[MS-GPDPC]:
Group Policy:
Deployed Printer Connections 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's Open Specification Promise (available here: http://www.microsoft.com/interop/osp) or the Community Promise (available here: http://www.microsoft.com/interop/cp/default.mspx). 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.

- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail 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
05/11/2007	0.1		MCPP Milestone 4 Initial Availability
08/10/2007	0.1.1	Editorial	Revised and edited the technical content.
09/28/2007	0.1.2	Editorial	Revised and edited the technical content.
10/23/2007	0.1.3	Editorial	Revised and edited the technical content.
11/30/2007	0.1.4	Editorial	Revised and edited the technical content.
01/25/2008	0.1.5	Editorial	Revised and edited the technical content.
03/14/2008	1.0	Major	Updated and revised the technical content.
05/16/2008	1.0.1	Editorial	Revised and edited the technical content.
06/20/2008	2.0	Major	Updated and revised the technical content.
07/25/2008	2.0.1	Editorial	Revised and edited the technical content.
08/29/2008	3.0	Major	Updated and revised the technical content.
10/24/2008	3.0.1	Editorial	Revised and edited the technical content.
12/05/2008	3.1	Minor	Updated the technical content.
01/16/2009	3.1.1	Editorial	Revised and edited the technical content.
02/27/2009	3.1.2	Editorial	Revised and edited the technical content.
04/10/2009	3.1.3	Editorial	Revised and edited the technical content.
05/22/2009	3.1.4	Editorial	Revised and edited the technical content.
07/02/2009	3.2	Minor	Updated the technical content.
08/14/2009	3.3	Minor	Updated the technical content.
09/25/2009	3.4	Minor	Updated the technical content.
11/06/2009	3.4.1	Editorial	Revised and edited the technical content.
12/18/2009	3.4.2	Editorial	Revised and edited the technical content.
01/29/2010	3.5	Minor	Updated the technical content.
03/12/2010	3.5.1	Editorial	Revised and edited the technical content.
04/23/2010	3.5.2	Editorial	Revised and edited the technical content.
06/04/2010	3.6	Minor	Updated the technical content.

Date	Revision History	Revision Class	Comments
07/16/2010	3.7	Minor	Clarified the meaning of the technical content.
08/27/2010	3.7	No change	No changes to the meaning, language, or formatting of the technical content.
10/08/2010	3.7	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	3.7	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	3.7	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	4.0	Major	Significantly changed the technical content.

Contents

1   Introduction

The Group Policy: Deployed Printer Connections Extension supports managing connections to printers that are hosted by **print servers** and shared by multiple users.

A Deployed Printer Connections protocol implementation consists of server and client components. The server component allows a network administrator to configure the printer connections. The client component allows a user to discover the printer connections that have been configured.

1.1   Glossary

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

Active Directory
Active Directory object
administrative tool
client-side extension GUID (CSE GUID)
computer policy mode
directory service (DS)
distinguished name (DN)
domain
domain controller (DC)
fully qualified domain name (FQDN)
globally unique identifier (GUID)
group
Group Policy
Group Policy object (GPO)
Group Policy object (GPO) distinguished name (DN)
Group Policy object (GPO) GUID
Kerberos
Lightweight Directory Access Protocol (LDAP)
policy application
policy setting
policy target
print server
registry
schema
scoped Group Policy object (GPO) path
Simple and Protected GSS-API Negotiation Mechanism (SPNEGO)
tool extension GUID
UncPath
Unicode
Universal Naming Convention (UNC)
UTF-8
user policy mode

The following terms are specific to this document:

directory string: A string encoded in **UTF-8**, as defined in [RFC2252] section 6.10.

machine connection: A connection to a printer that is shared from a **print server** from a client machine. The connection may be displayed in the user interface as a printer. **Machine connections** are displayed to all users in all user environments of a particular client machine.

user connection: A connection to a printer that is shared from a **print server** from a client machine. The connection may be displayed in the user interface as a printer. **User connections** are seen by only a specified user account on the client machine.

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

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.

[MS-ADA3] Microsoft Corporation, "Active Directory Schema Attributes N-Z", June 2007.

[MS-ADSC] Microsoft Corporation, "Active Directory Schema Classes", June 2007.

[MS-GPOL] Microsoft Corporation, "Group Policy: Core Protocol Specification", June 2007.

[MS-RPRN] Microsoft Corporation, "Print System Remote Protocol Specification", June 2007.

[MS-SPNG] Microsoft Corporation, "Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Extension", January 2007.

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

[RFC2251] Wahl, M., Howes, T., and Kille, S., "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997, http://www.ietf.org/rfc/rfc2251.txt

[RFC2252] Wahl, M., Coulbeck, A., Howes, T., and Kille, S., "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997, http://www.ietf.org/rfc/rfc2252.txt

1.2.2   Informative References

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary", March 2007.

[SYSPRINT] Microsoft Corporation, "Microsoft Windows Server 2003 R2 Server System Print Management Step-by-Step Guide", September 2005, http://download.microsoft.com/download/a/4/a/a4a3a46e-a10b-45f8-bb7b-da69bd95f04c/PrintMgmtConsole.doc

1.3   Overview

The Group Policy: Deployed Printer Connections Extension uses the Group Policy: Core Protocol [MS-GPOL] to support the use of preconfigured collections of shared printer connections. The Deployed Printer Connections administrative tool plug-in to the **group policy administrative tool** allows network administrators to configure connections to printers that are hosted by print servers and shared to other users, so that those printer connections will appear on a set of client computers or to a set of users, no matter which computers those users log on to.

The Deployed Printer Connections client-side plug-in uses the Deployed Printer Connections protocol to query the **Active Directory domain controller (DC)** in order to obtain the list of printer connections that have been configured by the network administrator for the computer or the user.

1.3.1 Background

The Group Policy: Core Protocol [MS-GPOL] allows clients to discover and retrieve **policy settings** that were created by the administrators of a **domain**. These settings are stored in **Group Policy objects (GPOs)**, which are assigned to **policy target** accounts in Active Directory.<1> By assigning a GPO to policy target accounts, network administrators can ensure that a GPO is associated with certain computer or user accounts in the Active Directory. Each client uses the **Lightweight Directory Access Protocol (LDAP)** [RFC2251], to determine which GPOs apply to it, by querying the **Active Directory objects** that correspond to the computer's account and the user accounts of the users who log on to the client computer.

Each GPO is interpreted on each client computer and acted upon by software components known as client-side plug-ins. The client-side plug-ins that are responsible for a given GPO are specified in an attribute of the GPO. This attribute contains a list of **globally unique identifier (GUID)** pairs. The first GUID of each pair is the **client-side extension GUID (CSE GUID)** that identifies the client-side plug-in and the second GUID is the **tool extension GUID** that identifies the administrative tool plug-in (section 3.1).

For each GPO that is applicable to a client, the client consults the CSE GUID listed in the GPO to determine which client-side plug-ins on the client should handle the GPOs. The client then invokes the client-side plug-ins to handle the GPOs. A client-side plug-in uses the contents of the GPOs to retrieve settings that are specific to its class in a manner that is specific to its class. Once its class-specific settings are retrieved, the client-side plug-in uses those settings to perform class-specific processing.

1.3.2 Deployed Printer Connections

The following diagram shows the consumers of the Deployed Printer Connections protocol.
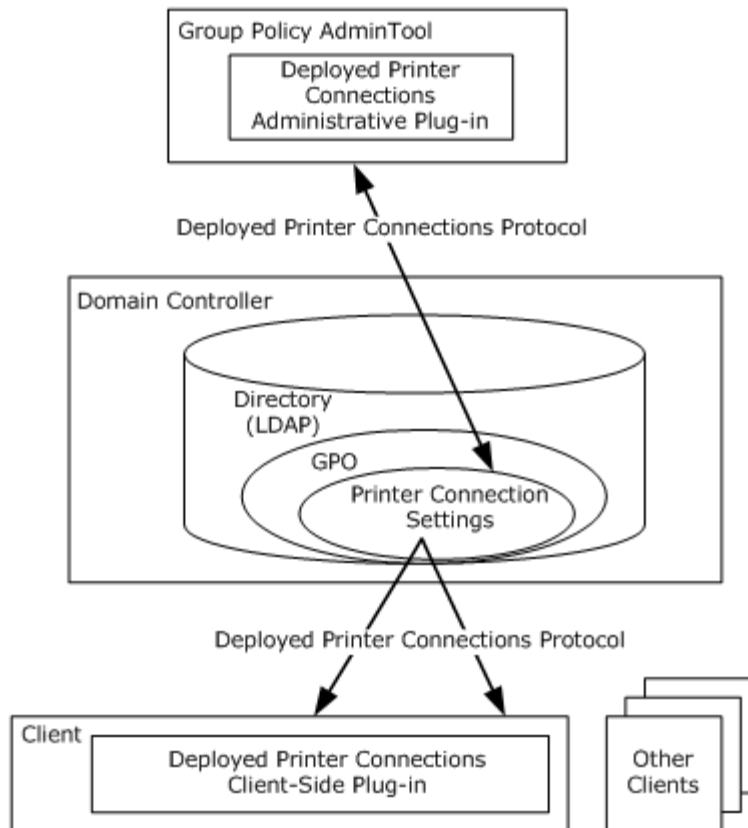
Figure 1: Consumers of the Deployed Printer Connections Protocol

The situations in which this protocol is used are described in two scenarios: the **administrative scenario** and the **client scenario**, which are presented in sections 1.3.2.1 and 1.3.2.2, respectively.

1.3.2.1   Administrative Scenario

An administrator invokes a Group Policy administrative tool to manage a Group Policy Object (GPO), using the Policy Administration Protocol specified in [MS-GPOL] sections 2.2.7 and 2.2.8.<2> This administration is performed on the administrator's machine.

Using the Group Policy: Core Protocol [MS-GPOL], the presence of the tool extension GUID for the Deployed Printer Connections administrative tool plug-in is queried. If present, the GPO contains policy settings that should be administered by using the Deployed Printer Connections administrative tool plug-in.

The administrative tool plug-in stores and retrieves the data from a GPO on a domain controller (DC). This data describes the printer connections that the administrator wants to add to a client that is affected by the GPO. The administrator can view the existing printer connection data and also update it to add new printer connections.

1.3.2.2 Client Scenario

When a client computer that is affected by a GPO starts, or if it is connected to the network after it has been started, it performs **policy application** by retrieving the policy settings for the computer account from the DC using the Group Policy: Core Protocol [MS-GPOL].<3>

When a user logs on or when policy application occurs, the computer connects to the network after the user has logged on. When policy application is performed, the client computer retrieves the policy settings for the user from the DC, by using the Group Policy: Core Protocol.

In both cases, if the Deployed Printer Connections client-side plug-in GUID is read from one or more of the GPOs as part of the GPO processing, the client computer must invoke the Deployed Printer Connections client-side plug-in component to perform policy application.

When the Deployed Printer Connections client-side plug-in performs policy application, the client computer identifies the directive to add the printer connection, which is specified by the administrator, either to all users of the machine or to only the current user.

- In **computer policy mode**, the printer connection was deployed by the administrator as a **machine connection**, and the printer connection is applied to all users of the computer.

- In **user policy mode**, the printer connection was deployed by the administrator as a **user connection**, and the printer connection is applied only to the current user of the computer.

1.4 Relationship to Other Protocols

The Group Policy: Deployed Printer Connections Extension depends on the Group Policy: Core Protocol [MS-GPOL] to update version information in applicable Group Policy objects (GPOs). The administrative tool plug-in for this protocol uses LDAP version 3 [RFC2251] to read and write protocol-specific data. These relationships are illustrated in the following diagram:
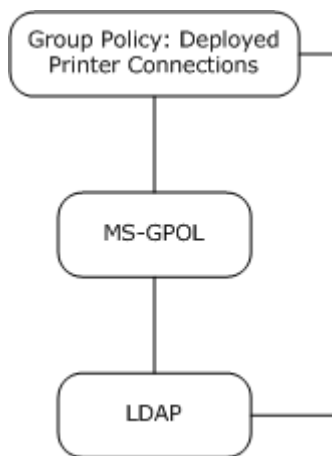

Figure 2: Group Policy: Deployed Printer Connections dependencies

1.5 Prerequisites/Preconditions

The Group Policy: Deployed Printer Connections Extension has no additional prerequisites or preconditions beyond those specified in the Group Policy: Core Protocol.

1.6   Applicability Statement

The Group Policy: Deployed Printer Connections Extension is applicable only within the Group Policy framework, as specified in [MS-GPOL].

1.7   Versioning and Capability Negotiation

The Group Policy: Deployed Printer Connections Extension does not provide versioning or capability negotiations, and it defines no locale-specific data.<4>

1.8   Vendor-Extensible Fields

The Group Policy: Deployed Printer Connections Extension does not define any vendor-extensible fields.

1.9   Standards Assignments

The Group Policy: Deployed Printer Connections Extension defines the CSE GUID and tool extension GUID values, as specified in [MS-GPOL] section 1.8. The assignments are as follows.

Parameter	Value
Tool extension GUID (both user policy settings and computer policy settings)	{180F39F3-CF17-4C68-8410-94B71452A22D}
CSE GUID	{8A28E2C5-8D06-49A4-A08C-632DAA493E17}

2   Messages

2.1   Transport

The Group Policy: Deployed Printer Connections Extension uses LDAP version 3, as defined in [RFC2251], to read and write deployed printer connection settings to GPOs on the domain controller (DC).

After writing a new deployed printer connection setting to a GPO, the Deployed Printer Connections protocol uses the messages specified in [MS-GPOL] section 2.2.4 to update the version information in the GPO.

2.2   Message Syntax

Messages exchanged in the Group Policy: Deployed Printer Connections Extension allow:

- The client-side plug-in to discover settings in the GPOs that indicate that the clients SHOULD add printer connections to the user's system.

- The administrative tool plug-in to query a GPO for a list of printer connection settings.

- The administrative tool plug-in to create and delete printer connection settings on the domain controller (DC).

The Deployed Printer Connections administrative tool plug-in MUST store data in an msPrint-ConnectionPolicy Active Directory object as specified in [MS-ADSC] section 2.140. The Active Directory object MUST be contained in the GPO.

msPrint-ConnectionPolicy objects MUST have the following attributes, as specified in [MS-ADA3] sections 2.330, 2.129, 2.240, and 2.123, respectively.

Attribute	Value
uNCName	The value of this attribute MUST be a **directory string** that specifies the full connection name, and it MUST consist of the server and printer names, as specified in the **Universal Naming Convention (UNC)**, in the form \\server name\printer name.
printerName	The value of this attribute MUST be a directory string that specifies the printer name part of the **uNCName** attribute in the format specified in [MS-RPRN], section 2.2.4.14.
serverName	The value of this attribute MUST be a directory string that specifies the server name part of the **uNCName** attribute in the format specified in [MS-RPRN], section 2.2.4.16.
printAttributes	The value of this attribute SHOULD be zero, and any value of this attribute MUST be ignored during policy application.

msPrint-ConnectionPolicy objects MUST be created in one of the following locations in the Active Directory where <x>, <y>, <z> is the **fully qualified domain name (FQDN)** of the domain/LDAP server and <GPO_GUID> is the GUID of the GPO that is being queried or updated.

- Printer connection settings in the User section of the GPO MUST use this location:

    CN=PushedPrinterConnections, CN=User, CN=<GPO_GUID>, CN=Policies, CN=System, DC=<x>, DC=<y>, DC=<z>

- Printer connection settings in the Machine section of the GPO MUST use this location:

CN=PushedPrinterConnections, CN=Machine, CN=<GPO_GUID>, CN=Policies, CN=System, DC=<x>, DC=<y>, DC=<z>

The messages that are used by this protocol perform the following functions:

- Printer connection setting creation

- Printer connection setting deletion

- Printer connection setting retrieval

Unless specified otherwise, the format used for GUID values in this protocol is the curly-braced string representation ([MS-DTYP] section 2.3.2.3).

2.2.1   Deployed Printer Connection Setting Creation Messages

2.2.1.1   PushedPrinterConnections Container Creation

The PushedPrinterConnections container, under the User or Computer that is contained in the GPO in Active Directory, is the container for all msPrint-ConnectionPolicy objects that represent deployed printer connections. This message is an LDAP AddRequest message as specified in [RFC2251] section 4.7. The message MUST have the following fields.

Parameter name	Value
entry	The value of this parameter MUST be a Computer or User section of the scoped **GPO distinguished name (DN)**, as specified in [MS-GPOL].
attributes	The value of this parameter MUST specify the values of the **objectClass** and **name** attributes in an **AttributeList** as specified in [RFC2251], section 4.7.

The *attributes* parameter of this message MUST contain the attribute name and value pairs that are specified in the following table.

Attribute name	Value
objectClass	The value of this attribute MUST be the directory string "container".
name	The value of this attribute MUST be the directory string "PushedPrinterConnections".

2.2.1.2   Printer Connections Creation

This message instructs the domain controller (DC) to create an msPrint-ConnectionPolicy object in the Active Directory. The LDAP portion of the message is an LDAP AddRequest as specified in [RFC2251], section 4.7, and MUST have the following parameters:

Parameter name	Value
entry	The value of this parameter MUST be the **distinguished name (DN)** that corresponds to the PushedPrinterConnections container in a User or Computer container in a scoped GPO DN.
attributes	The value of this parameter MUST specify the values of the **uNCName**, **printerName**, **serverName**, and **printAttributes** attributes in an **AttributeList**, as specified in

Parameter name	Value
	[RFC2251], section 4.7.

The *attributes* parameter of this message MUST contain a list of attribute name/value pairs, as specified in the following table:

Attribute name	Value
objectClass	The value of this attribute MUST be the directory string value "msPrint-ConnectionPolicy".
uNCName	The value of this attribute MUST specify a value of **uNCName**, as specified in section 2.2.
printerName	The value of this attribute MUST specify a value of **printerName**, as specified in section 2.2.
serverName	The value of this attribute MUST specify a value of **serverName**, as specified in section 2.2.
printAttributes	The value of this attribute MUST specify a value of **printAttributes**, as specified in section 2.2.

2.2.2 Deployed Printer Connection Setting Deletion Message

This message instructs the DC to delete an **msPrint-ConnectionPolicy** object in Active Directory. The LDAP portion of the message is an LDAP **DelRequest**, as specified in [RFC2251], section 4.8.

The *LDAPDN* parameter specifies the Printer Connection Setting distinguished name (DN) of the msPrint-ConnectionPolicy object.

2.3 Directory Service Schema Elements

The Group Policy: Deployed Printer Connections Extension to the Group Policy: Core Protocol [MS-GPOL] accesses the **directory service (DS) schema** classes and attributes that are listed in the following table. For the syntactic specifications of the <Class> or <Class> <Attribute> pairs, refer to [MS-ADSC] and [MS-ADA3].

Class	Attribute
msPrint-ConnectionPolicy	All
container	name

3   Protocol Details

The Group Policy: Deployed Printer Connections Extension administrative tool plug-in reads and writes printer connection settings on the Active Directory server.

The Deployed Printer Connections client-side plug-in reads printer connection settings from the Active Directory server.

3.1   Administrative Tool Plug-in Details

The administrative tool abstract data model, as specified in [MS-GPOL] section 3.3.1, allows the Deployed Printer Connections administrative tool plug-in to write extension-specific data that it receives from a user interface to Active Directory.

3.1.1   Abstract Data Model

The administrative tool plug-in has a user interface that allows an administrator to deploy a printer connection to a GPO in the format that is specified in section 2.2.

3.1.2   Timers

None.

3.1.3   Initialization

When the administrative tool plug-in starts up, it gets a **scoped GPO path** from the Group Policy: Core Protocol in the following form:

CN=<GPO_GUID>,CN=Policies,CN=System,DC=<x>,DC=<y>,DC=<z>

where <x>,<y>,<z> is the fully qualified domain name (FQDN) of the domain/LDAP server, and <GPO_GUID> is the GUID of the GPO that is being queried or updated. The administrative tool plug-in MUST attempt to use LDAP to retrieve any existing printer connection settings from the scoped GPO path, as specified in section 3.1.5.3.

3.1.4   Higher-Layer Triggered Events

When a network administrator adds a printer connection to a GPO by using the administrative tool plug-in, the administrative tool plug-in MUST add the connection to Active Directory, as specified in section 2.2.1. If this fails, the administrator MUST be informed.

When a network administrator deletes a printer connection from a GPO by using the administrative tool plug-in, the administrative tool plug-in MUST delete the connection from Active Directory, as specified in section 2.2.2. If this fails, the administrator MUST be informed.

3.1.5   Message Processing Events and Sequencing Rules

This section specifies message processing and sequencing for the following events:

- An administrator adding a printer connection to a GPO (section 3.1.5.1).

- An administrator deleting a printer connection from a GPO (section 3.1.5.2).

- An administrator retrieving a GPO (section 3.1.5.3).

3.1.5.1 Adding a Printer Connection

This section specifies the processing events and sequencing for an administrator adding a printer connection to a GPO.

The Deployed Printer Connections administrative tool plug-in receives extension-specific information from a user interface and writes the data in conformance with [RFC2251].

One msPrint-ConnectionPolicy object is created for each Deployed Printer Connection setting that is received from the user interface.

The Deployed Printer Connections administrative tool plug-in sends a message to the DC indicating that a new printer connection setting SHOULD be added to a GPO. This message is sent using the LDAP as a transport. Authentication MUST be either **Kerberos** with credentials in **Unicode** for computer policy mode, or **Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) [MS-SPNG]** for user policy mode.

The following protocol sequences MUST be generated to add a printer connection to a GPO:

1. The administrative tool plug-in MUST send an LDAP BindRequest to Active Directory, and Active Directory MUST generate an LDAP BindResponse in reply. The parameters for the BindRequest MUST include a zero-length string for the distinguished name (DN) parameter; and the authentication choice MUST be either Kerberos for computer policy mode, or SPNEGO for user policy mode. The value of the **version** field MUST be 3.

2. The administrative tool plug-in MUST wait for a successful BindResponse from Active Directory.

3. The user interface administrative tool SHOULD allow the network administrator to specify:

   ▪ The LDAP address of the GPO that is to be modified.

   ▪ A choice of modifying either the Machine section or the User section of the GPO, so that the connections can be added for either all users of the computer or only one user.

   ▪ The **UncPath** of the printer connection that is to be added.

4. Using the LDAP address that was obtained from a successful BindResponse, the client MUST send an LDAP AddRequest message to create a container, as specified in PushedPrinterConnections Container Creation (section 2.2.1.1), in one of the following locations, where <x>,<y>,<z> is the fully qualified domain name (FQDN) of the domain/LDAP server, and <GPO_GUID> is the SPNEGO GUID of the GPO that the administrator selected in the user interface.

   ▪ Printer connection settings in the User section of the GPO MUST use this location:

   CN=PushedPrinterConnections, CN=User, CN=GPO_GUID,
   CN=Policies,CN=System,DC=<x>,DC=<y>,DC=<z>

   ▪ Printer connection settings in the Machine section of the GPO MUST use this location:

   CN=PushedPrinterConnections, CN=Machine, CN=GPO_GUID,
   CN=Policies,CN=System,DC=<x>,DC=<y>,DC=<z>

   If the **resultCode** field of the corresponding LDAP AddResponse message is nonzero, this protocol sequence MUST skip the intervening steps and the administrative tool plug-in MUST make an LDAP UnbindRequest to close the connection.

5. The administrative tool plug-in MUST send an LDAP AddRequest message, as specified in Printer Connections Creation (section 2.2.1.2), to add an msPrint-ConnectionPolicy object in the PushedPrinterConnections container (section 2.2.1.1) that was created in the previous step.

   If the **resultCode** field of the corresponding LDAP AddResponse message is nonzero, this protocol sequence MUST skip the intervening steps and the administrative tool plug-in MUST make an LDAP UnbindRequest to close the connection.

6. Using the methods that are specified in [MS-GPOL] section 3.3.4.5, the version of the GPO MUST be updated, and the GUID of the Deployed Printer Connection administrative tool plug-in MUST be written in the GPO.

7. An LDAP UnbindRequest MUST be made by the administrative tool plug-in to close the connection.

3.1.5.2   Deleting a Printer Connection

This section specifies the processing events and sequencing for an administrator deleting a printer connection from a GPO.

The Deployed Printer Connections administrative tool plug-in sends a message to the DC indicating that a new printer connection setting SHOULD be removed from a GPO. This message uses LDAP as a transport. Authentication MUST be either Kerberos with credentials in Unicode for computer policy mode, or SPNEGO [MS-SPNG] for user policy mode.

The following protocol sequences MUST be generated to delete a printer connection from a GPO:

1. The administrative tool plug-in MUST send an LDAP BindRequest to Active Directory, and Active Directory MUST generate an LDAP BindResponse message in reply. The parameters for the BindRequest MUST include a zero-length string for the DN parameter; and the authentication choice MUST be either Kerberos for computer policy mode, or SPNEGO for user policy mode. The value of the **version** field MUST be 3.

2. The administrative tool plug-in MUST wait for a successful BindResponse from Active Directory.

3. The administrative tool plug-in SHOULD present a list of the printer connection settings in the GPO to the user in an interface using the search specified in section 3.1.5.3, and it SHOULD allow the user to select a printer connection setting for deletion. The LDAP addresses of the printer connection objects in the GPO MUST be maintained by the administrative tool plug-in.

4. Using the LDAP address that was obtained from a successful BindResponse, an LDAP DelRequest message MUST be sent by using the message that is specified in section 2.2.2 to delete the printer connection setting.

   If the **resultCode** field of the corresponding LDAP DelResponse message is nonzero, the administrative tool plug-in SHOULD indicate to the user that an error has occurred.

5. Using the methods that are specified in [MS-GPOL] section 3.3.4.5, the version of the GPO MUST be updated, and the GUID of the Deployed Printer Connection administrative tool plug-in MUST be written in the GPO.

6. An LDAP UnbindRequest MUST be made by the administrative tool plug-in to close the connection.

3.1.5.3 Retrieving a Group Policy Object

This section specifies the processing events and sequencing for an administrator to retrieve an existing Group Policy object (GPO).

The Deployed Printer Connections administrative tool plug-in sends a policy retrieval message. One policy retrieval message is sent by using an LDAP **SearchRequest** message ([RFC2251] section 4.5) to read the extension-specific data from the LDAP **directory** store.

This message uses LDAP as a transport. Authentication MUST be either Kerberos with credentials in Unicode for computer policy mode, or SPNEGO [MS-SPNG] for user policy mode. The purpose of this message is to allow the client to query Active Directory for printer connections settings that are associated with the GPO.

The following protocol sequences MUST be generated for this message:

1. An LDAP **BindRequest** message MUST be sent from the client to Active Directory and an LDAP **BindResponse** message MUST be sent to the client in reply. The parameters of the BindRequest MUST include a zero-length string for the DN parameter, and the authentication choice MUST be either Kerberos for computer policy mode, or SPNEGO for user policy mode. The value of the **version** field MUST be 3.

2. After the client receives a successful BindResponse message, the client MUST send an LDAP SearchRequest message to Active Directory with the following parameters.

Parameter name	Value
baseObject	The value of this parameter MUST be the LDAP DN for the [PushedPrinterConnections container (section 2.2.1.1)](#) inside the User or Machine section of the GPO; and it MUST be in the following form, where <GPO_GUID> is the GUID of the GPO that is being queried, and <x>,<y>,<z> is the fully qualified domain name (FQDN) of the domain/LDAP server: ▪ CN=PushedPrinterConnections, CN=Machine, CN=<GPO_GUID>, CN=Policies,CN=System,DC=<x>,DC=<y>,DC=<z> ▪ CN=PushedPrinterConnections, CN=User, CN=<GPO_GUID>, CN=Policies,CN=System,DC=<x>,DC=<y>,DC=<z>
scope	The value of this parameter MUST be 2 to search the whole subtree.
derefAliases	The value of this parameter MUST be 0.
sizeLimit	The value of this parameter MUST be 0.
timeLimit	The value of this parameter might be 0 if there is no time limit, or it might be the number of seconds; however, it has no direct influence on the protocol defined in this specification.
typesOnly	The value of this parameter MUST be 0 (FALSE).
filter	The value of this parameter MUST be an LDAP filter of "(objectClass=msPrint-ConnectionPolicy)". The query is filtered so that only msPrint-ConnectionPolicy objects are returned.
attributes	The value of this parameter MUST be an **AttributeDescriptionList** ([RFC2251] section 4.1.5). The **AttributeDescriptionList** MUST contain **uNCName** and

Parameter name	Value
	printAttributes attribute names.

3. A successful search response ([RFC2251] section 4.5.2) MUST consist of zero or more LDAP **SearchResultEntry** messages, followed by one LDAP **SearchResponseDone** message. One LDAP SearchResultEntry message MUST be returned for each msPrint-ConnectionPolicy object found in the PushedPrinterConnections container that is identified by the *baseObject* parameter of the LDAP SearchRequest.

   Each LDAP SearchResultEntry message MUST have the following parameters:

Parameter name	Value
objectName	The value of this parameter MUST be the LDAP DN for the msPrint-ConnectionPolicy object found in the PushedPrinterConnections container that is identified by the *baseObject* parameter of the LDAP SearchRequest.
attributes	The value of this parameter MUST be a **PartialAttributeList** ([RFC2251] section 4.5.2). The **PartialAttributeList** MUST contain name and value pairs for the **uNCName** and **printAttributes** attributes.

4. An LDAP **UnbindRequest** MUST be made by the client to close the connection.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2   Client–Side Plug-in Details

The Group Policy: Deployed Printer Connections Extension client-side plug-in has a logical client role because it is responsible for reading the settings that were written by the administrative tool plug-in, and it implements client-specific logic based on those settings. The client-side plug-in is a logical client because either a physical client or a physical server that is used in a client role can host it.

3.2.1   Abstract Data Model

This section describes a conceptual model of a possible data organization that an implementation SHOULD maintain to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This specification does not require that implementations adhere to this model as long as their external behavior is consistent with that described in this specification.

The client-side plug-in uses the following data stores:

DesiredConnections list: A list of printer connections that a network administrator has assigned to a user or to a machine.

PreviouslyAppliedConnections list: A list of printer connections that were assigned to a user or machine, at the previous policy application. When the operating system is installed, the PreviouslyAppliedConnections list MUST be empty.

Printer connections list: A list of printer connections that are maintained by the spooler component. Printer connections are maintained in this list as per-user connections or per-machine connections. Per-machine connections are added for, and usable by, all users of a client computer.

3.2.2 Timers

None.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

The Deployed Printer Connections client-side plug-in reads a list of printer connections, shared from a central server, that a network administrator would like to deploy to client computers, and it configures the client computer based on this information. The client computer then uses the applicable printer connection settings to create connections to printers that a user on the client computer can use.

During policy application, as specified in [MS-GPOL], the Group Policy client MUST obtain a list of all the GPOs that apply to the machine and to the user who is logged on. The Group Policy client MUST then invoke all client-side plug-ins that have data in the applicable GPOs. The applicable data is not passed to the client-side plug-ins. Instead, the client-side plug-ins are passed a list of LDAP addresses for all GPOs in which they have data.

The Deployed Printer Connections client-side plug-in MUST then do the following with the list of LDAP addresses of GPOs that were provided by the Group Policy client, as specified in [MS-GPOL]:

1. The client-side plug-in MUST issue one LDAP search for each GPO to obtain a list of all printer connection settings. The message format for this LDAP search is specified in section 3.1.5.3.

2. The list of printer connection settings that was obtained in the previous step MUST then be stored in the DesiredConnections list, as specified in section 3.2.1.

3. The client-side plug-in MUST filter out duplicate UncPaths from the DesiredConnections list using a string comparison that is case-insensitive for only those characters with code-points in the inclusive ranges from Unicode 'A' (U+0041) through 'Z' (U+005A) and 'a' (U+0061) through 'z' (U+007A).

4. The client-side plug-in MUST compare the DesiredConnections list with the PreviouslyAppliedConnections list, and then:

   - If a connection is in the DesiredConnections list and the PreviouslyAppliedConnections list, the client-side plug-in MUST do nothing.

   - If a connection is not in the DesiredConnections list but is in the PreviouslyAppliedConnections list, the client-side plug-in MUST delete the printer connection from the client system. The

connection is removed from the list of connections that are maintained by the spooler. This can be performed by calling a local operation equivalent to DeletePrinterConnection(UncPath).

- If a connection is in the DesiredConnections list and not in the PreviouslyAppliedConnections list, then:

  - The client-side plug-in MUST add the printer connection by creating a new connection to the printer. The connection is added to the list of connections maintained by the spooler. This can be performed by calling a local operation equivalent to AddPrinterConnection(UncPath).

  - If the printer connection could not be added, a failure case MUST NOT be logged. The client-side plug-in MUST try adding the connection again during the next policy application.

  - A printer connection MUST be added for the current user only or for all users of the machine depending on whether the connection settings are in the User section or Machine section of the GPO.

5. The client-side plug-in MUST save the list of all the printer connections that it maintains as a new version of the PreviouslyAppliedConnections list.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4 Protocol Examples

The Group Policy: Deployed Printer Connections Extension allows network administrators to deploy printer connections to a printer that is shared by a central server to multiple client computers.

For example, suppose that in the fabrikam.com domain, a network administrator wants to deploy the printer connection, "\\fabprint44\b2-2003-clr", to all users on the second floor of the building.

The network administrator uses the administrative tool plug-in to add the \\fabprint44\b2-2003-clr printer connection setting to a previously existing GPO named "Deploy b2-2003-clr printer."

The "Floor2" GPO is linked to the Floor 2 Organizational Unit.

User "JohnQ" is a user with a user account in the Floor 2 Organizational Unit. JohnQ regularly logs on to a computer called "JohnQ-Laptop".

When the network administrator configures the printer connections, the administrative tool plug-in performs the following tasks:

- The network administrator selects the "Deploy b2-2003-clr printer" GPO for editing, and opens a tool that hosts the Deployed Printer Connections administrative tool plug-in.

- The administrator directs the Deployed Printer Connections administrative tool to deploy printer \\fabprint44\b2-2003-clr to the GPO.

- Using the Group Policy: Core Protocol [MS-GPOL], the plug-in creates a new msPrint-ConnectionPolicy object in

  CN=PushedPrinterConnections, CN=User, CN=<GPO_GUID>, CN=Policies, CN=System, DC=fabrikam, DC=com

  where GPO_GUID is the **GPO GUID** of the Deploy b2-2003-clr printer GPO.

- The msPrint-ConnectionPolicy object has the following attributes and values:

Attributes	Values
uNCName	\\fabprint44\b2-2003-clr
printerName	b2-2003-clr
serverName	\\fabprint44
printAttributes	0x00000000

When JohnQ logs on to JohnQ-Laptop, the client-side plug-in performs the following tasks:

- During policy application, the client-side plug-in gets a list of GPOs that apply to the user JohnQ or computer JohnQ-Laptop from the Group Policy system.

- Using [MS-GPOL], the client-side plug-in issues one LDAP search for each GPO to obtain a list of all printer connection settings that apply to "JohnQ" or "JohnQ-Laptop". In this example, the client-side plug-in discovers a user connection that applies to JohnQ, but does not discover a machine connection that applies to JohnQ-Laptop.

- The client-side plug-in adds the discovered printer connection \\fabprint44\b2-2003-clr to its DesiredConnections list, as specified in section 3.2.1. It then compares the DesiredConnections

list with its PreviouslyAppliedConnections list. It discovers that it needs to add that printer connection to the client machine, because it does not appear in the PreviouslyAppliedConnections list.

- The printer connections that are specified in the GPOs are added to the client machine. The client-side plug-in now removes the printer connection \\fabprint44\b2-2003-clr from its DesiredConnections list and adds the printer connection to its PreviouslyAppliedConnections list. JohnQ will subsequently observe a representation of that printer connection in the user interface.

Later, the network administrator wants to remove the printer connection \\fabprint44\b2-2003-clr. The network administrator uses the administrative tool plug-in to remove that printer connection setting from the GPO named "Deploy b2-2003-clr printer." The administrative tool plug-in performs the following tasks:

- The network administrator selects the "Deploy b2-2003-clr printer" GPO for editing, and opens a tool that hosts the Deployed Printer Connections administrative tool plug-in.

- The administrator directs the Deployed Printer Connections administrative tool to remove printer \\fabprint44\b2-2003-clr from the GPO.

- Using [MS-GPOL], the plug-in removes the msPrint-ConnectionPolicy object that corresponds to the \\fabprint44\b2-2003-clr from the GPO Deploy b2-2003-clr printer.

When JohnQ logs onto JohnQ-Laptop, the client-side plug-in performs the following tasks:

- During policy application, the client-side plug-in gets a list of GPOs that apply to the user JohnQ or computer JohnQ-Laptop from the Group Policy system.

- Using [MS-GPOL], the client-side plug-in issues one LDAP search for each GPO to obtain a list of all printer connection settings that apply to "JohnQ" or "JohnQ-Laptop". In this example, the client-side plug-in discovers that there is no user connection that applies to JohnQ, and there is no machine connection that applies to JohnQ-Laptop.

- The client-side plug-in compares its DesiredConnections list with its PreviouslyAppliedConnections list; and discovers that it needs to remove printer connection \\fabprint44\b2-2003-clr from the client machine because it appears in the PreviouslyAppliedConnections list but does not appear in the DesiredConnections list.

- The client-side plug-in removes the printer connection \\fabprint44\b2-2003-clr from the client machine. It also removes the printer connection from its PreviouslyAppliedConnections list. JohnQ will subsequently observe that the representation of the \\fabprint44\b2-2003-clr printer connection is removed from the user interface.

Release: Friday, February 4, 2011

5 Security

5.1 Security Considerations for Implementers

Because printer connections are added automatically without any user intervention, implementers of the Group Policy: Deployed Printer Connections Extension should be aware that spoofing of print servers is a concern. Implementers should ensure that a printer connection is added only if the client computer is on a secure network environment; that is, on a network where Active Directory can be contacted.

5.2 Index of Security Parameters

The Group Policy: Deployed Printer Connections Extension does not define any security parameters.

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:

- Microsoft 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

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 1.3.1: The following domain controller (DC)/server versions of Windows support the storing of settings that this protocol generates:

- Windows 2000 Server with an LDAP schema update

- Windows Server 2003 with an LDAP schema update

- Windows Server 2003 R2

- Windows Server 2008

- Windows Server 2008 R2

<2> Section 1.3.2.1: The following versions of Windows support the Group Policy: Deployed Printer Connections Extension in the administrative scenario:

- Windows Server 2003 R2

- Windows Vista

- Windows Server 2008

- Windows 7

- Windows Server 2008 R2

In addition, the administrative scenario is supported when the Administration Tools Pack for Windows Server 2003 R2 is installed on one of the following platforms:

- Windows XP SP2

- Windows XP Professional x64 Edition

- Windows Server 2003

<3> Section 1.3.2.2: The following versions of Windows support the Group Policy: Deployed Printer Connections Extension in the client scenario:

- Windows Server 2003 R2

- Windows Vista

- Windows Server 2008

- Windows 7

- Windows Server 2008 R2

In addition, the client scenario is supported when the application **pushprinterconnections.exe** [SYSPRINT], from one of the preceding versions of Windows, is set up to run as part of a logon script to deploy printers on one of the following platforms:

- Windows 2000

- Windows XP

- Windows Server 2003

<4> Section 1.7: Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 contain the Deployed Printer Connections client-side plug-in.

Windows Server 2003 R2, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 contain the Deployed Printer Connections administrative tool plug-in.

7 Change Tracking

This section identifies changes that were made to the [MS-GPDPC] protocol document between the January 2011 and February 2011 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.

- An extensive rewrite, addition, or deletion of major portions of content.

- The removal of a document from the documentation set.

- Changes made for template compliance.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the language and formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical or language changes were introduced. The technical content of the document is identical to the last released version, but minor editorial and formatting changes, as well as updates to the header and footer information, and to the revision summary, may have been made.

Major and minor changes can be described further using the following change types:

- New content added.

- Content updated.

- Content removed.

- New product behavior note added.

- Product behavior note updated.

- Product behavior note removed.

- New protocol syntax added.

- Protocol syntax updated.

- Protocol syntax removed.

- New content added due to protocol revision.

- Content updated due to protocol revision.

- Content removed due to protocol revision.

- New protocol syntax added due to protocol revision.

- Protocol syntax updated due to protocol revision.

- Protocol syntax removed due to protocol revision.

- New content added for template compliance.

- Content updated for template compliance.

- Content removed for template compliance.

- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated.**

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.

- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact protocol@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
1.1 Glossary	59214 Removed "Unicode string" [MS-GLOS] term and added "directory string" local term.	N	Content updated.
1.1 Glossary	Added [MS-GLOS] term "Simple and Protected GSS-API Negotiation Mechanism (SPNEGO)".	N	Content updated.
1.2.1 Normative References	59214 Added a definition for reference [RFC2252].	N	Content updated.
2.2 Message Syntax	59214 Replaced "Unicode String" with "directory string".	N	Content updated.
2.2.1.1 PushedPrinterConnections Container Creation	59214 Replaced "Unicode String" with "directory string".	N	Content updated.
2.2.1.2 Printer Connections Creation	59214 Replaced "Unicode String" with "directory string".	N	Content updated.
3.1.5 Message Processing Events and Sequencing Rules	59326 Added a reference to the section specifying the retrieval of a GPO.	N	Content updated.
3.1.5.1 Adding a Printer Connection	59386 Specified that Kerberos credentials must be in Unicode.	N	Content updated.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
3.1.5.1 Adding a Printer Connection	60848 Specified a reference to the "Printer Connections Creation" section in the processing step for sending an AddRequest message.	N	Content updated.
3.1.5.1 Adding a Printer Connection	60852 Specified a reference to the "PushedPrinterConnections Container Creation" section in the processing step for sending an AddRequest message.	N	Content updated.
3.1.5.1 Adding a Printer Connection	60914 Specified the processing rule when the result code from an AddResponse message is nonzero.	N	Content updated.
3.1.5.2 Deleting a Printer Connection	59386 Specified that Kerberos credentials must be in Unicode.	N	Content updated.
3.1.5.2 Deleting a Printer Connection	60853 Specified the processing rule when the result code from a DelResponse message is nonzero.	N	Content updated.
3.1.5.3 Retrieving a Group Policy Object	59326 Moved the processing rules for retrieving a group policy object from "Deployed Printer Connection Setting Retrieval Message" section.	Y	Content updated.
3.1.5.3 Retrieving a Group Policy Object	59386 Specified that Kerberos credentials must be in Unicode.	N	Content updated.

Release: Friday, February 4, 2011

8   Index