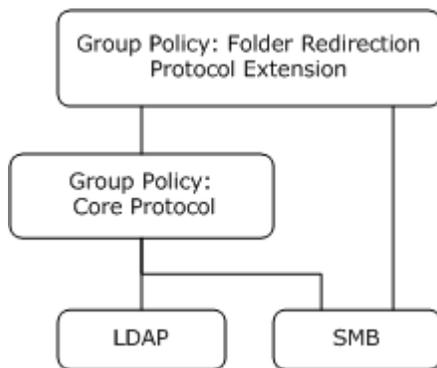**Figure 1: Group Policy: Folder Redirection Protocol Extension relationship diagram**

1.5 Prerequisites/Preconditions

The prerequisites for this protocol include those for the Group Policy Protocol.

In addition, each participating client is required to have an operating system subsystem capable of redirecting user profile folders, including intercepting and modifying application file system operations, and moving and merging directory contents to implement changes to user profile folder locations.

1.6 Applicability Statement

The folder redirection protocol is only applicable within the Group Policy Protocol as specified in [MS-GPOL].

Commonly-used configurations (those that use the Check Ownership and Exclusive Access flags of section 2.2.2.2.1) require that the destination server of a redirection specification support New Technology File System (NTFS)-compatible security operations such as testing ownership of a

directory and modifying directory **access control lists (ACL)**. The client folder redirection subsystem will fail if the policy uses these flags and the destination server does not provide these operations.<2>

1.7 Versioning and Capability Negotiation

The Group Policy: Folder Redirection Protocol Extension does not provide for capability negotiations.

The Group Policy: Folder Redirection Protocol Extension does provide versioning capability through its configuration data that is stored in the remote storage location. The Folder Redirection Administrative-Side Plug-in generates additional, secondary configuration data for an operating system version if the folder redirection policies specified by an administrator affect user profile folders (which are features provided only by that version of an operating system).<3>

Folder Redirection Client-Side Plug-ins that support the later Version One format must read and use only the Version One configuration data from the remote storage location, when it is available. If the remote storage location provides only Version Zero configuration data, client-side plug-ins that support the later Version One format should read and use the Version Zero configuration data.

The Version One format specifies a **VersionNumber** field designed to allow future versions of the protocol, but only a single value of that field is presently defined, and thus Version One of the protocol must set that field to a constant value.

1.8 Vendor-Extensible Fields

The Group Policy: Folder Redirection Protocol Extension defines a vendor-extensible GUID (as specified in [MS-DTYP] section 2.3.4.3)   field for well-known user profile folders. Vendors can obtain a value by generating one, according to the standard GUID algorithm, as specified in [C706]. The current assigned values are shown in section 1.9.

1.9 Standards Assignments

This protocol defines CSE GUID and tool extension GUID values using the assignment algorithm (as specified in section 1.8) that refers to the GUID generation algorithm, as specified in [C706]. This same algorithm is used to generate other GUIDs for well-known user profile folders (shown in the following table for reference).

Parameter	Value
CSE GUID	{25537BA6-77A8-11D2-9B6C-0000F8080861}
Tool Extension GUID (User Policy Settings)	{88E729D6-BDC1-11D1-BD2A-00C04FB9603F}

Well-known user profile folder GUIDs	
AppData\Roaming	{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}
Contacts	{56784854-C6CB-462b-8169-88E350ACB882}
Desktop	{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}
Documents	{FDD39AD0-238F-46AF-ADB4-6C85480369C7}
Downloads	{374DE290-123F-4565-9164-39C4925E467B}

Well-known user profile folder GUIDs	
Favorites	{1777F761-68AD-4D8A-87BD-30B759FA33DD}
Links	{bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968}
Music	{4BD8D571-6D19-48D3-BE97-422220080E43}
Pictures	{33E28130-4E1E-4676-835A-98395C3BC3BB}
SavedGames	{4C5C32FF-BB9D-43b0-B5B4-2D72E54EAAA4}
Searches	{7d1d3a04-debb-4115-95cf-2f29da2920da}
Start Menu	{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}
Videos	{18989B1D-99B5-455B-841C-AB7C74E4DDFC}

2   Messages

2.1   Transport

The Group Policy: Folder Redirection Protocol Extension requires the SMB transport with mutual authentication, as specified in [MS-GPOL] section 2.1. All messages are exchanged as files, as specified in [MS-GPOL]. The client-side plug-in MUST use this protocol's CSE GUID, and the administrative-side plug-in MUST use the tool extension GUID.

The Group Policy Protocol uses this protocol protocol's CSE GUID and tool extension GUID values to invoke this protocol only to access GPOs from which messages of this protocol can be generated.

2.2   Message Syntax

Messages exchanged in this protocol allow the client to discover settings in the GPOs that instruct clients to configure their operating system folder redirection subsystems according to administrator directives.

There are two versions of the protocol specified in the following sections:

- 2.2.1 Folder Redirection Protocol Version Zero Configuration Data

- 2.2.2 Folder Redirection Protocol Version One Configuration Data

Both versions convey a message as a .ini file. Each file is encoded in UTF-16LE with Byte Order Mark (0xFFFE). The syntax of each file, and thus the syntax of each message, is specified by the Augmented Backus-Naur Form (ABNF) non-terminal IniFile, as specified in [MS-GPOL] section 2.2.4. The following sections use the terminology sections, keys, and values of that document to specify concrete syntax of each message.

2.2.1   Folder Redirection Protocol Version Zero Configuration Data

Version Zero of the protocol uses the SMB transport to copy a file that MUST be named <gpo path>\User\Documents & Settings\fdeploy.ini, where <gpo path> is a scoped GPO path. The message is the file itself.

The file MUST contain one section with the SectionID Folder Status. The folder status section MUST contain zero or more key-value pairs (called redirection options) where:

- The key MUST be one of the following five string constants, specifying the user profile folder to which the redirection options apply:

  - My Documents

  - My Pictures

  - Start Menu

  - Application Data

  - Desktop

- The value corresponding to each key MUST be a string representation of a hexadecimal value, representing the binary OR of a collection of flags. The following section specifies the flags.

To see an example of a version zero configuration file example, please see section 4.4.

2.2.1.1 Interpreting the Redirection Options Value

The client-side plug-in passes the flags to the underlying operating system folder redirection subsystem. Other than the exceptions indicated in the following table with the prescriptive words MUST and MUST NOT, the redirection options flags do not affect the behavior of the protocol itself.

Flag value	Behavior
0x00000001	Move Contents This flag indicates that all contents of the specified folder MUST be moved to the redirected path location.<4>
0x00000002	Follow Parent Folder This flag indicates that the user profile folder MUST be handled (for purposes of redirection) as ordinary contents of its parent folder. This flag is only meaningful when the specified user profile is a descendent of some other user profile folder. In Version Zero of the protocol, this flag MUST NOT be set in redirection options other than for those associated with the key My Pictures and, in this case, the My Pictures user profile folder MUST be treated as an ordinary subfolder of the My Documents user profile folder. If this flag is set, the client-side plug-in MUST configure the folder redirection subsystem to use the redirection options associated with the user profile folder of which the present user profile folder is a descendent. If this flag is set, all other flags MUST NOT be set, and the Per-Profile section (as specified in section 2.2.1.2) for the corresponding user profile folder MUST NOT appear in the file.
0x00000004	Redirection Not Specified This flag indicates that the administrator has specified no specific redirection path for the folder, and the folder redirection subsystem MUST continue using whatever redirection configuration it was last configured with.<5> If this flag is set, all other flags MUST NOT be set, and the Per-Profile section (as specified in section 2.2.1.2) for the corresponding user profile folder MUST NOT appear in the file.
0x00000008	Advanced Redirection The client-side plug-in MUST ignore its value.
0x00000010	Check Ownership with Exclusive Access This flag indicates that the folder redirection subsystem, before initiating redirection, MUST verify that the file system permissions on the destination folder indicate that the user owns the destination folder. If the check fails, the folder redirection subsystem MUST behave as if no redirection had been specified for this user profile folder.<6>
0x00000020	Relocate On Move This flag indicates that if the policy is ever deleted in the future, the folder redirection MUST be undone.

2.2.1.2 Per-Profile Sections

For each redirection options key-value pair present in the Folder Status section with neither the Follow Parent Folder nor the Redirection Not Specified flags set, the file MUST contain an additional section, called a Per-Profile Folder section, whose SectionID is the same as the key of the redirection options key-value pair. The SectionID identifies what user profile folder SHOULD be redirected. The corresponding key in the Folder Status section identifies what flags should be applied to the redirection of that user profile folder.

Each Per-Profile Folder section MUST contain zero or more key-value pairs called security group mappings. Each key MUST be the string representation of a security group **security identifier (SID)** (as specified in [MS-DTYP] section 2.4.2.1), and each value MUST be a **Universal Naming Convention (UNC)** path indicating the destination path to which the indicated user profile folder should be redirected. The client-side plug-in MUST determine what destination path to pass to the folder redirection subsystem by determining what security group the user belongs to. If the user belongs to more than one security group, the client-side plug-in MUST use the first matching securitygGroup mapping that appears in the section.

Note The security group SID MUST begin with either a lowercase or uppercase S and MUST be treated as case-insensitive by the client-side and administrative-side plug-ins.

2.2.2   Folder Redirection Protocol Version One Configuration Data

Version One of the protocol uses the SMB transport to copy a file that MUST be named <gpo path>\User\Documents & Settings\fdeploy1.ini, where <gpo path> is a scoped GPO path. The message is the file itself.

The file MUST contain one section with the SectionID version. The version section MUST contain exactly one key-value pair in the following format: The key MUST be the constant string VersionNumber and the value MUST be the constant string 100.

The Folder Redirection Client-Side Plug-in receives this file, and it MUST ignore entirely any fdeploy1.ini file that contains a version number less than 100 or greater than 199. The Folder Redirection Client-Side Plug-in MAY accept and process (as specified in this document) any fdeploy1.ini file that contains a version number in the range 100 to 199.<7>

To see an example of a version one configuration file example, please see section 4.3.

2.2.2.1   Folder Redirection Section

The file MUST contain another section with the SectionID folder redirection. This section MUST contain zero or more key-value pairs, called GUID-Groups, in the following format: The key is a string representation of a GUID identifying a user profile folder, and GUIDs of well-known folders are listed in the table in section 1.9. The value MUST be one of two representations specifying either a single SID or a list of SIDs, as specified in the sections that follow.

The client-side plug-in MUST determine what per-GUID section to interpret and pass to the folder redirection subsystem, by determining what security group the user belongs to. If the user belongs to more than one security group, the client-side plug-in MUST use the first matching GUID-Group that appears in the section.

2.2.2.1.1   Single-SID Value for the GUID-Groups Pair

In this form, the value of the GUID-Groups pair MUST be the string representation of the security descriptor SID of a security group.<8>

2.2.2.1.2   List-of-SID Values for the GUID-Groups Pair

In this form, the value MUST be a semicolon-delimited, whitespace-free list of *n* security descriptor SIDs. The meaning of this form MUST be interpreted exactly as *n* separate GUID-Groups pairs.

2.2.2.2 Per-GUID Section

For each GUID-Groups pair present in the Folder Redirection section, the file MUST contain an additional Per-GUID section. The SectionID of the Per-GUID section MUST be the string formed by concatenating the key of the GUID-Groups pair, an underscore "_", and the value of the Per-GUID pair.

Note If a list of SID values is defined for the GUID-Groups pair, the SectionID of the Per-GUID section MUST define a section for each individually valid GUID-SID combination separately, just as if the List-of-SIDs had been represented as n separate GUID-Groups pairs.

The Per-GUID section MUST contain one or more key-value pairs. The key names are as follows:

- Flags

- FullPath

- ParentFolder

- RelativePath

- Exclude Folders

The values for each of the keys are explained in the following sections.

2.2.2.2.1 Flags Key

The section MUST contain exactly one key with the constant string Flags. The value MUST be a string representation of a hexadecimal value representing the binary OR of a collection of flags. The client-side plug-in passes the flags to the underlying operating system folder redirection subsystem. As specified in the following table, some flags determine what other flags must or must not be set in the value and what keys must or must not be present in the section. Otherwise, the flags do not affect the behavior of the protocol itself. Those values marked "(same as section 2.2.1.1)" have semantics identical to those of the corresponding flags in section 2.2.1.1; all other flag values either deviate from the section 2.2.1.1 flags or introduce new behaviors relative to section 2.2.1.1.

Flag value	Behavior
0x00000001	Move Contents (same as section 2.2.1.1) Indicates that all contents of the specified folder MUST be moved to the redirected path location.<9>
0x00000002	Follow Parent Folder This flag indicates that the user profile folder MUST be handled (for purposes of redirection) as ordinary contents of its parent folder. Unlike Version Zero, where the parent folder was specified by convention, in Version One, the parent folder MUST be explicitly specified by the ParentFolder key (see section 2.2.2.2.3). Exactly one of the following flags: Follow ParentFolder, Redirect to FullPath, or Redirect To Local MUST be set. The key's parent folder and relative path MUST be present in this section if, and only if, this flag is set.
0x00000004	Redirection Not Specified (same as section 2.2.1.1) This flag indicates that the administrator has specified no specific redirection path for the folder, and that the folder redirection subsystem MUST continue using whatever redirection configuration it was last configured with.<10>

Flag value	Behavior
	If this flag is set, all other flags MUST NOT be set, and the Per-Profile section (see section 2.2.1.2) for the corresponding user profile folder MUST NOT appear in the file.
0x00000008	Advanced Redirection (same as section 2.2.1.1) This flag MUST be used only for display purposes in the administrative-side plug-in. It does not affect the folder redirection protocol, and the client-side plug-in MUST ignore its value.
0x00000010	Exclusive Access This flag indicates that the client folder redirection subsystem MUST create and set the file system access control list on the destination folder to ensure that only the user has access to the contents of the destination folder.<11>
0x00000020	Relocate On Move (same as section 2.2.1.1) This flag indicates that if the policy is ever deleted in the future, the folder redirection MUST be undone.<12>
0x00000200	Check Ownership This flag indicates that the folder redirection subsystem MUST verify (before initiating redirection) that the file system permissions on the destination folder indicate that the user owns the destination folder. If the check fails, the folder redirection subsystem MUST behave as if no redirection had been specified for this user profile folder.
0x00000800	Do Not InheritFlags This flag indicates any redirection flags specified for the parent folder MUST NOT be inherited by this folder. If the Follow Parent Folder flag is set and this flag (Do Not InheritFlags) is not set, all other flags MUST NOT be set. In this case, the plug-in MUST configure the folder redirection subsystem to use the redirection options associated with the user profile folder of which the present user profile is a descendent. If this flag is set, the Follow Parent Folder flag MUST be set. In this case, the plug-in MUST configure the folder redirection subsystem to use the redirection options specified by this flag's key.
0x00001000	Redirect To FullPath This flag indicates that the folder MUST be redirected to the full path, as specified in section 2.2.2.2.2. Exactly one of the following flags: Follow ParentFolder, Redirect To FullPath, or Redirect To Local MUST be set. The key FullPath MUST be present in this section if, and only if, this flag is set.
0x00002000	Redirect To Local This flag indicates that the plug-in MUST configure the folder redirection subsystem to use the default destination for the user profile folder, typically a directory on the local computer file system. Exactly one of the following flags: Follow ParentFolder, Redirect to FullPath, or Redirect To Local MUST be set.
0x00004000	Exclude Known SubFolders If set, this flag indicates that the specified redirection options MUST NOT be applied to any subfolder associated with a user profile folder identified by a GUID in the value list using the ExcludeFolders key, as specified in section 2.2.2.2.5. This section MUST contain an ExcludeFolders key if, and only if, this flag is set.

Flag value	Behavior
0x00008000	Apply to Downlevel This flag is used only for display purposes in the administrative-side plug-in. It does not affect the folder redirection protocol, and the client-side plug-in MUST ignore its value.

2.2.2.2.2 FullPath Key

The section MUST contain one key with the constant string FullPath if the flag 0x00001000 is set, as defined in section 2.2.2.2.1. The value MUST be a UNC path identifying the destination path to which the folder redirection subsystem should redirect the user profile folder that is identified by the GUID in the SectionID for this section. The value of this pair communicates the same information as the value part of the security group mapping in the Version Zero file format.

2.2.2.2.3 ParentFolder Key

The section MUST contain one key with the constant string ParentFolder if the flag 0x00000002 is set, as defined in section 2.2.2.2.1. The value MUST be a **curly braced GUID string**. If this key is present, it indicates that the folder redirection subsystem MUST redirect this user profile folder to a child directory of the redirection destination for the user profile folder that is specified by the value GUID. The name of the child directory MUST be the string value associated with the RelativePath key defined in section 2.2.2.2.4.

2.2.2.2.4 RelativePath Key

The section MUST contain at most one key with the constant string RelativePath if the flag 0x00000002 is set, as defined in section 2.2.2.2.1. This key indicates to the folder redirection subsystem that it MUST treat the value as a relative file system path, using the backslash character "\" as a directory delimiter. The subsystem MUST determine the redirection destination as the concatenation of the destination path of the parent folder (as specified by the ParentFolder key) and the relative path indicated by the value of this key. The RelativePath key value MUST NOT start with a backslash character "\".

2.2.2.2.5 ExcludeFolders Key

The section MUST contain one key with the constant string ExcludeFolders if the flag 0x00004000 is set, as defined in section 2.2.2.2.1. This pair has a key with the constant string ExcludeFolders. The value MUST be a semicolon-delimited list of curly braced GUID strings. This key indicates that the folder redirection subsystem MUST NOT apply the redirection options specified in this section to any subfolder associated with a user profile folder identified by a GUID in the value list.

3 Protocol Details

3.1 Folder Redirection Administrative-Side Plug-In Details

3.1.1 Abstract Data Model

This section describes a model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to explain how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with what is described in this document.

This Folder Redirection Administrative-Side Plug-in relies on a collection of settings specified in section 2.2.1.1, and it is stored as a configuration file with encoded **Unicode** characters at a remote storage location, such as a network share whose path is passed to it by the Group Policy Object, as specified in [MS-GPOL].

The Folder Redirection Administrative-Side Plug-in reads these settings from the remote storage location and displays them to an administrator by way of a user interface.

An administrator may then use the user interface to make further configuration changes to users' folders, and the administrative-side plug-in should write these changes back to the remote storage location as a Unicode configuration file whose format is defined in section 2.2.1.1.

Note The preceding conceptual data can be implemented using a variety of techniques. Any data structure that stores the preceding conceptual data may be used in the implementation.

3.1.2 Timers

None.

3.1.3 Initialization

Initialization occurs upon initiation of the administrative-side plug-in by an administrator using the Group Policy Protocol, as specified in [MS-GPOL]. The plug-in then relies on the Group Policy Protocol to give it a GPO path. From the GPO path, the administrative-side plug-in MUST construct the location of the remote storage location in which to store the folder redirection configuration data, and attempt to read the file. For Version Zero of the folder redirection protocol, the file name used MUST be <gpo path>\User\Documents & Settings\fdeploy.ini; and for Version One of the protocol, the file name used MUST be <gpo path>\User\Documents & Settings\fdeploy1.ini, where <gpo path> is the GPO path. File reads MUST be performed, as specified in [MS-GPOL].

3.1.4 Higher-Layer Triggered Events

When initiated by an administrator, the Folder Redirection Administrative-Side Plug-in MUST read the protocol configuration data from the remote storage location and pass that information to a user interface to display the current settings to an administrator. If the administrator makes any settings changes for a folder through the user interface of the administrative-side plug-in, the Folder Redirection Administrative-Side Plug-in MUST write that configuration data as Unicode (in a file using the format specified in section 2.2.1) to the remote storage location using remote file access.

For Version Zero of the folder redirection protocol, the file name used MUST be <gpo path>\User\Documents & Settings\fdeploy.ini; and for Version One of the protocol, the file name MUST be <gpo path>\User\Documents & Settings\fdeploy1.ini, where <gpo path> is provided by the Group Policy Protocol, as specified in [MS-GPOL].

After every creation, modification or deletion that affects a Folder Redirection Protocol Configuration Data file on SYSVOL, the administrative tool MUST invoke the Group Policy Extension Update event as specified in [MS-GPOL] 3.3.4.4.

3.1.4.1 Extraneous Data Ignored

Any sections or keys in the configuration file that do not conform to the configuration format, as specified in sections 2.2.1 and 2.2.2, MUST be ignored by the administrative-side plug-in. When the administrative-side plug-in modifies a configuration file, the new file it stores MUST include any unrecognized sections and any unrecognized keys in sections that the plug-in has not deleted or replaced entirely.

3.1.4.2 Using the Protocol Versions

The administrative-side plug-in SHOULD store both a Version One and a Version Zero file to ensure that heterogeneous clients can make maximum use of the protocol. That is, the administrative-side plug-in MUST store a Version Zero file and SHOULD store a Version One file in addition.<13>

3.1.5 Timer Events

None.

3.1.6 Other Local Events

None.

3.2 Folder Redirection Client-Side Plug-in Details

3.2.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to explain how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with what is described in this document.

This Folder Redirection Client-Side Plug-in uses a collection of settings specified in section 2.2.1.1, and stored as a Unicode configuration file at a specific remote storage location, such as a network share. This location is passed to the plug-in by the Group Policy Object, as specified in [MS-GPOL].

The Folder Redirection Client-Side Plug-in parses and interprets the file as specified in section 2 and then configures the folder redirection subsystem with the relevant parameters extracted from the file. The folder redirection subsystem may store its configuration persistently. From the configuration, the Client-Side Plug-in MUST persist the setting that determines the behavior when the folder redirection is removed for the folder.<14> At some later time, if the folder redirection subsystem learns via Group Policy that the user no longer belongs to the security group that established the previous redirection, and the previous redirection configuration had the Relocate On Move flag set (for Version Zero of the protocol) or had Redirect To Local set (for Version One), then the folder redirection subsystem moves the contents of the user profile folder from the previously configured destination to the default destination for the user profile folder (typically a directory on the local computer file system).

Note This conceptual data can be implemented using a variety of techniques. An implementation is at liberty to implement such data in any way it pleases.

AlwaysWaitForNetworkAtStartupAndLogon: A Boolean value indicating whether a computer waits for network connectivity at the time of the startup and logon process.<15>

Redirection Destination: For each GPO contained in the **New or Changed GPO list** and for each security descriptor SID, the UNC path identifying the destination path.

Parent Folder ID: For each GPO contained in the **New or Changed GPO list** and for each security descriptor SID, the GUID for the well-known user profile folder (see section 1.9) that is the parent folder for the user profile folder being redirected.

Excluded Folders List: For each GPO contained in the **New or Changed GPO list** and for each security descriptor SID, the list of folders, in the form of binary GUIDs, whose subfolders are excluded from the redirection options being applied.

3.2.2 Timers

None.

3.2.3 Initialization

When the client-side plug-in is initialized by the Group Policy Protocol, as specified in [MS-GPOL], it MUST read in the configuration data from the remote storage location, as specified in section 3.1.3. If **AlwaysWaitForNetworkAtStartupAndLogon** is TRUE, the client-side plug-in MUST wait for network connectivity before attempting to read the configuration data from the remote storage location.

3.2.4 Higher-Layer Triggered Events

3.2.4.1 Process Group Policy

When a user logs on to a computer that implements Group Policy, the Group Policy: Core Protocol invokes this Process Group Policy event, whose abstract interface is specified in [MS-GPOL] section 3.2.4.1, to apply policies handled by this extension.

When this event is triggered, the Folder Redirection Client-Side Plug-in ignores the **Deleted GPO list** and takes action on the **New or Changed GPO list**, **SessionFlags**, and **SecurityToken**, as described in section 3.2.5.

3.2.5 Message Processing Events and Sequencing Rules

If **SessionFlags**, as specified in [MS-GPOL] section 3.2.4.1, has the Computer Policy Application Mode flag (0x00000001) set, the Folder Redirection Client-Side Plug-in MUST NOT attempt to process the group policy configuration, and MUST return ERROR_INVALID_PARAMETER to the caller.

If **SessionFlags** has the Policy applying as a background process flag (0x00000010) set, and the Policy applying as a foreground process flag (0x00001000) not set, the Folder Redirection Client-Side Plug-in MUST NOT attempt to process the group policy configuration, and MUST return ERROR_SYNC_FOREGROUND_REFRESH_REQUIRED to the caller.

For all other values of **SessionFlags**, the Folder Redirection Client-Side Plug-in MUST process the group policy configuration as follows. The client-side plug-in MUST use the location of fdeploy1.ini or fdeploy.ini passed to it in the **New or Changed GPO list** by the Group Policy: Core Protocol (as specified in [MS-GPOL] section 3.2.4.1), and MUST read protocol-specific data from the configuration file from the remote storage location. For accessing the fdeploy.ini file, the client-side plug-in SHOULD impersonate the policy target using **SecurityToken** as specified in [MS-DTYP]

section 2.7.1 and [MS-DTYP] section 2.7.2. Based on the configuration file, the client-side plug-in determines what user folder locations need to be updated with the new locations specified in the configuration data, and calls on the operating system folder redirection subsystem to perform that action. The client-side plug-in also passes any additional redirection options, as specified in sections 2.2.1.1 and 2.2.2.2.1, to the external component.

The steps to read the "fdeploy1.ini" file and store the folder redirection information are described as follows.

For each GPO in "**New or Changed GPO list**"

- From entries under [Folder_Redirection] section of "fdeploy1.ini" file, create an array of unique user profile folder GUIDs

- For each user profile folder GUID

  - Parse the semicolon-delimited string of SIDs

  - For each SID

    - Under section [{folder GUID}_<SID>], read the value associated with the "**Flags**" key

    - If 0x00000004 (Redirection Not Specified) is not set

      - If 0x00001000 (Redirect To FullPath) is set

        - Read the value associated with the "FullPath" key

        - Store the value in abstract element **Redirection Destination**

      - Else if 0x00000002 (Follow Parent Folder) is set

        - Read the value associated with the "ParentFolder" key

        - Convert curly braced GUID string to a binary GUID

        - Store the binary GUID in abstract element **Parent Folder ID**

        - Read the value associated with the "RelativePath" key

        - Store the value in abstract element **Redirection Destination**

    - Read the value associated with the "ExcludeFolders" key

    - Parse the semicolon-delimited string to obtain list of folder curly braced GUID strings

    - For each curly braced GUID string

      - Convert the string to a binary GUID

      - Append the binary GUID to abstract element **Excluded Folders List**

3.2.5.1 Ignoring Extraneous Data

Any sections or keys in the configuration file that do not conform to the configuration format, as specified in sections 2.2.1 and 2.2.2, MUST be ignored by the client-side plug-in.

3.2.5.2 Using the Protocol Versions

When Group Policy provides a GPO path, the client SHOULD try Version One of the protocol; the client should attempt to retrieve fdeploy1.ini using the GPO path, as specified in section 3.1.3, and parse it according to section 2.2.2. If the client successfully accesses the Version One file, it MUST NOT try Version Zero. If the Version One file is absent, the client SHOULD try Version Zero. It SHOULD attempt to retrieve fdeploy.ini, and, if successful, parse it according to section 2.2.1.

Alternatively, the client MAY simply attempt Version Zero of the protocol, fetching only fdeploy.ini and, if successful, parsing it according to section 2.2.1.<16>

3.2.5.3 Using Redirection Values

The client-side plug-in MUST pass the value of each key present in the User Profile Folder section to the operating system folder redirection subsystem.<17>

3.2.5.4 Unspecified Redirection

If the protocol does not specify redirection for a particular user profile folder, or if it does specify redirection but sets the flag Redirection Not Specified, the client-side plug-in MUST configure the folder redirection subsystem to allow the user to explicitly redirect that user profile folder. Otherwise, if a policy with the Redirection Not Specified flag not set is provided, the folder redirection subsystem MUST prevent the user from explicitly redirecting that user profile folder.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4   Protocol Examples

In the following example, consider two user profile folders, Documents and My Pictures, that an operating system makes available for redirection. Suppose that, due to security and backup concerns, the network administrator wants to enforce a policy that no users store documents and pictures on their local machines. Therefore, the network administrator expects that for users to whom a certain GPO applies, computers to which they log on will relocate the users' Documents and My Pictures folders to a network UNC path that the administrator has defined.

The administrator invokes the Folder Redirection Administrative-Side Plug-in by way of its user interface, and establishes a folder redirection Group Policy that redirects the Documents and My Pictures folders for all users on that specific GPO from those folders' current locations to a centralized network storage location. The administrator also specifies that all current contents of these folders be moved to the new location. Suppose that each user in the network belongs to exactly one of two security groups: S-1-1-0 and S-1-2-3. The administrator declares that:

- For every user in either security group S-1-1-0 or security group S-1-2-3, the user's Documents folder should be redirected to:

    - \\fileserver1\%USERNAME%\My Documents, or

    - \\fileserver2\%USERNAME%\My Documents, respectively.

- For every user in security group S-1-1-0, the user's My Pictures folder should be redirected to:

    - \\fileserver1\%USERNAME%\My Pictures.

Based on the administrator's selections, the Folder Redirection Administrative-Side Plug-in creates both a Version Zero and a Version One configuration file for that GPO at the GPO path provided by the Group Policy Protocol, as specified in [MS-GPOL]. Examples of each version of the Folder Redirection configuration data file appear in sections 4.1 and 4.2.

When each user logs on to a machine in the network, the Folder Redirection Client-Side Plug-in will be initiated by the Group Policy Protocol, as specified in [MS-GPOL], during the user logon process. If the user belongs to the GPO, the client-side plug-in will read this configuration data from the remote storage location. Based on the configuration, the plug-in configures the folder redirection subsystem to redirect the user's current Documents and My Pictures folder paths from their current locations to the locations declared by the administrator. During this process, the subsystem will also copy all the current contents of these folders to the new locations.

Folder redirection allows users to access their data from any authenticated machine participating in the domain. It also enables the IT department to back up all the user's data from a centralized location.

4.1   Folder Redirection Protocol Version Zero Configuration Data

The following example is a Version Zero folder redirection configuration file implementing the example policy:

```
[FolderStatus]
My Documents=11
My Pictures=11

[My Documents]
S-1-1-0=\\fileserver1\%USERNAME%\My Documents
S-1-2-3=\\fileserver2\%USERNAME%\My Documents
```

Release: Friday, October 25, 2013

```
[My Pictures]
S-1-1-0=\\fileserver1\%USERNAME%\My Pictures
```

4.2   Folder Redirection Protocol Version One Configuration Data

The following example is a Version One folder redirection configuration file implementing the example policy:

```
[version]
version=100

[Folder_Redirection]
{33E28130-4E1E-4676-835A-98395C3BC3BB}=S-1-1-0;
{FDD39AD0-238F-46AF-ADB4-6C85480369C7}=S-1-1-0; S-1-2-3

[{33E28130-4E1E-4676-835A-98395C3BC3BB}_S-1-1-0]
Flags=1001
FullPath=\\FileServer1\FR\%USERNAME%\Pictures

[{FDD39AD0-238F-46AF-ADB4-6C85480369C7}_S-1-1-0]
Flags=1001
FullPath=\\FileServer1\%USERNAME%\Documents

[{FDD39AD0-238F-46AF-ADB4-6C85480369C7}_S-1-2-3]
Flags=1001
FullPath=\\FileServer2\%USERNAME%\Documents
```

4.3   Version One Configuration File Example

The following is an example of a Version One configuration file. This example illustrates only some of the redirection options, as specified in section 2.2.1.

```
[version]
version=100

[Folder_Redirection]
{1777F761-68AD-4D8A-87BD-30B759FA33DD}=S-1-1-0;
{33E28130-4E1E-4676-835A-98395C3BC3BB}=S-1-1-0;
{FDD39AD0-238F-46AF-ADB4-6C85480369C7}=S-1-1-0;
{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}=S-1-1-0; S-1-2-0

[{1777F761-68AD-4D8A-87BD-30B759FA33DD}_S-1-1-0]
Flags=2001

[{33E28130-4E1E-4676-835A-98395C3BC3BB}_S-1-1-0]
Flags=1001
FullPath=\\FileServer1\FR\%USERNAME%\Pictures

[{FDD39AD0-238F-46AF-ADB4-6C85480369C7}_S-1-1-0]
Flags=1001
FullPath=\\FileServer1\%USERNAME%\Documents
```

```
[{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}_S-1-1-0]
Flags=1001
FullPath=\\FileServer1\%USERNAME%\Appdata

[{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}_S-1-2-0]
Flags=4001
FullPath=\\FileServer1\%USERNAME%\AppData
ExcludeFolders=625B53C3-AB48-4EC1-BA1F-A1EF4146FC19
```

4.4   Version Zero Configuration File Example

An example of a Version Zero configuration file follows. This example illustrates only some of the redirection options specified in section 2.2.1.

```
[FolderStatus]
My Documents=11
My Pictures=2
Desktop=11
[My Documents]
S-1-1-0=\\fileserver1\%USERNAME%\My Documents
S-1-2-3=\\fileserver2\%USERNAME%\My Documents
[Desktop]
S-1-1-0=\\fileserver1\%USERNAME%\Desktop
```

5   Security

5.1   Security Considerations for Implementers

The Group Policy: Folder Redirection Protocol Extension has security considerations in common with the ones specified in [MS-GPOL], section 5.1 for the Group Policy Protocol.

The administrator can configure folder redirection to use a network on any chosen share, including a hidden share. If this is done, the target share will become accessible via the visible, redirected path. The administrator needs to consider this potential visibility of otherwise hidden shares.

Implementers should take care to follow secure coding and development practices necessary to avoid buffer overflows, denial-of-service attacks, escalation of privilege attacks, and information disclosure risks. For an introduction to these concepts, secure development best practices, and common errors, see [HOWARD].

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:

▪ Windows 2000 operating system

▪ Windows XP operating system

▪ Windows Server 2003 operating system

▪ Windows Vista operating system

▪ Windows Server 2008 operating system

▪ 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

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 1.3.2: In Windows 2000 Server, Windows XP, and Windows Server 2003, a constant list of exactly five user profile folders can be redirected, including My Documents, My Pictures, Desktop, Start Menu, and Application Data. In Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2, the set of folders that can be redirected is extensible and includes, by default, the additional folders Music, Videos, Favorites, Contacts, Downloads, Links, Saved Games, and Searches. The Group Policy: Folder Redirection Protocol Extension is not available on operating system versions earlier than Windows 2000 Server.

<2> Section 1.6: The Check Ownership flag (and, in Windows Vista, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2, the Exclusive Access flag) is enabled by default. A destination folder implemented over a Windows FAT32 File System will not provide the requisite operations. For more information, see section 2.2.2.2.1.

<3> Section 1.7: To illustrate, Windows implementations that support the folder redirection protocol also support relocating the My Documents user profile folder. Windows Vista, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2 also support relocating a new Favorites user profile folder. Thus, when the administrator uses the Folder Redirection Administrative-Side Plug-in to define folder redirection policies for My Documents

and Favorites for a user, the administrative-side plug-in generates a Version One configuration file (described in section 2.2.2).

<4> Section 2.2.1.1: For each file with versions present in the source location of the user profile folder and in the redirected location, the version in the default location is copied to the redirected location only if its file system time stamp is newer than the version to be replaced.

<5> Section 2.2.1.1: For each file with versions present in the source location of the user profile folder and in the redirected location, the version in the default location is copied to the redirected location only if its file system time stamp is newer than the version to be replaced.

<6> Section 2.2.1.1: If the destination folder does not exist, the folder redirection subsystem creates the folder and modifies the file system ACL on the destination folder to ensure that only the user has access to the contents of the destination folder.

<7> Section 2.2.2: Version One configuration data was originally supported in Windows Vista. It is also supported in Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2, which will accept and process such a file.

<8> Section 2.2.2.1.1: Windows Vista, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2 support, by default, the 13 well-known user profile folders listed in section 1.9 and are vendor-extensible to support additional user profile folders.

<9> Section 2.2.2.2.1: For each file with versions present in the source location of the user profile folder and in the redirected location, the version in the default location is copied to the redirected location only if its file system time stamp is newer than the version to be replaced. Once the move is completed, the folder redirection subsystem deletes the user profile folder and all its contents from the source location.

<10> Section 2.2.2.2.1: If this flag is not set, the folder redirection subsystem prevents the user from explicitly changing how this user profile folder is redirected. If this flag is set, the folder redirection subsystem allows the user to change where the user profile is redirected.

<11> Section 2.2.2.2.1: If the destination folder already exists, and the security descriptor on the folder is protected, the folder redirection subsystem will not set the file system access control list on the destination folder, even if this flag is set.

<12> Section 2.2.2.2.1: The folder redirection subsystem remembers the setting of this flag as well as the security group associated with the Per-Profile mapping that establishes the folder redirection. At some later time, if the folder redirection subsystem learns via Group Policy that the user no longer belongs to the security group that established the previous redirection, and the previous redirection configuration had the Relocate On Move flag set, then the folder redirection subsystem moves the contents of the user profile folder from the previously configured destination to the default destination for the user profile folder. This destination is typically a directory on the local computer file system.

<13> Section 3.1.4.2: In Windows 2000 Server, Windows XP, and Windows Server 2003, the administrative-side plug-in stores only a Version Zero file. In Windows Vista, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2, the administrative-side plug-in stores both a Version One file and a Version Zero file.

<14> Section 3.2.1: In Windows 2000, Windows XP, and Windows Server 2003, the removal policy configuration is persisted in:

- %USERPROFILE%\Local Settings\Application Data\Microsoft\Windows\File Deployment\{25537BA6-77A8-11D2-9B6C-0000F8080861}.ini

In Windows Vista, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2, the removal data is stored under this registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\<User's SID>\fdeploy\

Under that key, there is a REG_DWORD value for each redirected folder. The folders are identified by their well-known user profile folder GUIDs (see section 1.9), and the values are set using the flags defined in section 2.2.2.2.1.

<15> Section 3.2.1: In Windows, this is not configured by default. It can be configured via Group Policy settings, and the default behavior can be modified in the computer-specific Registry Policy file in the following location.

Key: Software\Policies\Microsoft\Windows NT\CurrentVersion\Winlogon

Value: SyncForegroundPolicy

Type: REG_DWORD

Size: 4

Data:

- Wait for network: 0x1

- Don't wait for network: 0x0

<16> Section 3.2.5.2: Windows Vista, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2 follow the recommended behavior, trying first Version One and then, if the Version One file is not present in the GPO path folder, trying Version Zero of the protocol. Windows 2000 Server, Windows XP, and Windows Server 2003 follow the alternative behavior, implementing only Version Zero of the protocol.

<17> Section 3.2.5.3: Windows interprets the value as a file system path in which components are delimited by the backslash "\" character. By convention, substrings of the path of the form %USERNAME% are understood to be replaced by the value of an operating system environment variable before the path is interpreted by the operating system file subsystem.

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

Release: Friday, October 25, 2013