[MS-GPSO]:
Group Policy System Overview

This document provides an overview of the Group Policy System Overview Protocol Family. It is intended for use in conjunction with the Microsoft Protocol Technical Documents, publicly available standard specifications, network programming art, and Microsoft Windows distributed systems concepts. It assumes that the reader is either familiar with the aforementioned material or has immediate access to it.

A Protocol Family System Document does not require the use of Microsoft programming tools or programming environments in order to implement the Protocols in the System. Developers who have access to Microsoft programming tools and environments are free to take advantage of them.

Abstract

Group Policy enables administrators to define and manage desired computer configurations or policy settings for a large number of users and computers within an Active Directory environment. Administrators can define policy settings once and rely on the Windows operating system to enforce that policy. The Group Policy System (GP System) enables a Group Policy Client to retrieve policy settings from a Group Policy Server and enables administrative tools to retrieve, create, update, and delete policy settings.

This document describes how the protocols in the Group Policy System work together to support this functionality. It describes how this system interacts with the administrative tools used to define and apply policy settings, the data stores where the policy settings are stored, and the various client-side and server-side components that extend the policy application and policy administration functionality of the system.

Revision Summary

Date	Revision History	Revision Class	Comments
02/27/2009	0.1	Major	First Release.
04/10/2009	1.0	Major	Updated and revised the technical content.
05/22/2009	2.0	Major	Updated and revised the technical content.
07/02/2009	2.1	Minor	Updated the technical content.
08/14/2009	2.2	Minor	Updated the technical content.
09/25/2009	2.3	Minor	Updated the technical content.
11/06/2009	2.4	Minor	Updated the technical content.
12/18/2009	3.0	Major	Updated and revised the technical content.
01/29/2010	4.0	Major	Updated and revised the technical content.
03/12/2010	5.0	Major	Updated and revised the technical content.
04/23/2010	6.0	Major	Updated and revised the technical content.
06/04/2010	6.0.1	Editorial	Revised and edited the technical content.

Date	Revision History	Revision Class	Comments
07/16/2010	6.1	Minor	Clarified the meaning of the technical content.
08/27/2010	7.0	Major	Significantly changed the technical content.
10/08/2010	8.0	Major	Significantly changed the technical content.
11/19/2010	8.0	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	9.0	Major	Significantly changed the technical content.
02/11/2011	9.0	No change	No changes to the meaning, language, or formatting of the technical content.
03/25/2011	10.0	Major	Significantly changed the technical content.
05/06/2011	11.0	Major	Significantly changed the technical content.
06/17/2011	11.1	Minor	Clarified the meaning of the technical content.
09/23/2011	11.1	No change	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	11.1	No change	No changes to the meaning, language, or formatting of the technical content.
03/30/2012	11.1	No change	No changes to the meaning, language, or formatting of the technical content.
07/12/2012	11.1	No change	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	11.1	No change	No changes to the meaning, language, or formatting of the technical content.
01/31/2013	11.1	No change	No changes to the meaning, language, or formatting of the technical content.

Contents

1 Introduction 7
1.1 Glossary 7
1.2 References 8
1.2.1 Normative References 8
1.2.2 Informative References 10

2 Overview 11
2.1 System Summary 11
2.2 List of Member Protocols 12
2.3 Relevant Standards 13

3 Foundation 15
3.1 Background Knowledge and System-Specific Concepts 15
3.1.1 Policy Settings 15
3.1.2 Group Policy Objects 16
3.1.3 Group Policy Extensions 17
3.1.3.1 Group Policy Client-Side Extension List 18
3.1.3.2 Group Policy Tool Extension List 20
3.2 System Purposes 21
3.3 System Use Cases 22
3.3.1 Stakeholders and Interests Summary 22
3.3.2 Supporting Actors and System Interests Summary 22
3.3.3 Use Case Diagrams 23
3.3.4 Use Case Descriptions 24
3.3.4.1 Apply Group Policy – GP Client 24
3.3.4.2 Administer Policy – Admin Tool 26

4 System Context 28
4.1 System Environment 28
4.2 System Assumptions and Preconditions 28
4.3 System Relationships 29
4.3.1 Black Box Relationship Diagram 29
4.3.2 System Dependencies 30
4.3.3 System Influences 31
4.4 System Applicability 33
4.5 System Versioning and Capability Negotiation 33
4.6 System Vendor-Extensible Fields 33

5 System Architecture 34
5.1 Abstract Data Model 34
5.1.1 Server Abstract Data Model 34
5.1.2 Client Abstract Data Model 34
5.1.3 Administrative Tool Abstract Data Model 35
5.2 White Box Relationships 35
5.3 Member Protocol Functional Relationships 37
5.3.1 Member Protocol Roles 37
5.3.2 Member Protocol Groups 39
5.3.2.1 Group Policy Core Protocol Group 39
5.3.2.2 Group Policy Extension Protocol Group 39
5.4 System Internal Architecture 41
5.4.1 Group Policy Server (GP Server) 42

5.4.2 Group Policy Client (GP Client) 42
5.4.3 Group Policy Administrative Tool 43
5.5 Failure Scenarios 43
5.5.1 Connection Disconnected 43
5.5.2 Internal Failures 43
5.5.2.1 Operating System related failures 43
5.5.2.2 Failure in client side extensions 44
5.5.2.3 Link speed determination failure 44
5.5.3 History Repository Errors 44
5.5.4 SYSVOL file access failure 44

6 System Details 45
6.1 Architectural Details 45
6.1.1 Group Policy Protocols Processing 45
6.1.2 Populating Administrative Tools with Configuration Data 47
6.1.3 Authoring a New Policy 48
6.1.4 Administrative Tool Cannot Connect to a Domain Controller 49
6.1.5 Querying Active Directory for Scope of Management (SOM) and Version Information 50
6.1.6 Client Applying Policy 52
6.1.7 Client Cannot Connect to a Domain Controller When Applying Policy 54
6.2 Communication Details 55
6.2.1 Protocol communication between a Group Policy Client and Group Policy Server 55
6.2.1.1 Locate a GP Server 56
6.2.1.2 Domain SOM Search and Response 56
6.2.1.3 Site SOM Search and Response 56
6.2.1.4 GPO Search and Reply 56
6.2.1.5 WMI Filter Processing 57
6.2.1.6 Link Speed Determination 57
6.2.1.7 Policy File Read Operation 57
6.2.2 Protocol communication to and from the Administrative Tool and Group Policy Server 58
6.2.2.1 Creating Group Policy Objects (GPOs) 58
6.2.2.2 Editing Existing Policy 58
6.2.2.2.1 Extension Settings 59
6.2.2.2.2 GPO Property Update 59
6.2.2.2.3 SOM Updates 59
6.3 Transport Requirements 59
6.4 Timers 60
6.5 Non-Timer Events 60
6.6 Initialization and Re-initialization Procedures 60
6.7 Status and Error Returns 60

7 Security 62
7.1 Internal Security 62
7.1.1 Local Data Store 62
7.1.2 Timer Events/Network Events 63
7.1.3 Computer Boot/Logon Events 63
7.2 External Security 63

8 Appendix A: Product Behavior 64

9 Change Tracking 66

10 Index 67

1 Introduction

This Protocol Family System Document (PFSD) is primarily intended to cover the Protocol Family as a whole. In conjunction with the Member Protocols Technical Documents (TDs), which are intended to cover Member Protocols, it presents the rules for information exchange relevant to those Member Protocols and the Protocol Family that are used to interoperate or communicate with a Windows operating system in its various environments.

Managing user and computer behavior in large distributed computer environments requires the ability to implement configuration changes from a central location, and also to provide an effective way to define policies that affect large numbers of users and computers.

Group Policy provides the infrastructure used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers within an **Active Directory** environment. Policy settings are administrative directives that define the behavior of the computers and users in a domain. Administrators can define policy settings once and rely on the Windows operating system to enforce that policy.

1.1 Glossary

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

ACL
Active Directory
administrative tool
curly braced GUID string
directory
distinguished name (DN)
Distributed File System (DFS)
domain
domain controller (DC)
domain naming context (domain NC)
folder
globally unique identifier (GUID)
group
Group Policy
Group Policy Object (GPO)
Group Policy Object (GPO) GUID
Group Policy Object (GPO) path
Internet host name
Kerberos
Lightweight Directory Access Protocol (LDAP)
Netlogon
policy application
policy setting
policy target
print server
registry
scope of management (SOM)
Server Message Block (SMB)
share
site

system volume (SYSVOL)
tool extension GUID

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

Group Policy (GP) Server

The following terms are specific to this document:

Administrative plug-in: This extension plug-in provides the interface for the Group Policy administrator to author and manage policy settings related to the specific context provided by the plug-in.

Admin tool: See also administrative tool

Client plug-in: The client-side plug-in extension retrieves the policy settings from the specified GPO, and then applies these settings on the client.

Group Policy Administrator: The person responsible for defining policy settings and managing the Group Policy infrastructure in a **domain**.

Group Policy Client (GP Client): A client computer that receives and applies settings of a Group Policy Object (GPO).

Group Policy System: The collection of protocols that provide policy processing and administration.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. Note that in [RFC2119] terms, most of these specifications should be imperative, to ensure interoperability. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT. Any specification that does not explicitly use one of these terms is mandatory, exactly as if it used MUST.

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.

This section contains normative and informative references relevant to the **Group Policy System**.

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-ADTS] Microsoft Corporation, "Active Directory Technical Specification".

[MS-AUTHSO] Microsoft Corporation, "Windows Authentication Services System Overview".

[MS-DISO] Microsoft Corporation, "Domain Interactions System Overview".

[MS-DFSC] Microsoft Corporation, "Distributed File System (DFS): Referral Protocol".

[MS-GPAC] Microsoft Corporation, "Group Policy: Audit Configuration Extension".

[MS-GPDPC] Microsoft Corporation, "Group Policy: Deployed Printer Connections Extension".

[MS-GPEF] Microsoft Corporation, "Group Policy: Encrypting File System Extension".

[MS-GPFAS] Microsoft Corporation, "Group Policy: Firewall and Advanced Security Data Structure".

[MS-GPFR] Microsoft Corporation, "Group Policy: Folder Redirection Protocol Extension".

[MS-GPIE] Microsoft Corporation, "Group Policy: Internet Explorer Maintenance Extension".

[MS-GPIPSEC] Microsoft Corporation, "Group Policy: IP Security (IPsec) Protocol Extension".

[MS-GPNAP] Microsoft Corporation, "Group Policy: Network Access Protection (NAP) Extension".

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

[MS-GPPREF] Microsoft Corporation, "Group Policy: Preferences Extension Data Structure".

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

[MS-GPSB] Microsoft Corporation, "Group Policy: Security Protocol Extension".

[MS-GPSCR] Microsoft Corporation, "Group Policy: Scripts Extension Encoding".

[MS-GPSI] Microsoft Corporation, "Group Policy: Software Installation Protocol Extension".

[MS-GPWL] Microsoft Corporation, "Group Policy: Wireless/Wired Protocol Extension".

[MS-KILE] Microsoft Corporation, "Kerberos Protocol Extensions".

[MS-NLMP] Microsoft Corporation, "NT LAN Manager (NTLM) Authentication Protocol".

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

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

[MS-WMI] Microsoft Corporation, "Windows Management Instrumentation Remote Protocol".

[RFC792] Postel, J., "Internet Control Message Protocol", RFC 792, September 1981, http://www.ietf.org/rfc/rfc792.txt

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987, http://www.ietf.org/rfc/rfc1035.txt

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts -- Communication Layers", STD 3, RFC 1122, October 1989, http://www.ietf.org/rfc/rfc1122.txt

[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

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

[RFC4120] Neuman, C., Yu, T., Hartman, S., and Raeburn, K., "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005, http://www.ietf.org/rfc/rfc4120.txt

1.2.2 Informative References

[MS-FRS1] Microsoft Corporation, "File Replication Service Protocol".

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

2 Overview

2.1 System Summary

Group Policy enables an administrator to maintain standard operating environments for specific **groups** of users. As software changes and policies change over time, Group Policy can be used to update the already-deployed standard operating environment until it needs to be updated. Group Policy can also enforce rules, if necessary, by restricting the programs that can be run on company computers.

Group Policy is the enabling technology in Windows that allows programs and administrators to use Active Directory as an infrastructure to centralize network administration, centrally define management policy, and delegate administrative authority. Users, computers, devices, and resources are represented as objects in Active Directory. With Group Policy, administrators can target **policy settings** for everything from users and computers to individual objects throughout the Active Directory hierarchy.

The Group Policy System (GP System) enables a **Group Policy Client** (GP Client) to retrieve policy settings from a **Group Policy (GP) Server** (GP Server) and enables **administrative tools** to retrieve, create, update, and delete policy settings. The protocol that provides the core functionality of the GP System is the Group Policy: Core Protocol as specified in Group Policy: Core Protocol Specification ([MS-GPOL]). The Group Policy system is extensible on both the client side (**policy application**) and the administrative side (policy administration) of the functionality.

The following table describes the GP System components.

Group Policy components

Component	Abbreviation	Description
Administrative Tool	Admin tool	A tool or application that allows administrators to read and write policy settings to and from a **Group Policy Object (GPO)**. It provides the following administrative functions. Manage core aspects of Group Policy system, such as **scope of management (SOM)** and precedence. Edit GPOs, providing read and write access to Active Directory and **SYSVOL** in order to configure GPOs with specific policy directives or settings.
Group Policy Client	GP Client	The Group Policy Client provides the framework that handles common functionality for policy application and client-side extensions (CSEs). It is responsible for reading specific policy settings on target client computers.
Client-Side Store	Local Store	A repository of Group Policy information that is used to: Track changes to Group Policy administrative directives defined in Group Policy Objects. Record events in the Event Log. Store information about the computer and user-specific configuration of the operating system and applications.
Group Policy Server	GP Server	The server contains a writable copy of the Active Directory database, and controls access to network resources.
Active	AD	Active Directory, the Windows-based **directory** service, stores information about objects on a network and makes this information

Component	Abbreviation	Description
Directory		available to users and network administrators. Administrators link Group Policy Objects (GPOs) to Active Directory containers such as **sites**, **domain**, and organizational units (OUs) that include user and computer objects. In this way, policy settings can be targeted to users and computers throughout the organization.
SYSVOL	SYSVOL	The SYSVOL is a set of folders containing important domain information that is stored in the file system rather than in the directory. The SYSVOL contains the largest part of a GPO: the Group Policy template, which includes Administrative Template-based policy settings, security settings, script files, and information regarding applications that are available for software installation.

The following figure provides a high level diagram of the GP System components

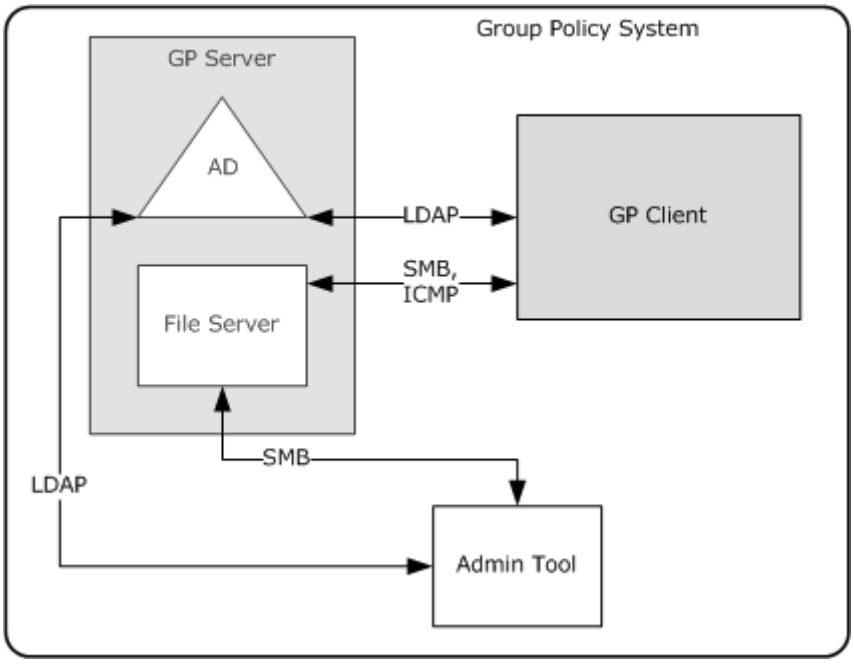

Figure 1: Group Policy System components

2.2 List of Member Protocols

The Group Policy System implements the following protocols:

Group Policy: Audit Configuration Extension, as specified in [MS-GPAC]. This protocol enables an administrator to control advanced audit policies on clients.

Group Policy: Core Protocol, as specified in [MS-GPOL]. This protocol communicates administrator-defined policies between a client and a **domain controller (DC)**.

Group Policy: Deployed Printer Connections Extension, as specified in [MS-GPDPC]. This protocol supports managing connections to printers that are hosted by **print servers** and shared by multiple users.

Group Policy: Encrypting File System Extension, as specified in [MS-GPEF]. The Group Policy: Core Protocol Specification enables remote administrative configuration of the Encrypting File System (EFS).

Group Policy: Firewall and Advanced Security Data Structure, as specified in [MS-GPFAS]. This protocol enables an administrator to control any firewall and advanced security behavior on a client by using group policy-based settings.

Group Policy: Folder Redirection Protocol Extension, as specified in [MS-GPFR]. This protocol enables an administrator to relocate certain file system **folders**, called user profile folders, to different paths, such as a shared network location.

Group Policy: Internet Explorer Maintenance Extension, as specified in [MS-GPIE]. This protocol enables an administrator to manage Internet Explorer configuration settings.

Group Policy: IPsec Protocol Extension, as specified in [MS-GPIPSEC]. This protocol enables centralized (common) configuration of the IPsec component on multiple client systems to provide basic traffic filtering, data integrity, and optionally, data encryption, for IP traffic.

Group Policy: Network Access Protection (NAP) Extension, as specified in [MS-GPNAP]. This protocol enables an administrator to control client computer access to network resources.

Group Policy: Name Resolution Policy Table (NRPT) Data Extension, as specified in [MS-GPNRPT]. This protocol enables an administrator to control any name resolution policy behavior on a client by using group policy-based settings.

Group Policy: Preferences Extension Data Structure, as specified in [MS-GPPREF]. This protocol provides a mechanism for an administrator to manage and deploy preferences.

Group Policy: Registry Extension Encoding, as specified in [MS-GPREG]. This protocol provides a mechanism for an administrator to control any behavior on a client that depends on **registry**-based settings.

Group Policy: Security Protocol Extension, as specified in [MS-GPSB]. This protocol enables security policies to be distributed to multiple client systems so that these systems can enact the policies in accordance with the intentions of the administrator.

Group Policy: Scripts Extension Encoding, as specified in [MS-GPSCR]. This protocol provides a mechanism for an administrator to instruct an arbitrary group of clients to execute administrator-specified code at computer start, computer shut-down, user logon, and user logoff. The code executed by clients is in the form of a command-line tool or batch-processing script that is present either on the client's local file system or at a network file system location.

Group Policy: Software Installation Protocol Extension, as specified in [MS-GPSI]. This protocol enables an administrator to install and remove software applications at client computers. New software versions can also be pushed out to client computers.

Group Policy: Wireless/Wired Protocol Extension, as specified in [MS-GPWL]. This administrative-side plug-in extension specifies and edits wireless or wired policy settings through a user interface, and uses **LDAP** to store the settings to a specific location in a logical structure known as the Group Policy Object. The client-side plug-in uses LDAP to retrieve the wireless or wired policy settings from the specified location, and then applies these settings to the client.

2.3 Relevant Standards

The system uses the standards listed below to allow interoperability with other external systems.

DNS, as specified in [RFC1035]. This standard is used for locating the GP Server and determining site membership.

Kerberos v5, as specified in [RFC4120]. This standard is used for authentication.

Lightweight Directory Access Protocol (LDAP), as specified in [RFC2251]. This standard is used for communication with the GP Server about GP metadata.

NTLM, as specified in [MS-NLMP]. This standard is used for authentication.

SMB, as specified in [MS-SMB]. This standard is used for communication with the GP Server about GP content.

SPNEGO, as specified in [MS-SPNG]. This standard is used for authentication and authorization.

TCP/IP, as specified in [RFC1122]. This standard is used for data transmission for the underlying network.

3 Foundation

This section describes the theoretical and practical information needed to understand this document and this system.

3.1 Background Knowledge and System-Specific Concepts

Organizations face increasingly complex challenges in managing their IT infrastructures. They must deliver and maintain customized desktop configurations for many types of workers, including mobile users, information workers, or others assigned to strictly defined tasks, such as data entry. Changes to standard operating system images might be required on an ongoing basis. Security settings and updates must be delivered efficiently to all the computers and devices in the organization. New users need to be productive quickly without costly training. In the event of a computer failure or disaster, service must be restored with a minimum of data loss and interruption. Specifically, an IT department must respond to various factors that require change in an IT environment including:

- New operating systems and applications.
- Updates to operating systems and applications.
- New hardware.
- New business requirements that require configuration changes.
- Security influences that require configuration changes.
- New users.

Managing user and computer behavior in large distributed computer environments requires the ability to implement configuration changes from a central location and also to provide an effective way to define policy that affects large numbers of users and computers.

Group Policy provides the infrastructure used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers within an Active Directory environment. Policy settings are administrative directives that define the behavior of the computers and users in a domain. Administrators can define policy settings once and rely on the Windows operating system to enforce that policy. Policy settings are specified by an administrator. This is in contrast to profile settings, which are specified by a user.

3.1.1 Policy Settings

There are two classes of policy settings:

User Policy Settings - Specify behaviors for interactively logged-on users. These settings can affect different users who are logged on to the same computer. Additionally, some settings will affect the user regardless of which computer the user logs on to; this depends on the policy source mode, as defined in section 3.2.1.3 in [MS-GPOL]. Examples of such settings include the user's default location for saving documents, or the desktop background image for a user.

Computer Policy Settings - Specify behaviors for either a computer (even when no users are logged on to the computer), or settings that globally affect every user who logs on to the computer. Examples include settings that enable a computer to host a web server, that schedule automated disk backups of the computer, or that specify a standard web home page for all users of the computer.

3.1.2 Group Policy Objects

The Group Policy System includes the protocols that are used to read and update Group Policy Objects (GPOs). Group Policy uses a document-centric approach to create, store, and associate policy settings. Group Policy settings are contained in GPOs. A GPO is a virtual object; policy-setting information is stored in two locations: the Active Directory container to which the GPO is linked, and the system volume (SYSVOL) on the domain controller. With Active Directory, GPOs can be linked to sites, domains, and organizational units (OUs), allowing policy settings to be applied to users and computers. This infrastructure provides a high degree of flexibility, enabling the administrator to customize configurations, such as delivering a specific piece of software to specialized users based on their membership in an OU.

A GPO has a unique name, which is a **globally unique identifier (GUID)** in the form of a **curly braced GUID string**. Group Policy settings are contained in a GPO. A GPO can represent policy settings in the file system and in the Active Directory. GPO settings are evaluated by GP Clients using the hierarchical nature of Active Directory.

By default, two Group Policy Objects with known GUID values are defined as part of a domain. The "Default Domain Policy" GPO is linked to the Active Directory domain object and contains settings applicable to all computers and users in the domain, and the "Default Domain Controllers Policy" GPO is linked to the "Domain Controllers" GPO OU and contains settings applicable to computers functioning as domain controllers. The settings in both Group Policy Objects may be changed by domain administrators. Both Group Policy Objects are preloaded with initial security settings in the machine portion of the GPO. Refer to Group Policy: Security Protocol Extension ([MS-GPSB]) for the format of the security settings files and the meaning of each setting.

"Default Domain Policy" known GUID: {31B2F340-016D-11D2-945F-00C04FB984F9}

```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 42
MinimumPasswordLength = 7
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
[Kerberos Policy]
MaxTicketAge = 10
MaxRenewAge = 7
MaxServiceAge = 600
MaxClockSkew = 5
TicketValidateClient = 1
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Lsa\NoLMHash=4,1
[Version]
signature="$CHICAGO$"
Revision=1
```

"Default Domain Controllers Policy" known GUID: {6AC1786C-016F-11D2-945F-00C04fB984F9}

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Registry Values]
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,
1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,1
[Privilege Rights]
SeAssignPrimaryTokenPrivilege = *S-1-5-19,*S-1-5-20
SeAuditPrivilege = *S-1-5-19,*S-1-5-20
SeBackupPrivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-549
SeBatchLogonRight = *S-1-5-32-568,*S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-559
SeChangeNotifyPrivilege = *S-1-1-0,*S-1-5-19,*S-1-5-20,*S-1-5-32-544,*S-1-5-11,*S-1-5-32-554
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-19,*S-1-5-20,*S-1-5-32-544
SeInteractiveLogonRight = *S-1-5-32-548,*S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-550,*S-1-5-32-
549
SeLoadDriverPrivilege = *S-1-5-32-544,*S-1-5-32-550
SeMachineAccountPrivilege = *S-1-5-11
SeNetworkLogonRight = *S-1-1-0,*S-1-5-32-544,*S-1-5-11,*S-1-5-9,*S-1-5-32-554
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-544,*S-1-5-32-549
SeRestorePrivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-549
SeSecurityPrivilege = *S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-544,*S-1-5-32-551,*S-1-5-32-549,*S-1-5-32-550
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-32-544
SeSystemTimePrivilege = *S-1-5-19,*S-1-5-32-544,*S-1-5-32-549
SeTakeOwnershipPrivilege = *S-1-5-32-544
SeUndockPrivilege = *S-1-5-32-544
SeEnableDelegationPrivilege = *S-1-5-32-544
SeRemoteInteractiveLogonRight = *S-1-5-32-544
```

3.1.3 Group Policy Extensions

The GP System can be extended through client-side extensions and administrative tool extensions. The GP system supports GP **Client plug-ins** for policy application of specific client functionality, such as the client security policies specified in [MS-GPSB], and administrative tool plug-ins for authoring administrative-specific settings, such as the registry-based settings specified in [MS-GPREG].

Client-side extensions are used for implementing application-specific policy settings on the client computer. These client-side extension protocols depend on the Group Policy: Core Protocol on the GP Client to execute first and to identify Group Policy Objects (GPOs) that the extension should query or update.

GPOs with settings for a particular extension are identified with a **tool extension GUID** in the form of a curly braced GUID string to enable administrative tools to identify a plug-in that is capable of administering the settings. Such extensions (for example, as specified in [MS-GPSB]) typically use

Lightweight Directory Access Protocol (LDAP) to store settings in Active Directory, or they use **Server Message Block (SMB)** to store files in the SYSVOL.

Policy settings for a given class of functionality are communicated by the extension protocol and not directly by the Group Policy: Core Protocol. The behavior of a given protocol extension is specific to each extension and is specified in the documentation of that extension protocol. For example, the Group Policy: Registry Extension Encoding extensions behave according to what is documented in [MS-GPREG].

3.1.3.1 Group Policy Client-Side Extension List

The following table lists the Group Policy Extension protocols with client-side extensions.

Client-side Extension GUID	Name	Reference
{F3CCC681-B74C-4060-9F26-CD84525DCA2A}	Audit Policy Configuration	[MS-GPAC]
{8A28E2C5-8D06-49A4-A08C-632DAA493E17}	Deployed Printer Connections	[MS-GPDPC]
{3610EDA5-77EF-11D2-8DC5-00C04FA31A66}	Disk Quota	DiskQuota.admx
{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}	Encrypting File System	[MS-GPEF]
{25537BA6-77A8-11D2-9B6C-0000F8080861}	Folder Redirection	[MS-GPFR]
{A2E30F80-D7DE-11D2-BBDE-00C04F86AE3B}	Internet Explorer Branding	[MS-GPIE]
{E437BC1C-AA7D-11D2-A382-00C04F991E27}	IP Security	[MS-GPIPSEC]
{C631DF4C-088F-4156-B058-4375F0853CD8}	Offline Files	OfflineFiles.admx
{426031C0-0B47-4852-B0CA-AC3D37BFCB39}	QoS Packet Scheduler	QOS.admx
{35378EAC-683F-11D2-A89A-00C04FBBCFA2}	Registry	[MS-GPREG]
{4BCD6CDE-777B-48B6-9804-43568E23545D}	Remote Desktop USB Redirection	TerminalServer.admx
{42B5FAAE-6536-11D2-AE5A-0000F87571E3}	Scripts	[MS-GPSCR]
{7933F41E-56F8-41D6-A31C-4148A711EE93}	Search	Search.admx
{827D319E-6EAC-11D2-A4EA-00C04F79F83A}	Security	[MS-GPSB]
{C6DC5466-785A-11D2-84D0-00C04FB169F7}	Software Installation	[MS-GPSI]

Client-side Extension GUID	Name	Reference
{B587E2B1-4D59-4E7E-AED9-22B9DF11D053}	Wired Networking	[MS-GPWL]
{0ACDD40C-75AC-47AB-BAA0-BF6DE7E7FE63}	WirelessNetworking	[MS-GPWL]
{F9C77450-3A41-477E-9310-9ACD617BD9E3}	Preferences:Applications	[MS-GPPREF]
{728EE579-943C-4519-9EF7-AB56765798ED}	Preferences:Data Sources	[MS-GPPREF]
{1A6364EB-776B-4120-ADE1-B63A406A76B5}	Preferences:Devices	[MS-GPPREF]
{5794DAFD-BE60-433F-88A2-1A31939AC01F}	Preferences:Drives	[MS-GPPREF]
{0E28E245-9368-4853-AD84-6DA3BA35BB75}	Preferences:Environment Variables	[MS-GPPREF]
{7150F9BF-48AD-4DA4-A49C-29EF4A8369BA}	Preferences:Files	[MS-GPPREF]
{A3F3E39B-5D83-4940-B954-28315B82F0A8}	Preferences:Folder Options	[MS-GPPREF]
{6232C319-91AC-4931-9385-E70C2B099F0E}	Preferences:Folders	[MS-GPPREF]
{74EE6C03-5363-4554-B161-627540339CAB}	Preferences:Ini Files	[MS-GPPREF]
{E47248BA-94CC-49C4-BBB5-9EB7F05183D0}	Preferences:Internet Settings	[MS-GPPREF]
{17D89FEC-5C44-4972-B12D-241CAEF74509}	Preferences:Local users and groups	[MS-GPPREF]
{3A0DBA37-F8B2-4356-83DE-3E90BD5C261F}	Preferences:Network Options	[MS-GPPREF]
{6A4C88C6-C502-4F74-8F60-2CB23EDC24E2}	Preferences:Network Shares	[MS-GPPREF]
{E62688F0-25FD-4C90-BFF5-F508B9D2E31F}	Preferences:Power Options	[MS-GPPREF]
{BC75B1ED-5833-4858-9BB8-CBF0B166DF9D}	Preferences:Printers	[MS-GPPREF]
{E5094040-C46C-4115-B030-04FB2E545B00}	Preferences:Regional Options	[MS-GPPREF]
{B087BE9D-ED37-454F-AF9C-04291E351182}	Preferences:Registry	[MS-GPPREF]
{AADCED64-746C-4633-A97C-	Preferences:Scheduled Tasks	[MS-GPPREF]

Client-side Extension GUID	Name	Reference
D61349046527}		
{91FBB303-0CD5-4055-BF42-E512A681B325}	Preferences:Services	[MS-GPPREF]
{C418DD9D-0D14-4EFB-8FBF-CFE535C8FAC7}	Preferences:Shortcuts	[MS-GPPREF]
{E4F48E54-F38D-4884-BFB9-D4D2E5729C18}	Preferences:Start Menu	[MS-GPPREF]

3.1.3.2 Group Policy Tool Extension List

The following table lists the Group Policy Extension protocols with tool extensions.

Tool Extension GUID	Name	Reference
{0F3F3735-573D-9804-99E4-AB2A69BA5FD4}	Audit Policy Configuration	[MS-GPAC]
{180F39F3-CF17-4C68-8410-94B71452A22D}	Deployed Printer Connections	[MS-GPDPC]
{53D6AB1B-2488-11D1-A28C-00C04FB94F17}	Encrypting File System	[MS-GPEF]
{B05566AC-FE9C-4368-BE01-7A4CBB6CBA11}	Firewall and Advanced Security	[MS-GPFAS]
{88E729D6-BDC1-11D1-BD2A-00C04FB9603F}	Folder Redirection	[MS-GPFR]
{FC715823-C5FB-11D1-9EEF-00A0C90347FF}	Internet Explorer Branding	[MS-GPIE]
{DEA8AFA0-CC85-11D0-9CE2-0080C7221EBD}	IP Security	[MS-GPIPSEC]
{A2A54893-AAF2-49A3-B3F5-CC43CEBCC27C}	Network Access Protection	[MS-GPNAP]
{0F6B957E-509E-11D1-A7CC-0000F87571E3}	Registry (User Policy) <1>	[MS-GPREG]
{0F6B957D-509E-11D1-A7CC-0000F87571E3}	Registry (Computer Policy)	[MS-GPREG]
{D02B1F73-3407-48AE-BA88-E8213C6761F1}	Registry (User Policy) <2>	[MS-GPREG]
{D02B1F72-3407-48AE-BA88-E8213C6761F1}	Registry (Computer Policy)	[MS-GPREG]
{40B66650-4972-11D1-A7CA-0000F87571E3}	Scripts (User)	[MS-GPSCR]
{40B6664F-4972-11D1-A7CA-0000F87571E3}	Scripts (Computer)	[MS-GPSCR]
{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}	Security	[MS-GPSB]
{BACF5C8A-A3C7-11D1-A760-00C04FB9603F}	Software Installation (User)	[MS-GPSI]
{942A8E4F-A261-11D1-A760-00C04FB9603F}	Software Installation (Computer)	[MS-GPSI]
{06993B16-A5C7-47EB-B61C-B1CB7EE600AC}	Wired Networking	[MS-GPWL]
{2DA6AA7F-8C88-4194-A558-0D36E7FD3E64}	WirelessNetworking	[MS-GPWL]
{0DA274B5-EB93-47A7-AAFB-65BA532D3FE6}	Preferences:Applications	[MS-GPPREF]

Tool Extension GUID	Name	Reference
{1612B55C-243C-48DD-A449-FFC097B19776}	Preferences:Data Sources	[MS-GPPREF]
{1B767E9A-7BE4-4D35-85C1-2E174A7BA951}	Preferences:Devices	[MS-GPPREF]
{2EA1A81B-48E5-45E9-8BB7-A6E3AC170006}	Preferences:Drives	[MS-GPPREF]
{35141B6B-498A-4CC7-AD59-CEF93D89B2CE}	Preferences:Environment Variables	[MS-GPPREF]
{3BAE7E51-E3F4-41D0-853D-9BB9FD47605F}	Preferences:Files	[MS-GPPREF]
{3BFAE46A-7F3A-467B-8CEA-6AA34DC71F53}	Preferences:Folder Options	[MS-GPPREF]
{3EC4E9D3-714D-471F-88DC-4DD4471AAB47}	Preferences:Folders	[MS-GPPREF]
{516FC620-5D34-4B08-8165-6A06B623EDEB}	Preferences:Ini Files	[MS-GPPREF]
{5C935941-A954-4F7C-B507-885941ECE5C4}	Preferences:Internet Settings	[MS-GPPREF]
{79F92669-4224-476C-9C5C-6EFB4D87DF4A}	Preferences:Local users and groups	[MS-GPPREF]
{949FB894-E883-42C6-88C1-29169720E8CA}	Preferences:Network Options	[MS-GPPREF]
{BFCBBEB0-9DF4-4C0C-A728-434EA66A0373}	Preferences:Network Shares	[MS-GPPREF]
{9AD2BAFE-63B4-4883-A08C-C3C6196BCAFD}	Preferences:Power Options	[MS-GPPREF]
{A8C42CEA-CDB8-4388-97F4-5831F933DA84}	Preferences:Printers	[MS-GPPREF]
{B9CCA4DE-E2B9-4CBD-BF7D-11B6EBFBDDF7}	Preferences:Regional Options	[MS-GPPREF]
{BEE07A6A-EC9F-4659-B8C9-0B1937907C83}	Preferences:Registry	[MS-GPPREF]
{CAB54552-DEEA-4691-817E-ED4A4D1AFC72}	Preferences:Scheduled Tasks	[MS-GPPREF]
{CC5746A9-9B74-4BE5-AE2E-64379C86E0E4}	Preferences:Services	[MS-GPPREF]
{CEFFA6E2-E3BD-421B-852C-6F6A79A59BC1}	Preferences:Shortcuts	[MS-GPPREF]
{CF848D48-888D-4F45-B530-6A201E62A605}	Preferences:Start Menu	[MS-GPPREF]

3.2 System Purposes

System administrators are tasked to provide consistency among groups of computers and/or users, including things like OS versions, sets of applications, and general user experience. Group policy is a tool that's designed to allow these administrators to remotely ensure that groups of computers are in conformance with standards, and that certain users are provided with a consistent experience no matter which computer they are using.

The Group Policy Core Protocol is a client/server protocol that allows clients to discover and retrieve policy settings that administrators of a domain create. Policy settings are administrative directives that administrators make regarding the behavior of the clients. For example, an administrator might want to configure every computer in a certain group of computers to open a specific port in their firewall. That administrator can use Group Policy to state that directive, and it will eventually be communicated to the clients through the Group Policy Protocol. Various extensions to the core protocol are provided to allow for detailed control over different aspects of the client systems.

3.3 System Use Cases

3.3.1 Stakeholders and Interests Summary

Group Policy (GP) Administrator: The individual who configures the policies aligned to the needs of the organization. The GP Administrator is responsible for deciding how to configure policy settings so that they align to business needs. The primary interests of the GP administrator are:

- Ensure policy settings stored in the GP Server are protected from unauthorized use.
- To be able to target policy settings for users and computers at different levels of granularity. This is called scope of management (SOM).
- Management of policy settings can be delegated as specified in [MS-DISO].
- The ability to alter the default processing of policy settings.
- The ability to configure a large number of computers to execute administrator-specified code at computer start, computer shut-down, user log-on, and user log-off as specified in [MS-GPSCR].

GP Client: Client systems that use the Group Policy system to enforce conformity with the policies defined by the administrators. The primary interests of the GP client are:

- Retrieve policy content from the GP server.
- Ensure that the policy settings defined by the administrator are enforced on the client.

GP Server: A domain controller (DC) that holds a database of Group Policy Objects (GPOs) that other machines can retrieve. The primary interests of the GP Server are:

- Enable a GP Client to retrieve Group Policy information from the domain based on the group memberships of the domain accounts, as well as the domain account's location in the LDAP directory structure.
- Support the admin tool operations, such as creating, updating, and deleting Group Policy content.

Admin Tool: A tool used to administer policy settings. The primary interest of the **admin tool** is to enable administrators to create, update, and delete policy settings by reading and writing policy settings to and from a GPO stored in the GP server.

Developers: The individual who intends to implement a client-side extensions or an administrative tool snap-in of the Group Policy system. The primary interest of a developer is to design plug-in extensions that alter how Group Policy is applied or customizes policy settings for a specific purpose

Users: The individual who uses a Group Policy-enabled computer. The primary interest of a user is how his or her user experience is influenced both by policies that affect the computer that they are using, and by any user-specific policies that apply to them.

3.3.2 Supporting Actors and System Interests Summary

Domain Interactions System: The Domain Interactions System as specified in [MS-DISO] provides a common infrastructure to provide the following services to the GP System:

- Management services
- Identity, authentication, and authorization services

- Remote file services
- Locating a domain controller

Authentication System: The Authentication System as specified in [MS-AUTHSO] provides authentication services through NTLM or **Kerberos** to secure communications in the GP system and the authentication services that support the client to server communication within and outside the GP system.

Replication System: In a system with more than one Domain Controller, the File Replication Service, as specified in [MS-FRS1], provides replication services to ensure that the data stored in SYSVOL is consistent across all Domain Controllers.

3.3.3 Use Case Diagrams

There are two summary-level uses cases for the Group Policy System:

- Applying Group Policy
- Administering Group Policy

Applying Group Policy involves the following steps:

1. The client must locate the domain controller that hosts the GP Server and identify the policy settings or GPOs that have been assigned to the **policy target** user or the computer account. During this step, the association between the specific account and the GPOs is determined.
2. The client queries GPO attributes. During this step, the separate portions of the GPO stored in Active Directory and SYSVOL are assembled. Then a query is performed through LDAP to obtain detailed attributes for each of the GPOs that are associated with the policy target. These attributes describe details such as:
    - Precedence between GPOs to allow for resolution of conflicts between different GPOs (for example, if one GPO requests to set the background to green and another requests to set it to blue).
    - Filtering of GPOs by using security filters and WMI filters for narrowing the scope of a GPO so that it applies only to a single group, user, or computer.
    - Identification of classes of settings that are contained within a GPO.
    - Version information for GPOs.
    - Location of information for that GPO stored in SYSVOL.
3. The client retrieves policy settings. In this step, the client uses its computed list of GPOs that contain different classes of settings to invoke a protocol sequence that is specific to each class of settings called a Group Policy extension (for example, the Group Policy: Registry Extension Encoding, as specified in [MS-GPREG]).
4. The client applies policy settings.

Administering Group Policy involves the following steps:

1. The admin tool locates the server, as specified in [MS-GPOL] section 1.3.4.
2. The admin tool invokes extension plug-ins to retrieve policy settings from the Active Directory portion of GPO by using the LDAP and/or SYSVOL portion of GPO using SMB.

3. The administrator edits retrieved policy settings and/or creates new policy settings. Accordingly, the admin tool invokes extension plug-ins to save the policy settings to the Active Directory portion of GPO by using LDAP and/or SYSVOL portion of GPO using SMB. In the case of new settings, the aforementioned portions MAY be created by the extension plug-ins and/or the admin tool.

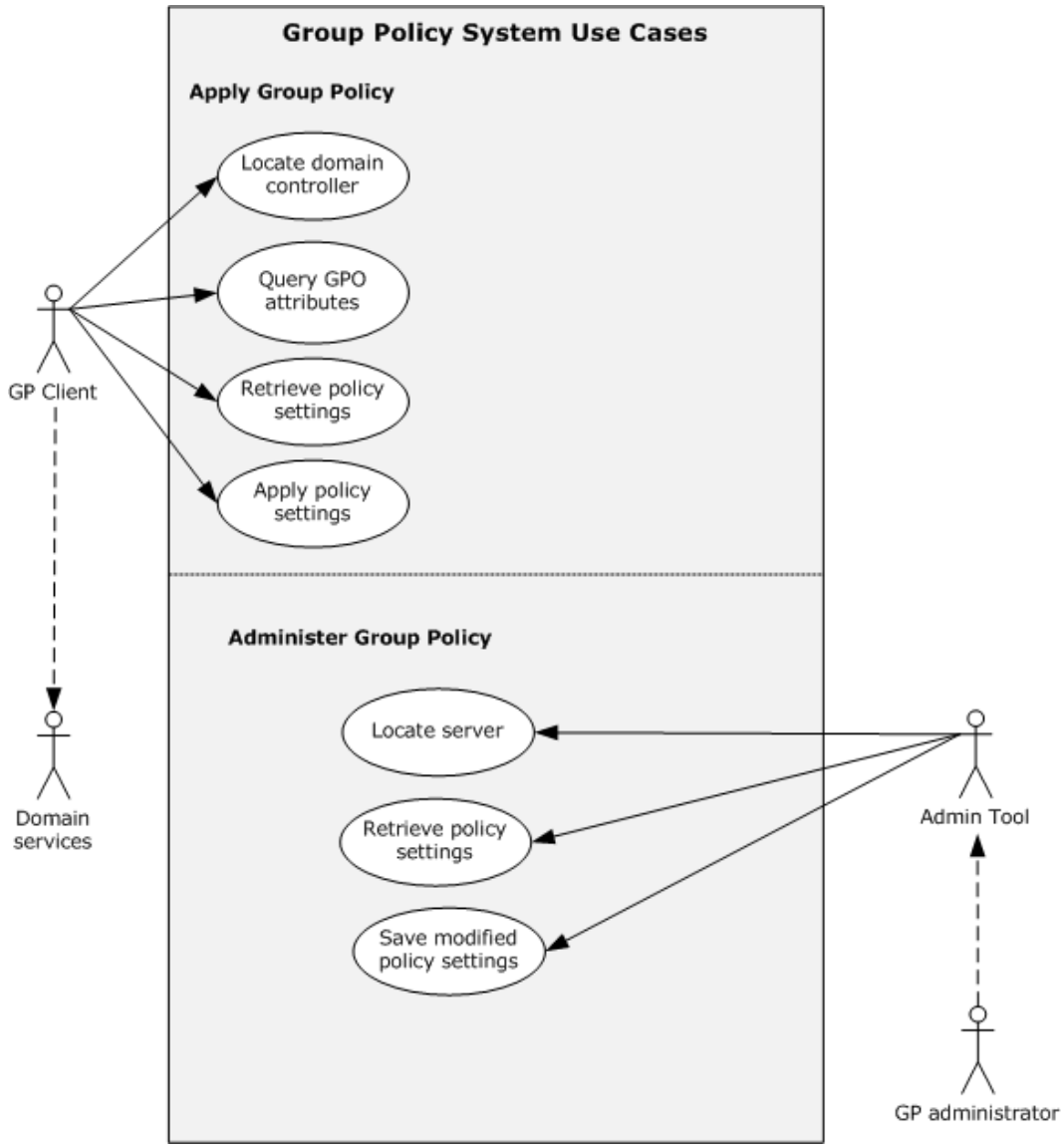

Figure 2: Group Policy System use case diagram

3.3.4 Use Case Descriptions

3.3.4.1 Apply Group Policy – GP Client

Goal: The goal of the use case is to retrieve policy content from the GP server and apply it on the GP client.

Context of use: The GP client contacts the GP server to retrieve new or updated content. Based on the scope of management, the client retrieves the list of GPOs to apply policy as described in section 3.2.5.1 in [MS-GPOL].

Direct Actor: The direct actor of this use case is the GP client.

Primary Actor: The primary actor is the same as the direct actor.

Supporting Actors: The supporting actors are domain services as described in [MS-DISO].

Stakeholders and Interests:

- GP client for maintaining a consistent configuration with the policy information stored on the GP server.
- GP server for storing policy and responding from requests from the GP client.
- GP administrator is interested in ensuring that the GP client is configured in way that aligns to business needs.

Preconditions:

- GP client must be able to access the GP server.

Minimal Guarantees:

If the main success scenario does not successfully finish, the GP system at least guarantees that:

- The GP Client does not modify the current configuration in case the policy application fails. In case of failure, an event is logged in the event log.
- The GP Client maintains the current configuration if the GP Client cannot connect to the GP Server or the GP Server does not respond.

Success Guarantee:

The Group Policy System guarantees that:

- The GP Client can maintain a consistent configuration with the policy information stored on the GP server.
- The GP server responds to requests from the GP client.
- The administrative intent is honored by the GP client.
- The GP server responds to GP client requests if the GP Server is operational and can be reached.
- Policy configuration on the client will be updated to match the administrator's defined configuration if there are no failures.

Trigger:

- The computer startup and user logon processes trigger this use case, as well as a periodic timer or network state change as described in sections 6.4 and 6.5.

Main Success Scenario:

1. When the trigger occurs, the GP Client connects to the GP Server.

2. GP Client queries for applicable policy from the GP Server.

3. GP Client retrieves the policy information based on the results from the query.

4. GP Client applies the policy.

Extensions:

- Based on WMI filters, the GP Client decides whether or not to apply a specific GPO.
- Based on the policy source, as described in section 3.2.1.3 in [MS-GPOL], the GP Client gets a set of GPOs that apply to that specific client.

3.3.4.2 Administer Policy – Admin Tool

Goal: The goal of the use case is to create, update, and delete Group Policy content.

Context of use: The administrator initiates the task defined in the goal for the Group Policy environment through the direct actor.

Direct Actor: The direct actor is the Group Policy admin tool.

Primary Actor: The primary actor is the **Group Policy administrator**.

Supporting Actors: The supporting actors are domain controllers as described in [MS-DISO].

Stakeholders and Interests:

- Admin tool is interested in ensuring it has read and write access to the GP server.
- GP administrator is interested in ensuring that the GP server is storing policy that aligns with business needs.

Preconditions:

- Admin tool must be able to access the GP server.
- The GP Server MUST be a Read/Write domain controller, not a read-only domain controller.

Minimal Guarantees:

If the main success scenario does not successfully finish, the GP system at least guarantees that:

- The admin tool does not modify the policy information stored on the GP server.
- The admin tool retrieves and displays the policy list, but does not modify the policy information stored on the GP server.

Success Guarantee:

- The Group Policy System guarantees that the admin tool can manipulate policy information stored on the GP server.
- The Group Policy System guarantees that the Group Policy administrator can apply policies that align to the business needs as expressed in the Group Policy System.
- The GP server stores the policy defined by the GP administrator.

Trigger:

- The Group Policy administrator launches the admin tool.

Main Success Scenario:

1. When the trigger occurs, the admin tool connects to the GP Server.
2. The admin tool queries for policy information from the GP Server.
3. The admin tool retrieves the policy list based on the results from the query.
4. The admin tool displays the policy list.
5. The Group Policy administrator updates, creates, or deletes policy information in the admin tool.
6. Updated information is written to the GP server.

Extensions:

- None.

4 System Context

This section describes the relationship between this system and its environment.

4.1 System Environment

Group Policy depends on a number of prerequisite factors for it to be configured, applied and utilized by client computers. There are core networking protocols and services that must be open, running and configured in order to correctly query and respond in order for policy to apply.

The network must be capable of supporting TCP/IP traffic such as DNS, LDAP and SMB communications to support the lookup, transport and transfer of services and policy data. Additionally the network must also support **Netlogon** (with Kerberos v5) authentication and authorization traffic. As part of this protocol access, any host based firewalls residing on the client and servers must have open TCP ports for each of these services to support Group Policy.

The Domain Naming Service (DNS) is required for GP Server service discovery and file server access discovery. It requires this server to look up service names to TCP/IP addresses.

A GP Server based on the Lightweight Directory Access Protocol version 3 (LDAPv3) is required to store Group Policy Object attributes. After discovering the location of the GP Server in DNS, the client will logon and use this server to discover and calculate which policies apply to it and where to find the necessary policy files for application. It also uses the GP Server to discover WMI filters that will determine whether a particular policy applies to that GP client.

A file server supporting SMB communications is used to store the policy files in a specific service location that the GP client must have full read access to in order to read the files. This is co-located on the GP Server and uses **DFS** to maintain distributed access to the policy files around the network to all the file servers providing access to this data.

The combination of the GP Server and file server services is known in this document as the GP Server.

4.2 System Assumptions and Preconditions

Preconditions for Group Policy: Core Protocol communications between a Client and Server are the following:

- The Server is assumed to be a Domain Controller (DC).
- The Client must be joined to the Server domain.
- For user policy mode, the Client must be joined to a domain for which the user domain has a bidirectional domain trust.
- All DCs in the domain must be configured to require signing of SMB traffic, as specified in [MS-SMB] section 3.2.4.2.4.
- All DCs in the domain must be configured to require signing of LDAP traffic, as specified in [RFC2251] section 4.2.2.

Preconditions on the client are:

- In order to process a policy that applies to a GP client, the client must be able to Read and Apply that policy to itself or the interactive user. Therefore it is important that **ACL's** are correctly configured to allow policy to be read.

4.3 System Relationships

This section describes the relationships between the system and external components, system dependencies, and other systems influenced by this system.

4.3.1 Black Box Relationship Diagram

Relationships within the GP system:

- **GP Server:** Comprises two co-located elements of Active Directory and the SYSVOL.
- **Active Directory:** Implementation-specific version of LDAP v3 directory service.
- **SYSVOL:** Implementation-specific version of a file system location on a File Server. This location and directory structure is shared with all GP clients.
- **GP Client:** The client service component; communicates using LDAP and SMB.
- **Admin Tool:** This is an implementation-specific tool to add, remove, edit, and manage the Group Policy settings specific to the client implementation.

External Relationships to the GP system:

- **DNS:** Used by both the GP Client and the Admin Tool to discover the location of the GP Server.
- **SMB:** Used by the Group Policy Protocol to read policy files from the File Server.
- **LDAP:** Used by the Group Policy Protocol to read policy attributes and WMI filters from the GP Server.
- **DFS:** Provides location-independent access to the Group Policy server for clients during policy application and policy administration.
- **MS-AUTHSO:** The Authentication System as specified in [MS-AUTHSO] provides authentication services through NTLM or Kerberos to secure communications in the GP system and the authentication services that support the client to server communication within and outside the GP system.
- **SMB:** Used to transmit Group Policy settings and instructions between the client and the Group Policy server.

The following figure depicts the Group Policy System and the components it interacts with.

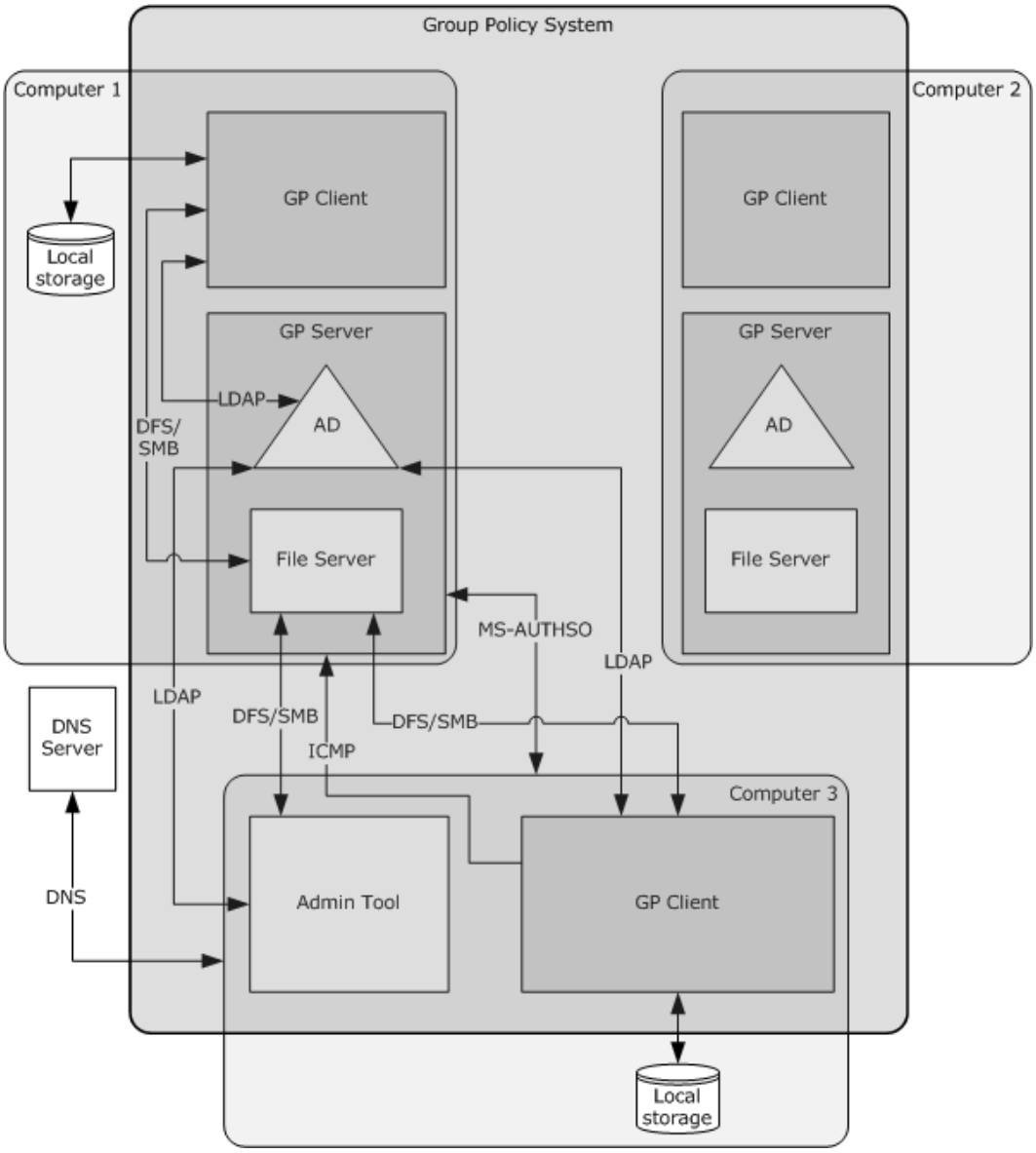

Figure 3: Black box relationship diagram

4.3.2 System Dependencies

The GP system requires physical network connectivity and correctly configured TCP/IP configuration on both the GP Server and the GP Client. There is no specific requirement for the type of physical networking topology.

In order to provide GP system service to GP clients, the GP Server must provide LDAP and SMB services as depicted in the Black box relationship diagram. The GP system also depends on a service for authentication, preferably via SPNEGO which can negotiate the choice between Kerberos v5 and NTLM. It relies on authentication and authorization through SPNEGO to assist in determining which policies apply to the computer and the user.

The connectivity from the GP Client to the GP Server should be continuous. Policies should be periodically refreshed with updates to existing policies as well as any new policies. The client should be able to tolerate network outages and refresh for policy changes once reconnected to the network<1>.

The GP client depends on an IP address of a correctly configured DNS server and the ability to connect and to be able to discover and resolve hostnames of GP Servers. It requires access to all the prerequisite GP Server services via TCP/IP and expects to access GP Server services via the TCP ports exposed by those services. Any host based firewalls on the GP Server must expose these ports. This includes services that expose SMB, LDAP, NTLM and Kerberos. The GP Client also depends on a place to store policy obtained from the GP Server<2>.

- To register the extension libraries that will process the settings in the policy files.
- To be able to persist the policies into user and machine configuration as this information is not stored in memory.

In complete reference to the protocol documentation for the exchange of information between a GP Client and a GP Server:

- For authentication, Simple and Protected Generic Security Service Application Program Interface Negotiation Mechanism (SPNEGO) Protocol Extensions, as specified in [MS-SPNG] and [MS-AUTHSO].
- For authentication, Kerberos Protocol Extensions, as specified in [MS-KILE] and [MS-AUTHSO].
- For authentication, NT LAN Manager (NTLM) Authentication Protocol, as specified in [MS-NLMP] and [MS-AUTHSO].
- DNS for discovering the Group Policy server.
- SMB Protocol, as specified in [MS-SMB], for transmitting Group Policy settings and instructions between the client and the Group Policy server.
- DFS: Referral Protocol, as specified in [MS-DFSC], to provide location-independent access to the Group Policy server for clients during policy application and policy administration.
- LDAP v3, as specified in [RFC2251], for transmitting Group Policy settings and instructions between the client and the Group Policy server.
- Windows Management Instrumentation Remote Protocol as specified in [MS-WMI], for Group Policy filtering. During preprocessing, the Group Policy service evaluates WMI filters to determine if a Group Policy Object is within scope of the computer or users. Failures with WMI can prevent Group Policy settings from applying as well as cause inaccurate reporting results.
- Internet Control Message Protocol (ICMP), as specified in [RFC792] MAY be used for Link Speed Determination.<3>

4.3.3 System Influences

The Group Policy System influences the configuration and change management in Windows. As such, it MAY influence the behavior of any application or service that runs on Windows and in particular it influences a large number of systems and protocols. The most salient examples of protocols and systems influenced by the Group Policy System are:

Active Directory System [MS-ADSO]: has a more in-depth description of how the directory is structured and how **LDAP** operations can be made. The Group Policy System depends on the Active

Directory System [MS-ADSO] for storing group policies in the directory service to enable Group Policy clients to discover and retrieve them.

Authentication System [MS-AUTHSO]: specifies how other protocols take advantage of the authentication protocols such as **NTLM** or Kerberos to secure their communications, and the authentication services that support the client to server communication. The Authentication System [MS-AUTHSO] depends on the Group Policy System for the user account for the domain logon. Depending on the policy configuration settings implemented, the Group Policy System influences the behavior of authentication tasks such as interactive domain logon, **HTTP** access authentication, SMB file system services authentication, and so on.

Certificate Autoenrollment System [MS-CAESO]: specifies how to enroll and renew computer certificates automatically. Configuration options of this task and information about CEP servers that this task can use are distributed through Group Policy when this task executes on the computer that is a domain member. This task SHOULD rely on a separate Group Policy Client (GP Client), as specified in [MS-GPSO], to retrieve configuration options needed for this task; however, such architectural design is not required and an implementation of this task MAY read required Group Policy data as part of this task processing by using the Registry Extension Encoding protocol, as specified in [MS-GPREG].

Domain Interaction Systems [MS-DISO]: specifies how systems and computers function within a Windows domain environment. The Group Policy System specifies how domain clients can retrieve group policy information from the domain controller (DC), which is based on the group memberships of the domain accounts, as well as the domain account's location in the LDAP directory structure.

File Access Services System [MS-FSSO]: specifies how file servers present a unified view of files and other resources, and rely upon the Authentication System [MS-AUTHSO] and Domain Interaction Systems [MS-DISO] for authentication when the file server is part of a domain. The File Access Services System [MS-FSSO] depends on the Group Policy System for the configuration of individual protocol capabilities within the File Access Services System [MS-FSSO]. Without the Group Policy System, the File Access Services System [MS-FSSO] cannot be centrally configured and managed.

Print Services System [MS-PSSO]: specifies how print servers can render content, and rely upon the Domain Interaction Systems [MS-DISO] for receiving authorization information about print operations when the print server is part of a domain.

Network Policy and Access Services System [MS-NAPSO]: specifies how machines can be examined for access to a network. The machines have to be members of a domain in order to authenticate to the **NAP** servers. The Group Policy System triggers and MAY affect the behavior of Network Policy and Access Services [MS-NAPSO] tasks such as creating a **statement of health (SoH)**.

Terminal Services System [MS-TSSO]: The Terminal Services System provides functionality for securely connecting remote clients and servers, for channeling communication between components of remote clients and servers, and for managing servers. The Group Policy System can alter capabilities of the remote experience in the Terminal Services System [MS-TSSO] through user-specific policies. A profile server that stores user-specific profiles (mandatory and roaming) can alter the capabilities of the remote experience. System Center for Virtual Machine Management (SCVMM) is used for desktop image management in a large Remote Desktop Virtualization environment. Internet Access Gateway (IAG) influences the TS Gateway in restricting what an **RDP** client can access.

Windows Management Services System [MS-WMSO]: specifies the set of protocols used to manage servers remotely. The Group Policy system enables the implementation of protocol-specific configuration settings, as specified in [MS-WMSO].

Windows Server Update Services System [MS-WSUSO]: specifies how different machines in a domain can have different update policies for patch management, which relies upon the Domain Interaction Systems [MS-DISO] to specify the domain authorization information. The Group Policy System is used by the Windows Server Update Services System [MS-WSUSO] to administer the WUSP client.

Group Policy Extensions: Group Policy is designed to be extended. Microsoft has implemented several extensions which depend on the Group Policy System to implement the specific configuration supported by a given Group Policy extension.

4.4 System Applicability

The Group Policy System is primarily applicable in scenarios where centralized administration of users and computers is desired. Other protocol systems that require centralized administration of policy settings for users and computers within an Active Directory environments rely on the Group Policy System.

4.5 System Versioning and Capability Negotiation

The Group Policy System is a collection of protocols each with its own system versioning and capability negotiation. The Group Policy System itself does not provide capability negotiation but relies on the member protocols to perform this action.

The Group Policy System relies on the Group Policy Core Protocol for the transport of policy information. It provides a versioning capability in an attribute of the Active Directory object class for a Group Policy Object (GPO) specified in section 2.2 of [MS-GPOL]. The version itself is a simple integer and is also written to a file on the fileserver as described in section 2.2.4 of [MS-GPOL]. There is only one version currently, and if the Client receives anything other than that version for a GPO, the GPO does not participate in this protocol, as specified in [MS-GPOL] section 3.2.5.1.5.

The System Versioning and Capability Negotiation implementation of the extension protocol specifications are documented in the respective protocol documents. These are specified in the "Versioning and Capability Negotiation" of section 1.7 in the respective technical documents (TDs).

4.6 System Vendor-Extensible Fields

The Group Policy Systemis a collection of protocols that can be extended by extending the GP Client or the administrative tools, and by adding extensions. Each of these extensions themselves can also potentially be extended. See sections 1.8 and 2.2 of [MS-GPOL] for more information about implementing extensions on the Client. To extend the administrative tool, the tool must understand the abstract data model, as specified in section 3.3.1 of [MS-GPOL].

The system Vendor-Extensible Fields of each extension protocol specification are documented in the respective protocol documents. These are specified in section 1.8 Vendor-Extensible Fields in the respective technical documents (TDs).

5 System Architecture

This section describes the basic structure of the system and the interrelationships among its parts, consumers, and dependencies.

The Group Policy Protocol enables clients to discover and retrieve policy settings that are created by domain administrators. Policy settings are administrative directives that administrators establish regarding the behavior of the clients. These policy settings fall into two classes: user policy settings and computer policy settings.

When policy is applied for a user it depends on the policy source mode, as defined in [MS-GPOL] section 3.2.1.3.

Group Policy has an extensible architecture and primarily consists of the Group Policy Core Protocol and the protocol extensions such as Group Policy: Software Installation Protocol Extension [MS-GPSI]. The core protocol provides the functionality of determining the policies that apply to a client, whereas extension, based on the policies determined by the Group Policy Core Protocol, is responsible for actual application of policies. The Group Policy Core Protocol does not effect the actual change on the clients, it is the extensions that effect changes.

The behavior of a given protocol extension is specific to each extension and is specified in the documentation of that extension. A failure in any protocol extension sequence does not cause the policy application to fail. Failure simply means that Clients are not able to enforce settings that are associated with that specific extension. This section describes the various events that trigger Group Policy System Processing; for example, when a machine starts up, a user logs on to the machine, a user logs off, or a machine shuts down.

Group Policy Computer Startup, Computer Shutdown, User Logon and Logoff scripts provide additional configuration opportunities to an administrator, as described in section 6.1.1. These scripts can be stored on any server **share**, which may or may not be located on a GP Server. This server share must be accessible by the user or by the computer.

5.1 Abstract Data Model

This abstract data model is based on the conceptual model that is specified in [MS-GPOL] sections 3.1, 3.2, and 3.3. These different components are shown in the figure in section 5.2 and are described in the following sections.

The data model has three distinct perspectives, as described in the sections below.

5.1.1 Server Abstract Data Model

The GP server has no knowledge of the Group Policy Protocols. It is merely an LDAP and SMB server that stores generic objects. The GP server primarily stores information on managed objects and policies that must affect those objects. The GP Server merely provides LDAP and SMB services so that GP Clients and the administrative tools can locate and access GPOs as described in section 3.1 of [MS-GPOL].

5.1.2 Client Abstract Data Model

The abstract data model (ADM) is a union of the ADMs that are defined in Group Policy System Protocols, which are defined in the table in section 5.3.1.

The Group Policy: Core Protocol passes the applicable GPO list (described in [MS-GPOL] section 2.2.7) to each Client Side extension protocol mentioned in the table in section 5.3.1. The Client Side extension protocol then processes the GPO List as specified in each Client Side extension protocol.

PolicyChange: A local event that indicates that the policy has changed.

5.1.3 Administrative Tool Abstract Data Model

The abstract data model (ADM) is a union of the ADMs that are defined in Group Policy System Protocols, which are defined in the table in section 5.3.1.

5.2 White Box Relationships

These diagrams show the white box relationships within the GP system:

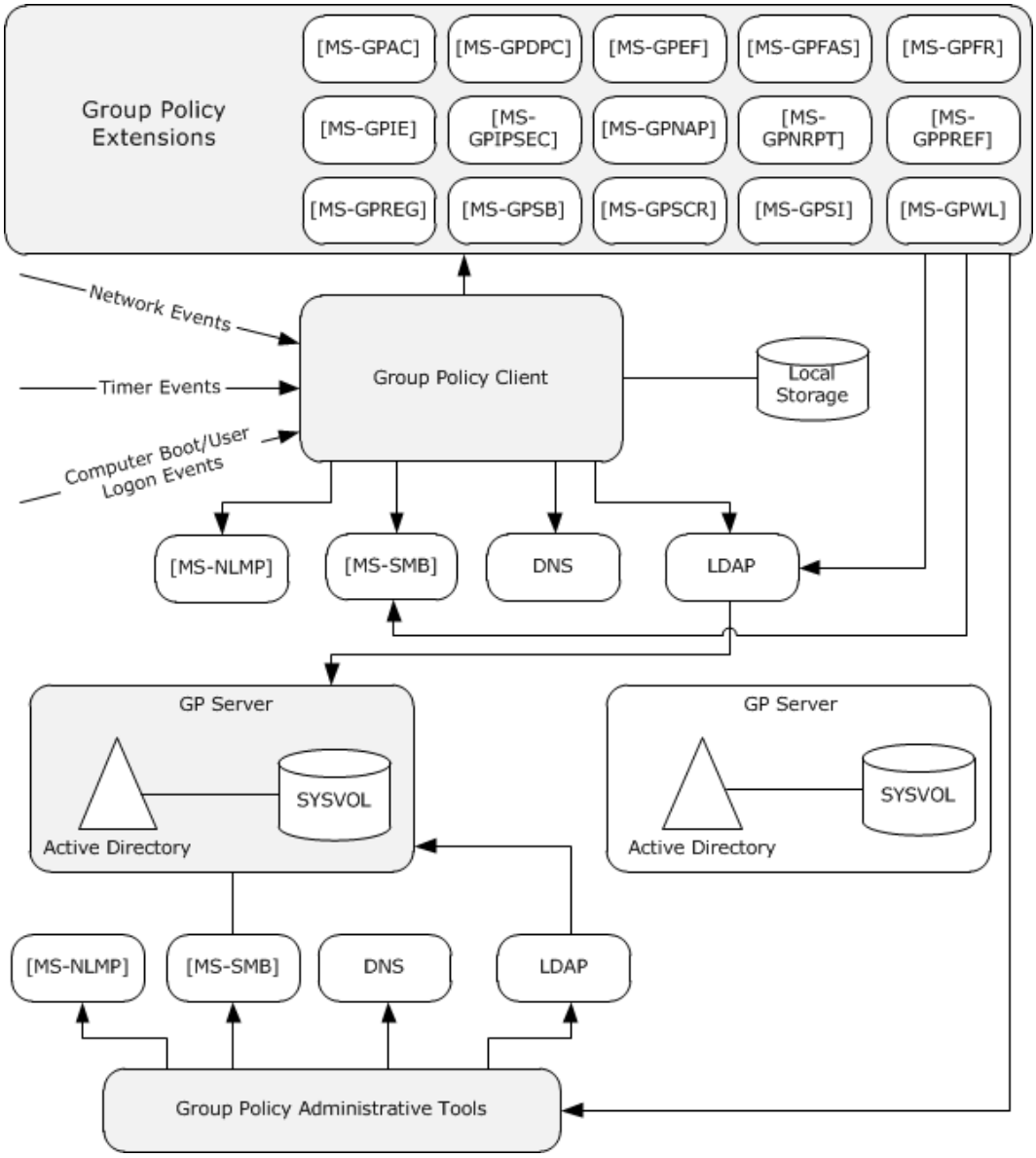

Figure 4: White box relationships

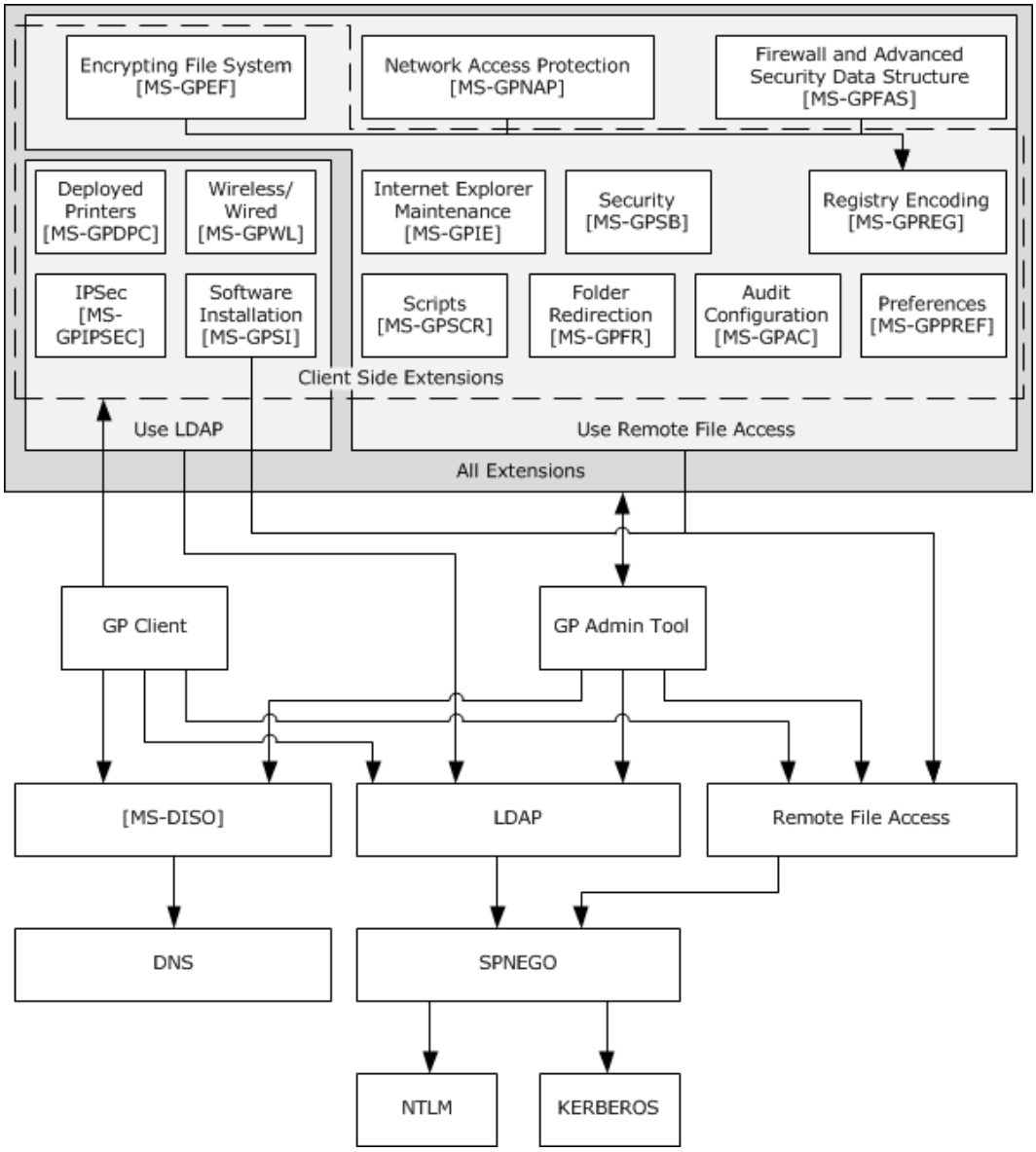

Figure 5: Protocol layering relationships

5.3 Member Protocol Functional Relationships

5.3.1 Member Protocol Roles

The following table lists the protocols that constitute the Group Policy System Protocols. These include the GP Core Protocol and the Client Side Extensions and Administrative Tools Extensions protocol.

Group Policy System protocols

Protocol name	Protocol description	Document short name
Group Policy: Audit Configuration Extension	Enables an administrator to control advanced audit policies on clients.	[MS-GPAC]
Group Policy: Core Protocol	The Microsoft protocol that communicates administrator-defined policies between a client and a domain controller (DC).	[MS-GPOL]
Group Policy: Deployed Printer Connections Extension	Supports managing connections to printers that are hosted by print servers and shared by multiple users.	[MS-GPDPC]
Group Policy: Encrypting File System Extension	Uses Group Policy: Core Protocol Specification, to enable remote administrative configuration of the Encrypting File System (EFS).	[MS-GPEF]
Group Policy: Firewall and Advanced Security Data Structure	Enables an administrator to control any Firewall and Advanced Security behavior on a client by using group policy-based settings.	[MS-GPFAS]
Group Policy: Folder Redirection Protocol Extension	Enables an administrator to relocate certain file system folders, called user profile folders, to different paths, such as a shared network location.	[MS-GPFR]
Group Policy: Internet Explorer Maintenance Extension	Enables an administrator to manage Internet Explorer configuration settings.	[MS-GPIE]
Group Policy: IPsec Protocol Extension	Enables centralized (common) configuration of the IPsec component on multiple client systems to provide basic traffic filtering, data integrity, and optionally, data encryption, for IP traffic.	[MS-GPIPSEC]
Group Policy: Network Access Protection (NAP) Extension	Enables an administrator to control client computer access to network resources.	[MS-GPNAP]
Group Policy: Name Resolution Policy Table (NRPT) Data Extension	Enables an administrator to control any name resolution policy behavior on a client by using group policy-based settings.	[MS-GPNRPT]
Group Policy: Preferences Extension Data Structure	Provides a mechanism for an administrator to manage and deploy preferences.	[MS-GPPREF]
Group Policy: Registry Extension Encoding	Provides a mechanism for an administrator to control any behavior on a client that depends on registry-based settings.	[MS-GPREG]
Group Policy: Security Protocol Extension	Enables security policies to be distributed to multiple client systems so that these systems can enact the policies in accordance with the intentions of the administrator.	[MS-GPSB]

Protocol name	Protocol description	Document short name
Group Policy: Scripts Extension Encoding	Provides a mechanism for an administrator to instruct an arbitrary group of clients to execute administrator-specified code at computer start, computer shut-down, user logon, and user logoff. The code executed by clients is in the form of a command-line tool or batch-processing script that is present either on the client's local file system or at a network file system location.	[MS-GPSCR]
Group Policy: Software Installation Protocol Extension	Enables an administrator to install and remove software applications at client computers. New software versions can also be pushed out to client computers.	[MS-GPSI]
Group Policy: Wireless/Wired Protocol Extension	The administrative-side plug-in extension specifies and edits wireless or wired policy settings through a user interface, and uses LDAP to store the settings to a specific location in a logical structure known as the Group Policy Object. The client-side plug-in uses LDAP to retrieve the wireless or wired policy settings from the specified location, and then applies these settings to the client.	[MS-GPWL]

5.3.2 Member Protocol Groups

This section describes the member protocol groups that are used together accomplish a conceptually separate subgoal of the system.

Details on about which external entities interact with the system by using these protocols, and specific interaction details, are provided in section 5.4. Group Policy System can be broken into two main groups: the core Group Policy Protocol, and the Group policy extensions protocol groups.

5.3.2.1 Group Policy Core Protocol Group

The Group Policy Core Protocol ([MS-GPOL]) is a client/server protocol that allows clients to discover and retrieve GPOs that administrators of a domain create. In the Policy application mode, the core protocol is responsible for discovering the GP server and getting the list of GPOs that are ultimately applicable to the computer or user. The GPOs contains the policy settings that are applied by the respective extensions for that group of settings. The Core GP protocol itself has no knowledge of the internal details of specific extensions or the settings that it applies.

In the Policy administration mode the Core Protocol supports extension plug-ins to the administrative tool for authoring extension-specific settings. GPOs with settings for a particular extension are identified with a tool extension GUID to enable administrative tools to identify a plug-in that is capable of administering the settings.

The Group Policy Core Protocol is required for group policy processing to be successful.

5.3.2.2 Group Policy Extension Protocol Group

The Group Policy Extension Protocol Group consists of the following protocols, all of which work together with the Group Policy Core Protocol [MS-GPOL]).

Document Short Name	Protocol Name
[MS-GPAC]	Group Policy: Audit Configuration Extension

Document Short Name	Protocol Name
[MS-GPDPC]	Group Policy: Deployed Printer Connections Extension
[MS-GPEF]	Group Policy: Encrypting File System Extension
[MS-GPFAS]	Group Policy: Firewall and Advanced Security Data Structure
[MS-GPFR]	Group Policy: Folder Redirection Protocol Extension
[MS-GPIE]	Group Policy: Internet Explorer Maintenance Extension
[MS-GPIPSEC]	Group Policy: IP Security (IPsec) Protocol Extension
[MS-GPNAP]	Group Policy: Network Access Protection (NAP) Extension
[MS-GPNRPT]	Group Policy: Name Resolution Policy Table (NRPT) Data Extension
[MS-GPPREF]	Group Policy: Preferences Extension Data Structure
[MS-GPREG]	Group Policy: Registry Extension Encoding
[MS-GPSB]	Group Policy: Security Protocol Extension
[MS-GPSCR]	Group Policy: Scripts Extension Encoding
[MS-GPSI]	Group Policy: Software Installation Protocol Extension
[MS-GPWL]	Group Policy: Wireless/Wired Protocol Extension

In addition, these protocols use Group Policy: Registry Extension Encoding, as specified in [MS-GPREG] to handle some or all of their settings.

Document Short Name	Protocol Name
[MS-GPEF]	Group Policy: Encrypting File System Extension
[MS-GPFAS]	Group Policy: Firewall and Advanced Security Data Structure
[MS-GPNAP]	Group Policy: Network Access Protection (NAP) Extension

All of these protocols use the Group Policy: Registry Extension Encoding ([MS-GPREG]) client-side extension to place their settings in the registry.

Group Policy: Encrypting File System Extension, as specified in [MS-GPEF], has a client-side extension that consumes its registry settings and makes local calls using those settings.

Group Policy: Firewall and Advanced Security Data Structure ([MS-GPFAS]) and Group Policy: Network Access Protection (NAP) Extension ([MS-GPNAP]) do not have client-side extensions. The Firewall and Advanced Security and Network Access Protection features of Windows consume the registry settings directly.

In policy application mode, the Group Policy Core Protocol identifies the GPOs that apply to the client, identifies the Group Policy extensions configured in those GPOs, and then invokes the configured extensions. The Group Policy extensions use their protocols to read application-specific policy settings from those GPOs, and apply the settings to the client. The settings can either be stored in Active Directory or in the file system SYSVOL share.

If an extension is not present or Policy settings related to the extension are not present then that specific extension is ignored by the GP Core Protocol. An extension is not required to be present for the Group Policy System to function.

In policy administration mode, the Group Policy Core Protocol ([MS-GPOL]) invokes extensions when an administrator adds, updates or deletes that extension's settings to a GPO. As described above, the protocols defined in [MS-GPEF], [MS-GPFAS] and [MS-GPNAP] invoke the protocol defined in [MS-GPREG] to store their settings.

5.4 System Internal Architecture

This section describes the flow of communication within the system components described in section 4.3.1. The following diagram depicts the main flow of communication.

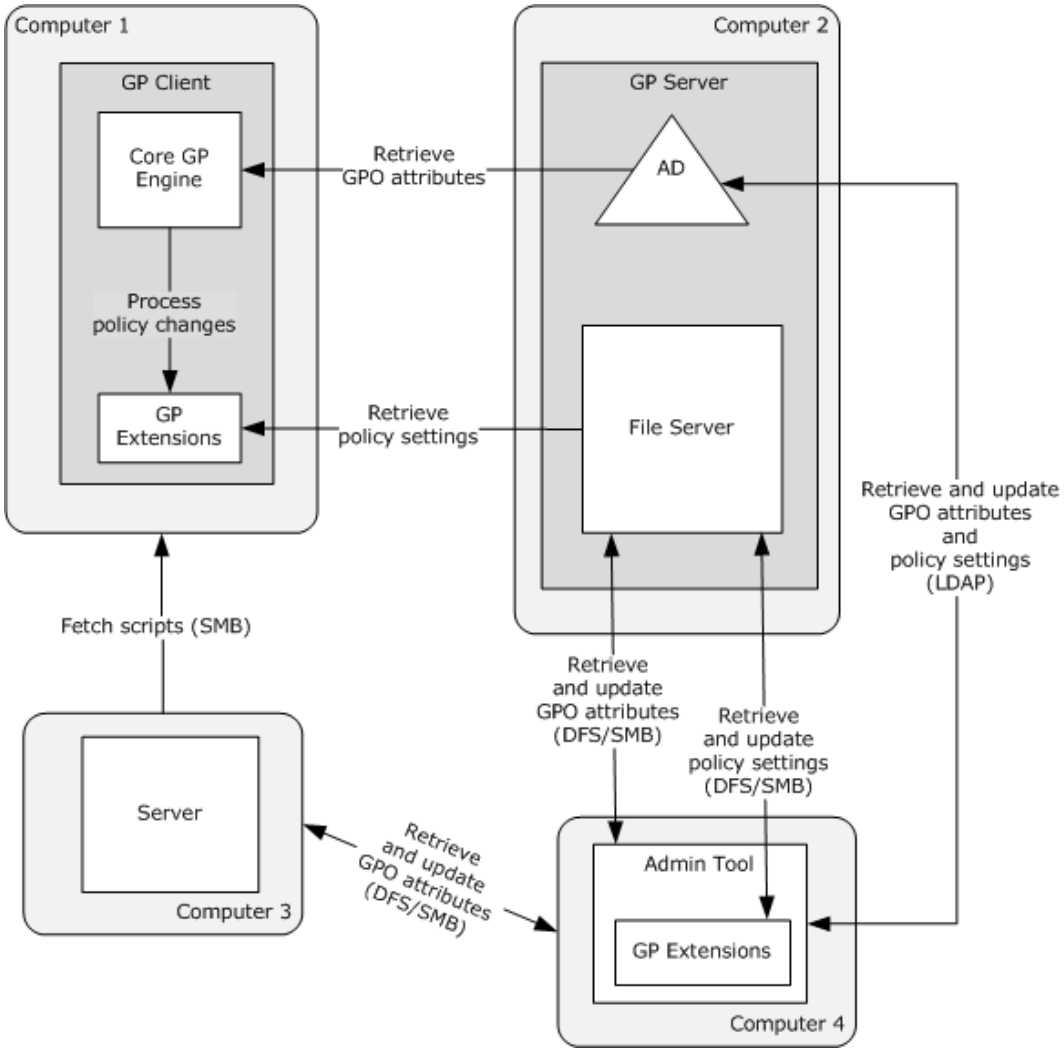

Figure 6: System internal architecture

5.4.1 Group Policy Server (GP Server)

The GP Server has no knowledge of the Group Policy. It is merely an LDAP and SMB server that stores generic objects. The GP Server primarily stores information on managed objects and policies that affect those objects. The GP Server keeps state in two stores: an LDAP server and a domain-based distributed file system (DFS) that is accessible through SMB. The details of these stores are described in section 3.1 of [MS-GPOL]. The changes to these stores happen as a result of Group Policy Administrative tools making changes to these stores. These stores are used a read-only store for the clients applying the policies.

5.4.2 Group Policy Client (GP Client)

The GP Client is composed of the Core Group Policy Engine described in [MS-GPOL] and also of the client side extension that extends Core Group Policy. The GP Client Side Extension that extends the Core GP is outlined in section 2.2 under Group Policy System Protocols.

Group Policy Core also provides the framework that manages the common functionalities across the client side extensions. It handles:

- Scheduling of Group Policy Processing, described in detail in sections 6.4 and 6.5.
- Getting the Group Policy Objects from the relevant configuration locations from Active Directory (AD) and SYSVOL.
- Handling special cases that affect all client-side extensions, such loopback mode (described in section 3.2.1.3 in [MS-GPOL]).
- Filtering and ordering Group Policy Objects appropriately (described in [MS-GPOL] sections 3.2.5.1.6 and 3.2.5.1.7).
- Maintaining version numbers and histories for all client-side extensions.
- Invoking the Client Side Extension providing a list of applicable GPOs (described in [MS-GPOL] section 3.2.5.1.10). The behavior of a given protocol extension is specific to each extension and is specified in the documentation of that extension.
- When the policy processing is completed, the Core Engine is responsible for notifying various components of any changes made by Group Policy.

The flow of communication is as follows:

1. The GP client locates the DC by following the steps as specified in [MS-DISO] section 5.4.4.1.
2. The GP Client queries the GP Server, using LDAP, to determine the list of Group Policy Objects (GPOs). This is described in detail in [MS-GPOL] section 3.2.5.1.5.
3. For each GPO in the computed list from the server, the GP client queries the GP Server for the GPO's attributes, using LDAP and SMB. This is described in detail in [MS-GPOL] sections 3.2.5.1.5, 3.2.5.1.6, and 3.2.5.1.7.
4. Based on the classes of settings in the computed list of GPOs, the GP client invokes the appropriate client-side extensions.
5. Each client-side extension queries the GP Server, using LDAP or SMB, to retrieve the appropriate policy settings. This is described in detail in [MS-GPOL] section 1.3.3.3.

5.4.3 Group Policy Administrative Tool

The administrative tool allows policies to be created, deleted and modified. The tool also defines how policies will be applied to the client.

The tool uses the same core protocols and extensions to discover the GP Server and author policy as the GP client uses to discover and apply policy settings. These protocols for communication and authoring are described in [MS-GPOL] section 1.3.3.1 and 1.3.4.

The flow of communication is as follows:

1. The administrative tool locates the DC by following the steps as specified in [MS-DISO] section 5.4.4.1.
2. The administrative tool queries the GP server, using LDAP, to retrieve the GPO's attributes.
3. The extension plug-in queries the GP server, using LDAP or SMB, to retrieve the policy settings in GPO. This is described in detail in [MS-GPOL] section 1.3.4.
4. The extension plug-in writes policy setting changes to the GP server using LDAP or SMB.
5. The administrative tool updates the GPO version information in the GP server using LDAP and SMB. This is described in detail in [MS-GPOL] section 3.3.4.5.

5.5 Failure Scenarios

This section describes the common failure scenarios and specifies the system behavior in such conditions.

5.5.1 Connection Disconnected

A common failure scenario is an unexpected connection breakdown between the Group Policy Server and the Group Policy Client, or between the Group Policy Server and Admin tool. A disconnection can be caused by the network not being available or by the GP Server becoming unavailable. In both cases, where the network or the GP Server is not available, the effect on the GP Client and the Admin tool is the same. When the GP Client is not able to reach the GP Server, the policy application fails and a message is logged in the event log. The GP Client will periodically try to contact the GP Server to refresh its policy set. <4>

When the Admin Tool is not able to reach the GP Server, due for example to the network not being available or the GP Server being unavailable, an error message is displayed to the administrator. It is up to the administrator to retry the task when the issue has been resolved.

5.5.2 Internal Failures

5.5.2.1 Operating System related failures

It is possible that the Group Policy Client or the Admin tool may detect an unrecoverable internal state at any point during its operation. For example, this may be due to some operating system resources being unavailable. For this kind of failure, consequences and recovery are similar to the loss-of-connection failure as described in section 5.5.1. This kind of failure is detected when the operating system indicates that it could not allocate virtual memory, or is unable to access critical system resources. Recovery from this failure allows successful policy application.

5.5.2.2 Failure in client side extensions

An internal failure in any client-side extension does not cause the entire policy application to fail. The behavior of a given protocol extension is specific to each extension and is specified in the documentation of that extension. The consequence of this failure is that the settings corresponding to that protocol extension are not applied to the system. In the case of a client-side extension that depends on the Group Policy: Registry Extension Encoding ([MS-GPREG]), the extension and the Group Policy: Registry Extension Encoding are considered separate extensions and the failure of one does not indicate a failure of the other. As an implementation-specific optimization, an extension MAY choose to be skipped if the Group Policy: Registry Extension Encoding has failed. The failure is detected when the client-side extensions indicate error. At the next scheduled policy application, the Group Policy client will call the client-side extension again in an attempt to recover from the failure. Recovery from the failure allows the successful application of settings corresponding to the client side extensions. If a client-side extension for which a policy is configured is missing from the client, Group Policy client will ignore the policy for that extension and continue with application of policies for rest of the extensions. In other words, it is not an error condition for a client-side extension to be absent from the Group Policy client.

5.5.2.3 Link speed determination failure

If link speed determination (as described in section 2.2.6 of [MS-GPOL]) fails, Group Policy Client will assume link speed to be above threshold and process policy settings belonging to all client side extensions. At the next scheduled policy application, the Group Policy client will initiate link speed determination again in an attempt to recover from the failure. Recovery from the failure helps prevent application of policies from those client-side extensions that do not want to be invoked when link speed is below threshold.

5.5.3 History Repository Errors

The Group Policy Client maintains a history of policy application in order to optimize client performance and for certain cleanup tasks. If the history repository is corrupted or lost, the GP Client proceeds as though the policy was being applied for the first time, and the history repository is recreated.

5.5.4 SYSVOL file access failure

Group Policy Client may not be able to access SYSVOL [MS-SMB] file due to a few reasons: file replication delays, mis-configuration of file permissions by administrator. The consequence of this failure on Group Policy Client is that it will not be able to apply any policy. At the next scheduled policy application, the Group Policy client will attempt to apply policy again. Recovery from the failure helps ensure that the client has the latest set of policies.

6 System Details

This section contains the details that complete the descriptions in earlier sections of the document. These details are needed to understand and implement this system. Information already in the TDs should be referenced whenever available.

6.1 Architectural Details

This section documents the system architecture of the Group Policy System in terms of the following scenarios. Each scenario describes one or more goals of the Group Policy System. The scenarios are:

- Group Policy Processing
- Populating Administrative Tools with Configuration Data
- Authoring a New Policy
- Administrative Tool Cannot Connect to a Domain Controller
- Querying Active Directory for Scope Of Management (SOM) and Version Information
- Client Applying Policy
- Client Cannot Connect to a Domain Controller When Applying Policy

6.1.1 Group Policy Protocols Processing

The Group Policy Protocol allows clients to discover and retrieve policy settings that administrators of a domain create. Policy settings are administrative directives that administrators make regarding the behavior of the clients. These behaviors (or policy settings) fall into two classes: user policy settings and computer policy settings.

This section shows the various events that trigger Group Policy System Processing internal architecture. This gives a very high level picture of when different events happen when a machine starts up, a user logs on to the machine, a user logs off from the machine and when the machine shuts down. At the end of the diagram, references are provided to the different documents that describe these message sequences.

The figure also shows when the Group Policy Machine Startup, Machine Shutdown, User Logon, and User Logoff scripts are run. These scripts can also be stored at any location of the administrators choosing.

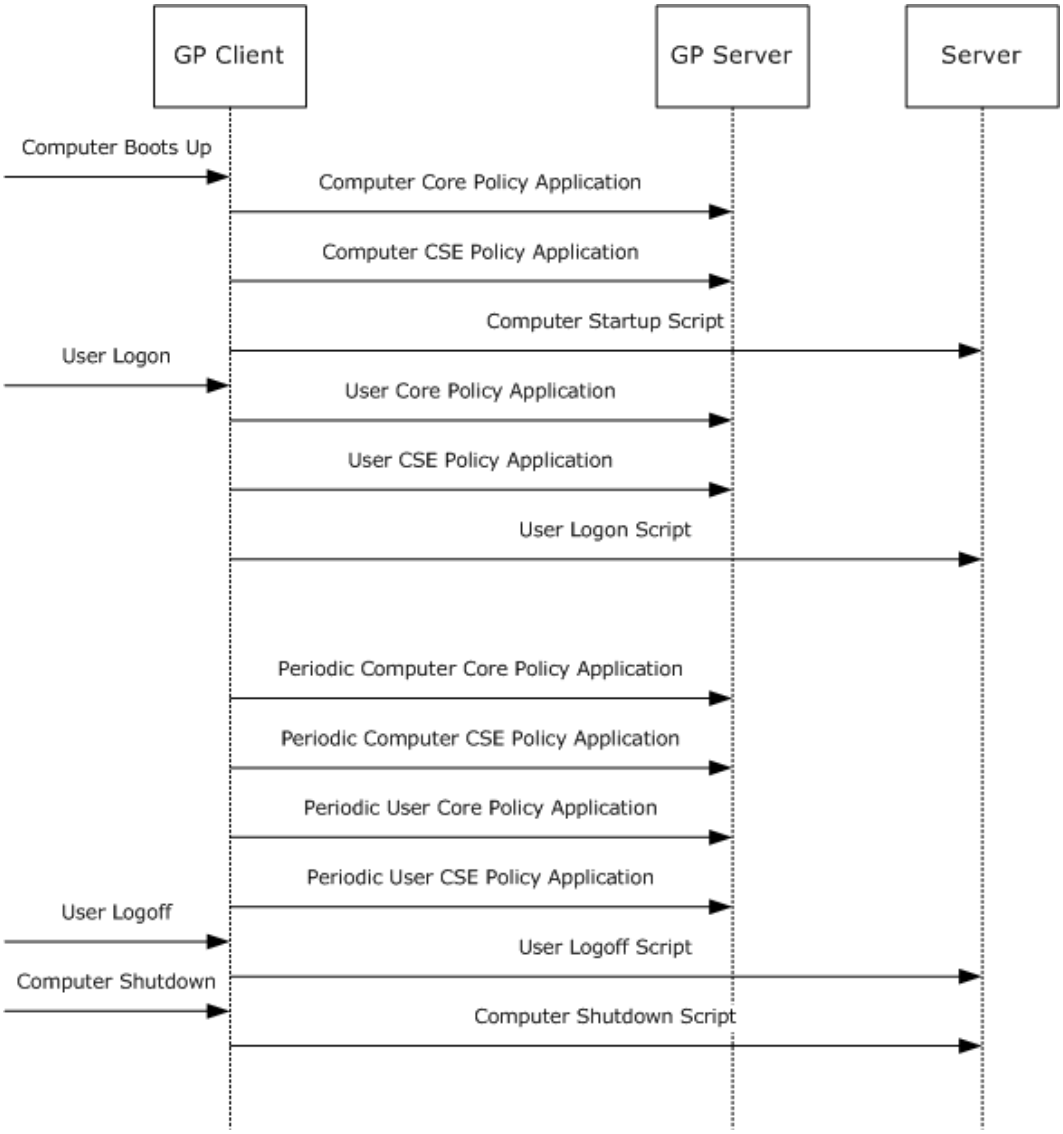

Figure 7: Group Policy System Processing internal architecture

The following table provides the document references for the messages in the figure that precedes it.

Group Policy messages and document references

Protocol message	Document name	Section
Computer Core Policy Application	[MS-GPOL]: Group Policy: Core Protocol Specification	1.3.3 Policy Application
Computer CSE Policy Application	[MS-GPOL]: Group Policy: Core Protocol Specification	3.2.5.1.10, Extension Protocol Sequences
Computer Startup Scripts	[MS-GPSCR]: Group Policy Scripts	3.2.5 Message Processing Events

Protocol message	Document name	Section
	Extension: Protocol Specification	and Sequencing Rules
User Core Policy Application	[MS-GPOL]: Group Policy: Core Protocol Specification	1.3.3 Policy Application
User CSE Policy Application	[MS-GPOL]: Group Policy: Core Protocol Specification	3.2.5.1.10, Extension Protocol Sequences
User Logon Scripts	[MS-GPSCR]: Group Policy Scripts Extension: Protocol Specification	3.2.5 Message Processing Events and Sequencing Rules
Periodic Computer Core Policy Application	[MS-GPOL]: Group Policy: Core Protocol Specification	1.3.3 Policy Application
Periodic Computer CSE Policy Application	[MS-GPOL]: Group Policy: Core Protocol Specification	3.2.5.1.10, Extension Protocol Sequences
Periodic User Policy Core Application	[MS-GPOL]: Group Policy: Core Protocol Specification	1.3.3 Policy Application
Periodic User CSE Policy Application	[MS-GPOL]: Group Policy: Core Protocol Specification	3.2.5.1.10, Extension Protocol Sequences
User Logoff Scripts	[MS-GPSCR]: Group Policy Scripts Extension: Protocol Specification	3.2.5 Message Processing Events and Sequencing Rules
Computer Shutdown Scripts	[MS-GPSCR]: Group Policy Scripts Extension: Protocol Specification	3.2.5 Message Processing Events and Sequencing Rules

6.1.2 Populating Administrative Tools with Configuration Data

This example demonstrates the process that occurs when the Group Policy administrative tools load and retrieve the appropriate data from the stores that contain policy data. The Admin tool will be populated with data retrieved from Active Directory and SYSVOL.

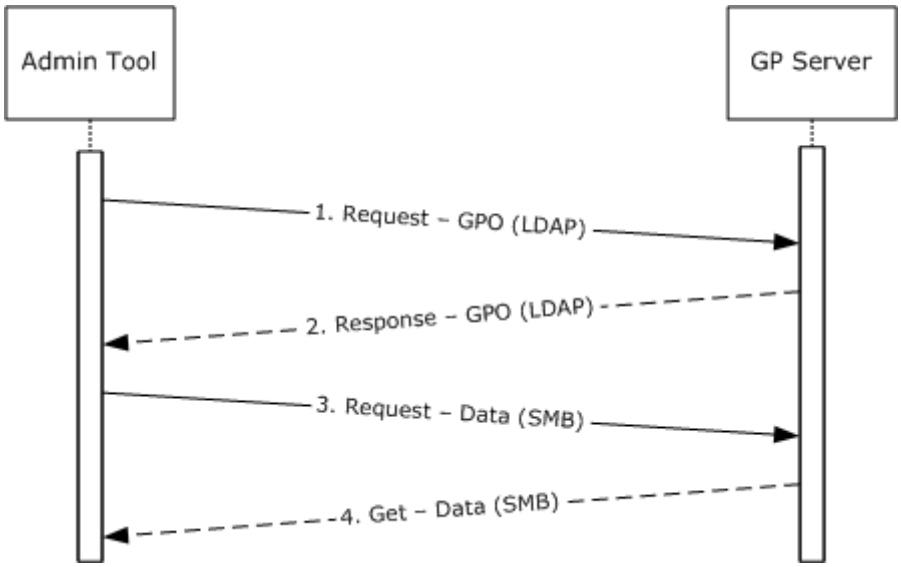

Figure 8: Populating administrative tools with configuration data

The message flow in this example is as follows:

1. When the Admin tool launches, it makes an LDAP call to Active Directory [MS-ADTS] to retrieve GPO information, as described in [MS-GPOL] sections 2.2.7 and 2.2.4.
2. The GPO information returned in response to the LDAP query is used to populate the tool.
3. During an editing operation, the Group Policy Protocol Admin tool invokes the Extension **Administrative plug-in**, which communicates with the SYSVOL [MS-SMB] to request the existing policy.
4. The policy data retrieved from SYSVOL is populated in the Admin tool.

6.1.3 Authoring a New Policy

This example describes the message flow during the action of authoring a new policy. The Admin tool will contact a domain controller (DC) and retrieve the list of existing policies. The administrator will then choose the action to create a new policy, and the GP server will handle the request by provisioning data in Active Directory (AD) and SYSVOL. When the policy is created, the administrator will open the policy and begin to author settings. As those settings are authored, the Admin tool will communicate with the GP Server, and both Active Directory and SYSVOL will be updated accordingly.

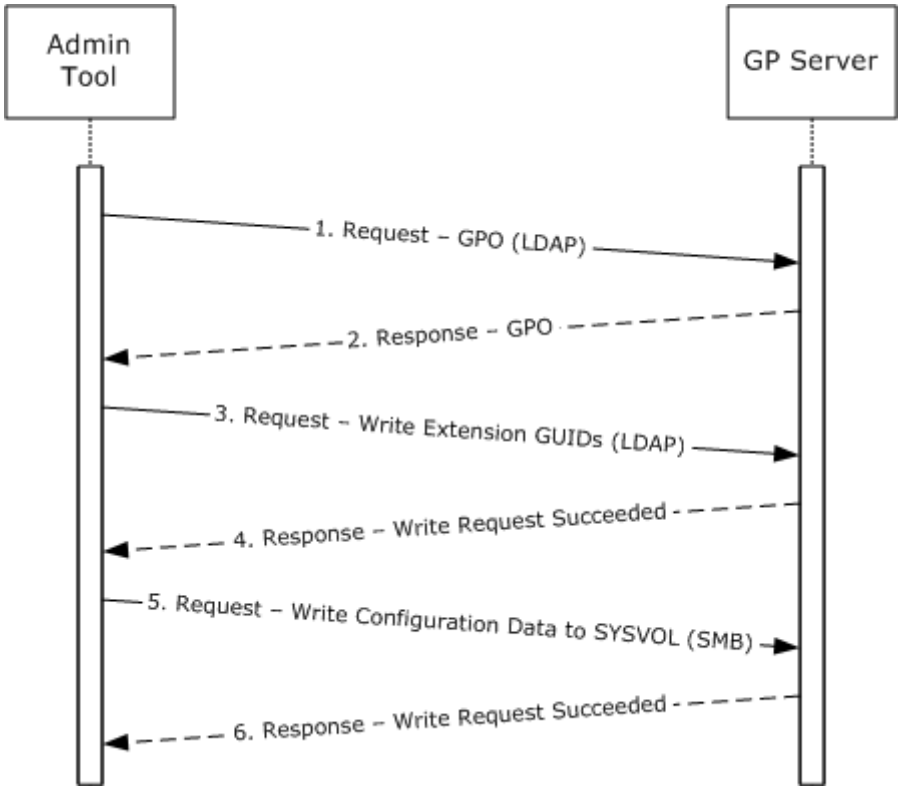

Figure 9: Authoring a new policy

The message flow in this example is as follows:

1. When the administrator creates a new GPO, the Admin tool makes an LDAP call to Active Directory [MS-ADTS] with the requested action.

2. The GP Server provisions data in Active Directory and SYSVOL to create the new GPO and sends a response to Admin Tool.

3. The administrator will begin to author specific settings within the policy. When any Extension Administrative plug-in modifies a GPO for the first time, an LDAP call is made to Active Directory [MS-ADTS], and the corresponding tool extension GUID and the client-side GUID are written to the **gPCMachineExtensionNames** or **gPCUserExtensionNames** attribute of the GPO.

4. The GP Server sends a response confirming the success of the write operation.

5. The configuration data is then written to SYSVOL [MS-SMB] in the folder that is created for the new policy.

6. The GP Server sends a response confirming the success of the write operation.

6.1.4 Administrative Tool Cannot Connect to a Domain Controller

This example describes the message flow during the action of editing a policy that ends in failure due to loss of connection with the domain controller (DC). Two scenarios are illustrated: failure to contact Active Directory (AD) and failure to contact SYSVOL.

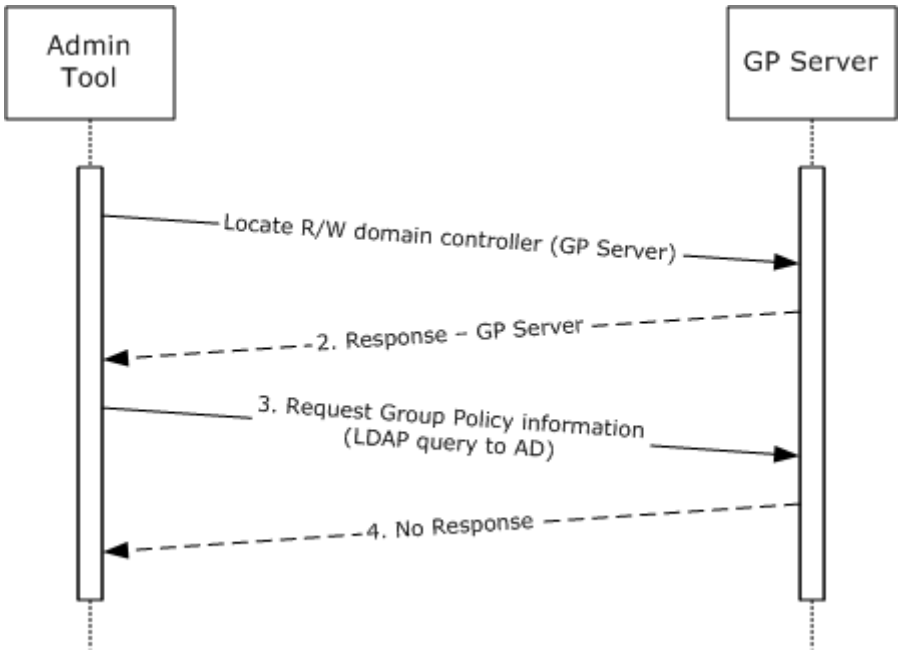

Figure 10: Administrative tool cannot contact Active Directory

The message flow in this example is as follows:

1. The Admin tool attempts to locate the GP Server in the domain by following the steps as specified in [MS-DISO] section 5.4.4.1.

2. The GP Server information is returned for the domain.

3. The Admin tool sends an LDAP query to Active Directory (AD) ([MS-ADTS]) to retrieve Group Policy Object (GPO) information, as described in [MS-GPOL] sections 2.2.4 and 2.2.7.

4. The Admin tool does not receive a response from the GP Server within the timeout interval.

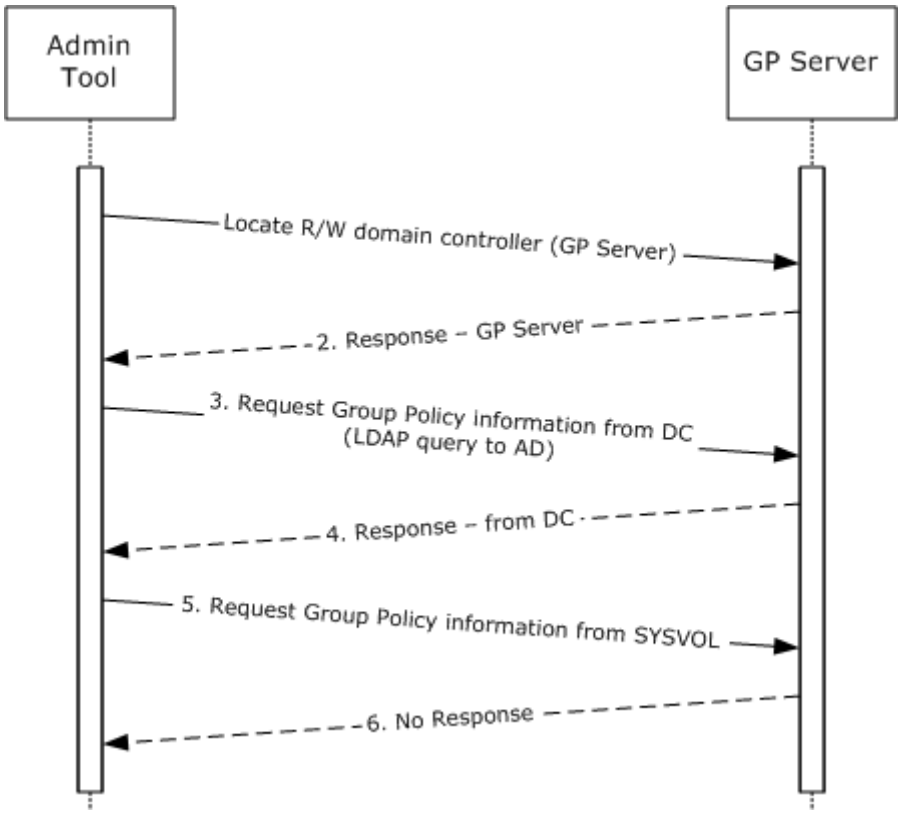

Figure 11: Administrative tool cannot contact SYSVOL

The message flow in this example is as follows:

1. The Admin tool attempts to locate the GP Server in the domain by following the steps as specified in [MS-DISO] section 5.4.4.1.

2. The GP Server information is returned for the domain.

3. The Admin tool sends a LDAP query to Active Directory (AD) ([MS-ADTS]) to retrieve GPO information, as described in [MS-GPOL] sections 2.2.4 and 2.2.7.

4. The Admin tool receives a response from the GP Server within the timeout interval.

5. The Admin tool requests the SYSVOL information from the GP Server.

6. The Admin tool does not receive a response from the GP Server within the timeout interval.

6.1.5 Querying Active Directory for Scope of Management (SOM) and Version Information

In this example, a GP Client queries a GP Server for Scope Of Management (SOM) and version information. SOMs contain user and computer account information and are associated with GP

objects. Each Group Policy Object (GPO) is associated with a specific policy target. Messages exchanged between the GP Client and the GP Server use LDAP as a transport.

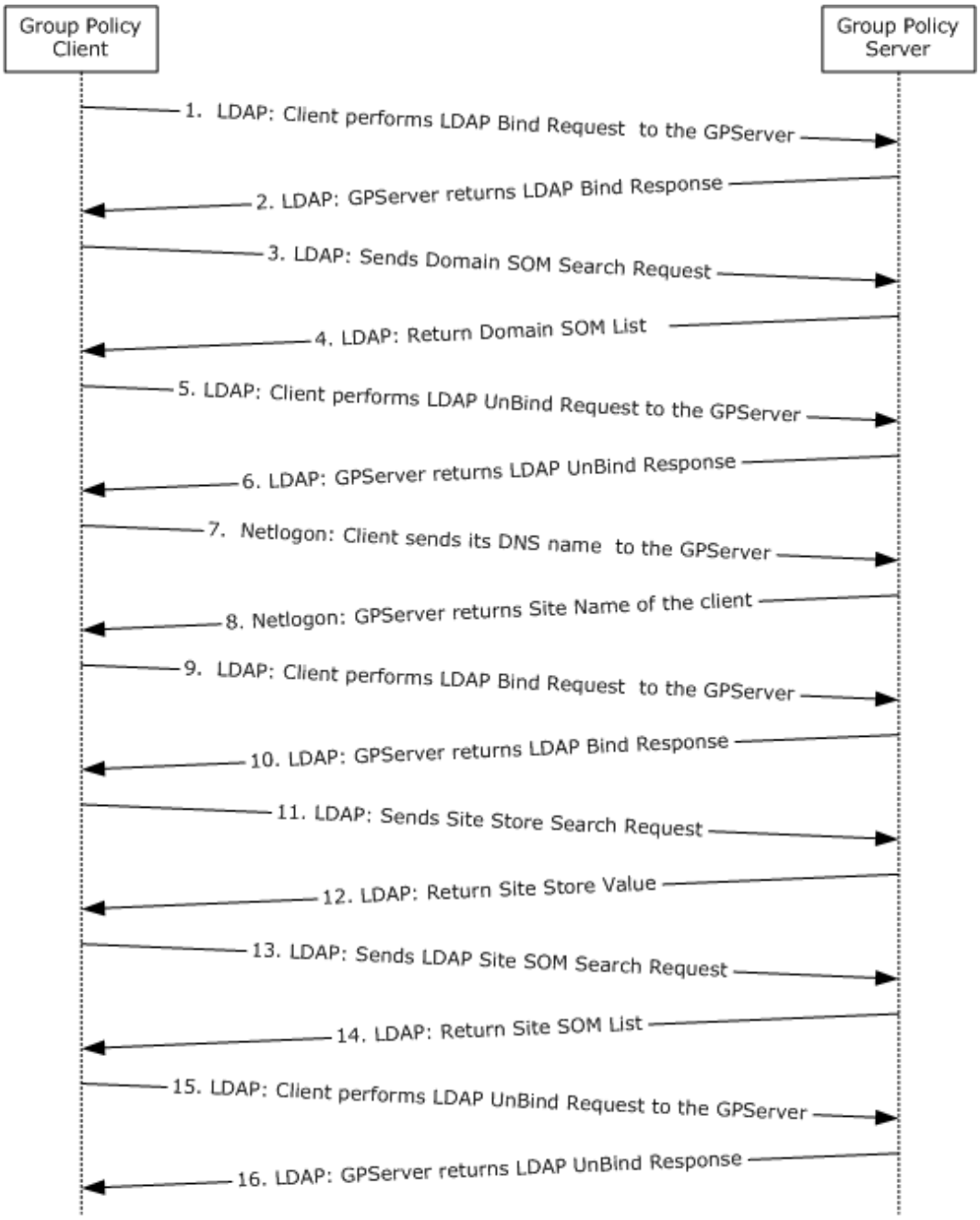

Figure 12: Querying Active Directory for Scope of Management (SOM) and version information

The message flow in this example is as follows:

1. The GP Client sends an LDAP BindRequest to the GP Server.

2. The GP Server sends an LDAP BindResponse to the GP Client.

3. The GP Client sends an LDAP Search Request to the GP Server, querying for GPlink and GPOption attributes for its **distinguished name (DN)** for the **domain naming context (domain NC)**. This is described in section 3.2.5.1.3 of [MS-GPOL].

4. The GP Client processes the GPlink and GPOption attributes information for the domain SOM and uses it to search for the list of GPOs for the domain SOM. This is described in section 3.2.5.1.5.

5. The GP Client sends an LDAP UnBindRequest to the GP Server.

6. The GP Server sends an LDAP UnBindResponse to the GP Client.

7. The GP Client sends a Netlogon request to the GP Server, using its **Internet host name**.

8. The GP Server responds with the site name to which the GP Client belongs.

9. The GP Client sends an LDAP BindRequest to the GP Server.

10. The GP Server sends an LDAP BindResponse to the GP Client.

11. The GP Client sends an LDAP Search Request to the GP Server, querying for configurationNamingContext attribute for the root of the domain. This is described in section 3.2.5.1.4 of [MS-GPOL].

12. The GP Client processes the **configurationNamingContext** attribute information for the root domain and uses it to compute the DN of the site. This is described in section 3.2.5.1.4 of [MS-GPOL].

13. The GP Client sends an LDAP Search Request to the GP Server, querying for **GPlink** and **GPOption** attributes for its DN for the Configuration Naming Context. This is described in section 3.2.5.1.4 of [MS-GPOL].

14. The GP Client processes the **GPlink** and **GPOption** attributes information for the site SOM and uses this information to search for the list of GPOs for the domain SOM. This is described in section 3.2.5.1.5.

15. The GP Client sends an LDAP UnBindRequest to the GP Server.

16. The GP Server sends an LDAP UnBindResponse to the GP Client.

6.1.6 Client Applying Policy

The Client's interaction with the GP Server in policy application exhibits a pull application in which the Client polls a GP server to check for new user GPOs.

When the Client discovers the GP Server, the Client performs two sets of queries on the directory of the GP server by using LDAP as a transport. The first set of queries determines which Group Policy Objects (GPOs) have been assigned.

The second set of queries determines attributes of the relevant policies, discovers the location of the policy files, and determines any exclusionary filtering.

The Client then processes any relevant filters and checks the link state to potentially filter down the extension list.

Finally, the client-side extensions read the relevant policy settings from the server (stored in the Active Directory (AD) or SYSVOL) using SMB or LDAP, and applies them.

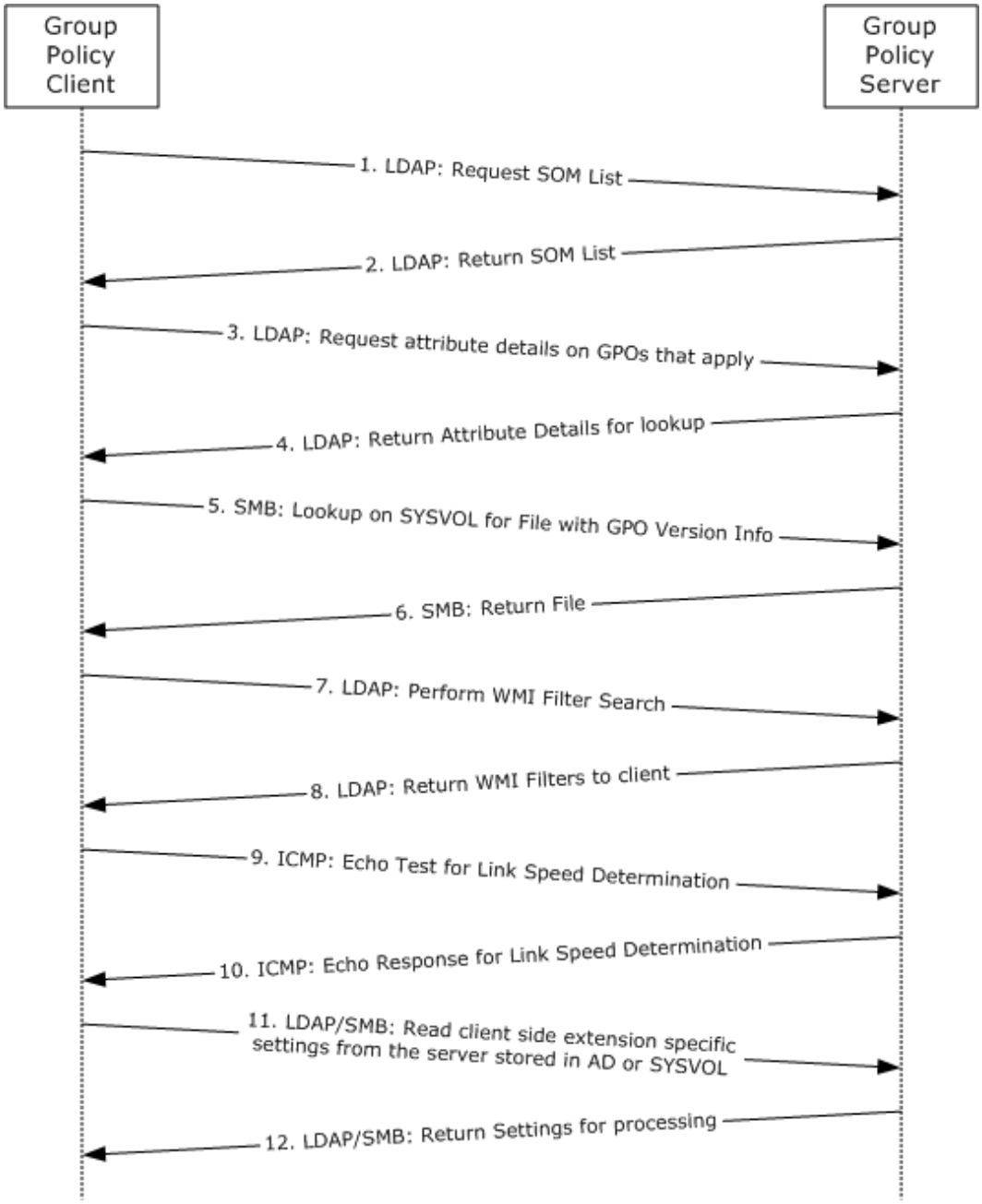

Figure 13: Client applying policy

The message flow in this example is as follows:

1. The Client sends an LDAP request to the GP Server to discover the policies that apply to the user and to the computer. For more information, see [MS-GPOL], sections 2.2.2 and 2.2.3.

2. The GP Server sends the Client, through LDAP, a list of policies that apply to the user and to the computer. For more information see [MS-GPOL], sections 2.2.2 and 2.2.3.

3. The Client receives the list of policies, then sends a query to the GP Server, through LDAP, requesting specific attributes that define further filtering, the location of the policy file, and the precedence order for sequential application of policies and classes of settings. For more information, see [MS-GPOL] section 2.2.4.

4. The GP Server returns, through LDAP, the list of attributes that the Client has requested. The Client then invokes any extension settings that are defined as part of the class attributes returned. For more information, see [MS-GPOL] section 2.2.4.

5. The Client sends a Server Message Block (SMB) request to the GP Server file system location of a file that contains version information for the GPO files. For more information, see [MS-GPOL] section 2.2.4.

6. The GP Server returns the file through SMB. The Client parses the file to check the versions applied. For more information, see [MS-GPOL] section 2.2.4.

7. The Client sends an LDAP request to the GP Server to retrieve any WMI filters that apply to the GPO's in scope of the client. For more information see [MS-GPOL] section 2.2.5.

8. The GP Server sends a response back to the client with any relevant GPOs that apply to the client. For more information, see [MS-GPOL] section 2.2.5.

9. The GP Client may send a request to the GP Server to determine the link speed. For more information, see [MS-GPOL] section 2.2.6.

10. The GP Client receives a response from the GP Server that assists the client in determining link speed. For more information, see [MS-GPOL] section 2.2.6.

11. If there is something to apply, the Client sends an SMB or LDAP request to the GP Server that stores the extension-specific policy settings. This can involve obtaining data from a server other than the GP Server. For more information, see [MS-GPOL] section 2.2.7.

12. The GP Client then retrieves the requested settings and applies them. For more information see [MS-GPOL] section 2.2.7.

6.1.7 Client Cannot Connect to a Domain Controller When Applying Policy

This example assumes that the Client has completed the step of discovering the domain controller (DC) during policy application. This example describes the message flow during a policy application that ends in failure due to loss of connection with the domain controller (DC). Two scenarios are illustrated: failure to contact Active Directory and failure to contact SYSVOL.

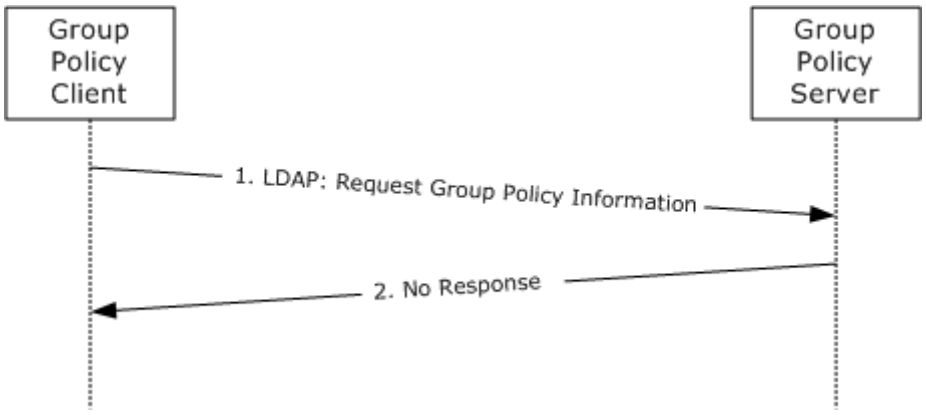

Figure 14: Client cannot contact Active Directory when applying policy

The message flow is as follows:

1. The Client sends an LDAP query to the GP Server.
2. The Client does not receive a response from a GP Server within the timeout interval.

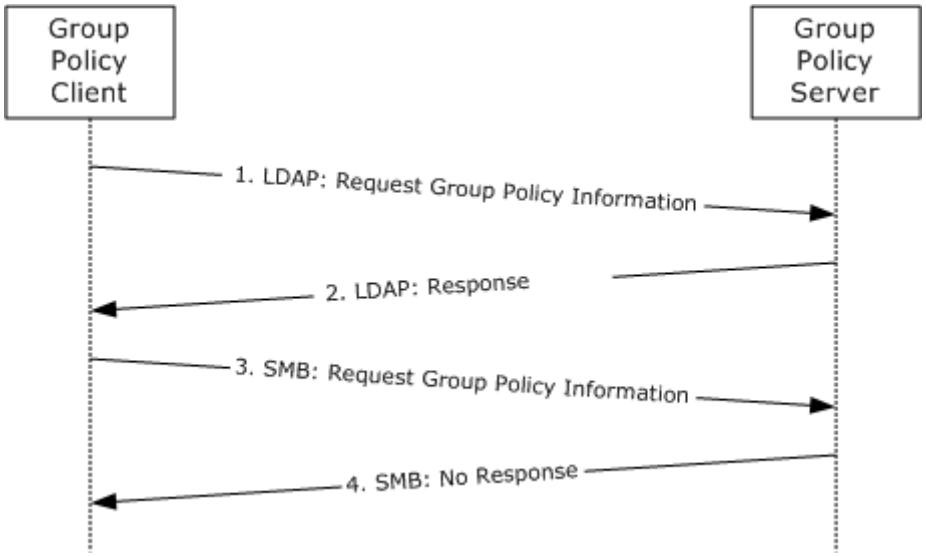

Figure 15: Client cannot contact SYSVOL when applying policy

The message flow is as follows:

1. The Client sends an LDAP query to the GP Server.
2. The Client receives an LDAP response from a GP Server.
3. The Client sends an SMB query to the GP Server.
4. The Client does not receive a response from a GP Server within the timeout interval.

6.2 Communication Details

The following two examples describe the protocol communications and interactions providing the transport for communication that the Group Policy system relies on. While these protocols have been noted in previous examples, the actual processes for communication have not. The two communication process flows of interest are the interactions between the Group Policy Client and the Group Policy server and the interaction between the Administrative tool and the Group Policy Server. In the following examples the domain is *corp.example.com*.

6.2.1 Protocol communication between a Group Policy Client and Group Policy Server

As described in previous sections, there are several core protocols used as transports for GP specific information between the GP Client and the GP Server. These protocols follow previous examples from section 6.1 and use protocols of DNS, DC Location, Netlogon and SMB. The following section describes how these protocols are used to transport the necessary data.

6.2.1.1 Locate a GP Server

The process of locating a GP Server involves discovering an LDAP server and, through the associated LDAP lookup, the file system where the policy files are located. In the Microsoft implementation both roles are located on the same server which is known as a domain controller.

The process of locating a domain controller is referred to in [MS-DISO] section 5.4 though the GP client relies on successful location based on DNS domain names. DNS Domain Name Service resolution is described in [MS-DISO] section 5.4.4.1.

6.2.1.2 Domain SOM Search and Response

An LDAP BindRequest from the Client to the GP server and an LDAP BindResponses in reply are generated. After the GP Client has received a successful BindResponse from the Domain Controller it sends an LDAP Search Request to the GP Server with LDAP information about its location in the directory, querying for gpLink and gpOption attributes that hold information on the GPOs in its scope of management for the Configuration Naming Context.

The Domain Controller processes the information provided as part of the request for the Domain SOM and returns the gpLink and gpOption object information as well as the distinguished name (DN) for which it applies to the GP Client.

The gpLink attributes in particular define a location in Active Directory to reference further information about a GPO. These locations to objects will be used later in the policy application process to determine the location of the policy files on the fileserver.

An example of a gpLink attribute is: [LDAP://CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=test,DC=example,DC=com;0]

6.2.1.3 Site SOM Search and Response

After the GP Client has determined its Domain SOM, it then determines the site that the computer belongs to. The site to which the Client computer belongs (the SiteName) is detailed in [MS-DISO] section 4.3.1.1. Because the site can change based on the GP client's location, this step must occur as part of policy processing.

Now that the GP Client knows the site it belongs to, it makes an LDAP query for the same attributes as the Domain SOM Search which are the gpLink and gpOptions attributes, though it passes the site name it has discovered as part of its SOM Search. The Domain Controller returns the gpLink and gpOptions attributes that apply to the client for processing.

If no site exists, the remainder of this message MUST be skipped, and the protocol sequence for the next message is initiated. If this message is invalid in any way, (as specified in section 2.2.3 of [MS-GPOL]), the entire Group Policy: Core Protocol policy application sequence MUST be terminated.

The retrieved gpLink attribute of the site contains LDAP DNs for GPOs that are associated with this site. The gpLink, gpOptions, and the site DN MUST be appended to the end of the SOM list.

6.2.1.4 GPO Search and Reply

After the GP Client has retrieved the Domain and Site SOM lists it is ready to discover more information about the GPO's that apply to it. This message requires the success of all previous messages that have retrieved a scope of management and a gpLink that are associated with each of the SOMs, and have stored them in the SOM list. If this message is invalid, the entire policy application mode sequence MUST be terminated. The GP Client MUST NOT generate further policy application messages for this cycle of the policy application sequence.

The GP Client creates a list of prioritized list of GPO's as per section 3.2.5.1.5 of [MS-GPOL] and sends an LDAP query to the Domain Controller with the list. The Domain Controller returns an LDAP reply with further attribute information about each policy object queried as per section 2.2.4 of [MS-GPOL].

These attributes describe the display name of the policy object, the location of the policy file on the file server, extensions used in that policy file, and any WMI filters that may apply to the GPO.

For each GPO successfully retrieved in each search, the following SMB Protocol sequences MUST be generated:

SMB File Open from Client to Server: The file <gpo path>\gpt.ini is a file on the Server. As part of this open operation, authentication MUST occur (SPNEGO for user policy mode and Kerberos for computer policy mode). The directory <gpo path> corresponds to the file system path retrieved for the GPO in the gPCFileSysPath attribute of the search.

SMB File Read Sequences: A series of SMB file reads MUST be done until either the entire contents of the opened file are read or an error in reading occurs.

File Close: An SMB file close operation MUST then be issued.

6.2.1.5 WMI Filter Processing

Once the GP client has processed the GPO attributes returned to it from the Domain Controller and determined that a policy object has a WMI query that applies to a GPO, it now has the location of that WMI filter in the LDAP directory and makes an LDAP query for it to the Domain Controller, passing in the location and attributes it requires as per section 2.2.5 of [MS-GPOL].

The Domain Controller responds with an LDAP response that returns the necessary attribute information as per section 2.2.5 of [MS-GPOL]. The client can now process the WMI query and determine if the policy (that the WMI query applies to) applies to it.

If it cannot be evaluated due to some local error on the Client, the entire policy application mode sequence MUST be terminated. If the WMI query returns no results, the GPO MUST be considered denied; otherwise, the GPO MUST be considered allowed as per section 3.2.5.1.7 of [MS-GPOL].

6.2.1.6 Link Speed Determination

The client SHOULD estimate the link speed of the network between the client and the domain controller by implementation-specific means.<5> The Link Speed Determination message MAY use Internet Control Message Protocol (ICMP) as a transport supporting at least 500 byte packets, as specified in [RFC792], as an implementation-specific means. If the determined Link Speed (3.2.5.1.9 of [MS-GPOL]) is below an implementation-defined threshold, an implementation SHOULD NOT invoke any Protocol Extension sequence that is bandwidth intensive.<6>

6.2.1.7 Policy File Read Operation

When the client has all the attribute information about the GPO's that apply to the GP Client, has evaluated any applicable filters, and has determined the link state it is ready to read the extension information from the policy files.

The GP Client, using the specific extensions relevant to the GPO, makes an SMB request to the file system location specified in the LDAP attributes returned in the LDAP queries from Section 6.2.1.4 and reads the specific extension settings from the policy files.

If the determined Link Speed (section 3.2.5.1.9 of [MS-GPOL]) is below an implementation defined threshold, an implementation SHOULD NOT invoke any Protocol Extension sequence that is bandwidth intensive. <7>

6.2.2 Protocol communication to and from the Administrative Tool and Group Policy Server

Group Policy is managed with an administrative tool that uses the same protocols and, in several instances the same protocol sequence methods that the GP Client itself uses. The protocol steps differ for the two main operations of new policy creation and existing policy editing.

6.2.2.1 Creating Group Policy Objects (GPOs)

In authoring new policy objects (GPOs), the first three steps of the protocol sequence for the administrative tool are identical. These are:

Locate a GP Server (refer to section 6.2.1.1)

Find location based on DNS Domain Name (refer to section 6.2.1.2)

Initiate LDAP Bind Request/Response (refer to section 6.2.1.3)

Creation of a GPO requires the creation of a groupPolicyContainer Active Directory object on the GP server and a corresponding directory on the GP server's SYSVOL file system share. The creation of the LDAP portion of the GPO MUST be accomplished through an LDAP message from the Client to the Server. The LDAP message is an addRequest message and follows the message format as per section 2.2.8.1 of [MS-GPOL].

The Admin tool receives an addResponse message in reply, as defined in section 4.7 of [RFC2251]. The resultCode field value determines a failure or success for the message. Success is indicated when the value of the addResponse message's resultCode is 0. Any other resultCode value indicates a failure.

After these messages are successfully processed, the user-scoped GPO DN and computer-scoped GPO DN MUST be created for this GPO. The SMB messages described in the GPO Creation Message section of [MS-GPOL] (section 2.2.8.1) make up the remainder of the GPO Creation message.

The final portion of this message is to generate a gpt.ini file with the format and semantics that are described in section 2.2.4 of [MS-GPOL]. This file Version field MUST be 0.

After the GPO Create operation has completed successfully, the editing process for a new policy follows the same process as editing existing policy.

6.2.2.2 Editing Existing Policy

Before the administrative tool can begin editing policy objects it must make a connection to the LDAP directory to lookup LDAP objects and follows the same three steps as in policy application.

These are:

Locate a GP Server (refer to section 6.2.1.1)

Find location based on DNS Domain Name (refer to section 6.2.1.2)

Initiate LDAP Bind Request/Response (refer to section 6.2.1.3)

When the administrative tool has discovered a writable Domain Controller and made a successful connection to the LDAP directory the administrator can select a policy to be edited or updated.

There are three types of updates that can be made to policy objects.

6.2.2.2.1 Extension Settings

When the administrative tool is required to update policies it invokes the extensions referenced in the GPO. These make direct writes against both the Active Directory using LDAP and against the policy file in the file system through SMB.

Whenever an administrative tool invokes an extension plug-in for a GPO and that plug-in modifies the GPO, the extension plug-in invokes the GPO Extension Update sequence, which produces the GPO Extension Update message. This message MUST be an LDAP modifyRequest with the parameters as specified in [MS-GPOL] section 2.2.8.2.

The administrative client receives a modifyResponse message in reply, and this value indicates a failure or success for the message. If the value of the modifyResponse message is the integer 0, this indicates success. Any other code indicates a failure.

The administrative client then uses SMB to update the GPT.ini file in the GPO path and receives responses that provide confirmation of success. Further details on the message flow are found in section 2.2.8.2 of [MS-GPOL].

6.2.2.2.2 GPO Property Update

Whenever an administrative tool modifies the properties of a GPO, it produces the GPO Property Update message. This message MUST be an LDAP modifyRequest with parameters described in section 2.2.8.3 of [MS-GPOL]. The Client receives a modifyResponse message in reply, and this value indicates a failure or success for the message. If the value of the modifyResponse message is the integer 0, this indicates success. Any other code indicates a failure.

The following SMB messages make up the remainder of the GPO Property Update message:

1. SMB Open GPO path, using SPNEGO (as specified in [MS-SPNG]) for authentication.
2. Modify the security descriptor on the directory.
3. SMB Close.

6.2.2.2.3 SOM Updates

Whenever an administrative tool modifies the properties of the SOM, it produces the SOM Property Update message. This message MUST be an LDAP modifyRequest with parameters described in section 2.2.8.4 of [MS-GPOL]. The client receives a modifyResponse message in reply, and this value indicates a failure or success for the message. If the value of the modifyResponse message is the integer 0, this indicates success. Any other code indicates a failure.

6.3 Transport Requirements

The figure in section 5.2 titled Protocol layering relationships shows the protocol dependencies of the protocols used by the GP Client.

The Client uses:

1. SMB and LDAP for transmitting Group Policy settings, and for transmitting instructions between the GP Client and the GP Server.

2. Kerberos and SPNEGO for authenticating the computer for computer policy application.

3. SPNEGO for user policy application.

6.4 Timers

The client SHOULD have the following timer:

Periodic Refresh timer: This timer SHOULD be triggered periodically to check for updated policy for the computer or each user interactively logged on to the computer. The frequency of this timer is implementation specific.<8>

6.5 Non-Timer Events

On the client, policy application in computer policy mode SHOULD be invoked at the time that the computer boots or connects to a new network and MAY be invoked at other times. Policy application in user policy mode SHOULD be invoked at the time a user logs in or connects to a new network and MAY be invoked at other times.

Events related to the use of administrative tools include the following:

Group Policy creation occurs whenever an administrator uses a Group Policy Admin tool to create a GPO. This triggers a GPO Creation (section 2.2.8.1 of [MS-GPOL]) message.

Group Policy property update occurs whenever an administrator uses a Group Policy extension's Policy Administration protocol to change properties on a GPO. This triggers a GPO Property Update (section 2.2.8.3 of [MS-GPOL]) message.

The Scope of Management (SOM) property update occurs whenever an administrator uses a Group Policy extension's Policy Administration protocol to change Group Policy properties on an SOM. This triggers an SOM Property Update (section 2.2.8.4 of [MS-GPOL]) message. The Group Policy extension settings update occurs when an administrator uses a Group Policy extension's Policy Administration protocol to change an extension's settings in a GPO. This triggers a GPO Extension Update (section 2.2.8.2 of [MS-GPOL]) message. The version number that is used for GPO container version and GPO file system version MUST be computed as specified in section 3.3.4.5 of [MS-GPOL].

The local **PolicyChange** event is triggered at the end of policy application to indicate that the policy has changed.

6.6 Initialization and Re-initialization Procedures

During initialization, the Group Policy client SHOULD register for computer boot and user logon notification. As part of re-initialization, the Group Policy client SHOULD recreate the operational state pertaining to the machine and every logged-on user.

6.7 Status and Error Returns

The system does not define any error handling requirements beyond those described in the specifications of the protocols supported by the system, as listed in section 2.2.

Various kinds of errors may occur impacting the system. More precisely, an error condition may impact one or more protocols supported by the system. Such error conditions and the resulting protocol semantics are described under section 2 of the corresponding protocol specifications.

Windows returns the following error codes for the failure scenarios described in section 5.5:

Connection disconnected: ERROR_NO_SUCH_DOMAIN

Operating system related failures: ERROR_OUTOFMEMORY, ERROR_ACCESS_DENIED.

SYSVOL file access failure: ERROR_FILE_NOT_FOUND, ERROR_ACCESS_DENIED.

Active Directory (AD) or SYSVOL Timeout Failures: ERROR_TIMEOUT

Client side extensions indicate error by returning an error code other than ERROR_SUCCESS or E_PENDING.

7 Security

This section documents system-wide security issues that are not otherwise described in the Technical Documents (TDs) for the Member Protocols. It does not duplicate what is already in the Member Protocol TDs unless there is some unique aspect that applies to the system as a whole.

In a distributed environment where information is stored and retrieved from clients to the server, it is essential to protect the information that is exchanged from tampering. Protocols that comprise the Group Policy System are not intended to transmit sensitive information, and therefore should not be used for transmitting this information. The security for the Group Policy System Protocols is described in the set of protocols that describe the Group Policy System Protocols, as specified in section 2.2.

7.1 Internal Security

This section describes the internal security of the GP Client. The GP Server and the Admin tool are not discussed here because their security requirements are covered under the respective protocol documents. It is necessary that any administrative intent is not tampered with and modified by a user who does not have the necessary privileges. The following figure shows the different components that defines the security boundary for Group Policy System on the client. The figure does not show the external pieces because those are described in [MS-GPOL]. The general guideline for any implementer of Group Policy System protocol is that it SHOULD ensure that the resources that are used by the engine and the extensions are protected so that no unauthorized access is possible.

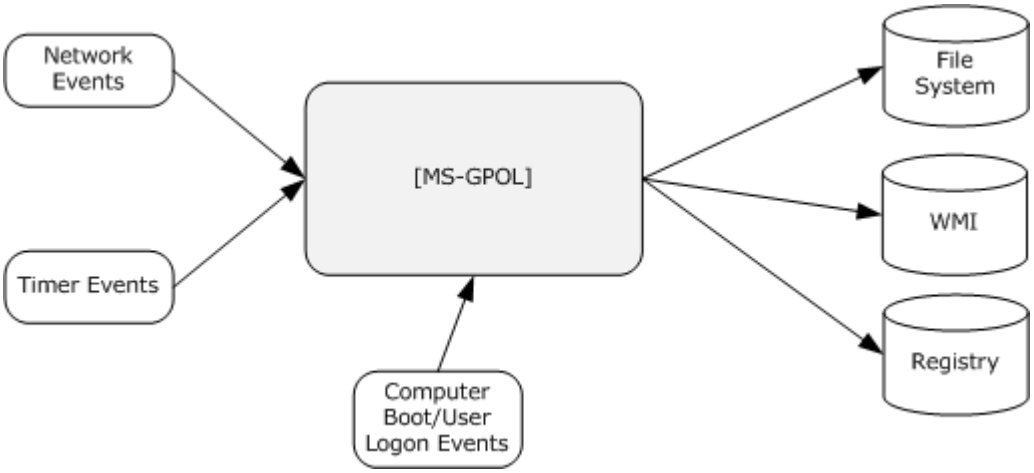

Figure 16: Group Policy System security boundary components

7.1.1 Local Data Store

Group Policy System writes policy information to various local data stores where the policy information is persisted, and ensures that appropriate permissions are set on each resource so that no user can tamper with the data unless the user has permissions to the resource. Group Policy Protocols set the permissions on the resources so that a user has only read permissions to the resources, and therefore cannot change the data. Group Policy cannot protect against a user with administrative privileges because that user can take ownership of the resource and make changes.

7.1.2 Timer Events/Network Events

The Group Policy client runs periodically in the background, triggered by the firing of a timer or a network event, such as the user's network state changing. Any implementation of Group Policy System Protocols SHOULD ensure that the source of these events are trusted and cannot be spoofed.

7.1.3 Computer Boot/Logon Events

These events are used to apply policies to a user or a computer at computer startup or user logon. Any implementations of Group Policy System Protocols SHOULD ensure that any component that generates these events are trusted and cannot be spoofed.

7.2 External Security

Group Policy System Protocol uses the mechanism provided by the transport to ensure that the data is protected against tampering, and it uses the authentication mechanism provided by the underlying protocols to establish the identity of the clients. Group Policy System Protocol uses LDAP and SMB signing for the policy data; Kerberos authentication for computer policy application; and SPNEGO authentication for user policy application. This is described in section 5 of [MS-GPOL]. The system does not define any additional external security beyond those described in the specifications of the protocols supported by the system, as listed in the table in section 2.2.

8 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 Server 2003 R2 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 4.3.2: In the Microsoft implementation, this refresh period is every 90mins plus or minus a random offset value.

<2> Section 4.3.2: In a Microsoft implementation, the Registry is used to store GP information.

<3> Section 4.3.2: Windows 2000, Windows XP, and Windows Server 2003 use ICMP to determine the link speed between the client and the domain controller.

<4> Section 5.5.1: For Windows Vista, Windows Vista SP1, Windows Server 2008, Windows 7, and Windows Server 2008 R2 only: when the network is unavailable, the GP Client also listens to network change notifications so that the policy can be applied as soon as the network is reachable. When a network change is detected and the GP Server is reachable the policy application is only applied if the time elapsed is greater than the periodic refresh interval.

<5> Section 6.2.1.6: Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 use normal protocol traffic for the link speed determination. Windows 2000, Windows XP, and Windows Server 2003 use ICMP to determine the link speed between the client and the domain controller. The following algorithm is used to determine the link speed when ICMP is used.

1. An ICMP Echo request with a packet size between 500–2,048 bytes is formed.
2. The request is sent to the domain controller three times, and the round-trip time for each of the echo responses is computed.

3. The packet size divided by average response time is used as the estimate of the link speed between the Client and the domain controller.

<6> Section 6.2.1.6: By default, Windows clients (versions Windows 2000, Windows XP, and Windows Server 2003) do not invoke the Software Installation [MS-GPSI] and Folder Redirection [MS-GPFR] extensions if the link speed is less than 500 kilobytes per second. An administrator can use Group Policy to modify the threshold speed and the set of extensions to be skipped.

<7> Section 6.2.1.7: By default, Windows clients (versions Windows 2000, Windows XP, and Windows Server 2003) do not invoke the Software Installation, as specified in [MS-GPSI], and Folder Redirection, as specified in [MS-GPFR], extensions if the link speed is less than 500 kilobytes per second. An administrator can use Group Policy to modify the threshold speed and the set of extensions to be skipped.

<8> Section 6.4: Periodic timer expiration for each user interactively logged on to the computer and for the computer itself: every 90 minutes, by default, plus a random offset between 0 and 30 minutes by default. Windows Group Policy client maintains separate timers for the Computer and each user interactively logged on to the computer. These timeouts can vary from as low as 1 minute to any number of days. The timer interval is a value determined by the client computer configuration and is typically configured by an administrator.

9 Change Tracking

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

10 Index

A

Abstract data model
  administrative tool 35
  client 34
  overview 34
  server 34
Administering Group Policy 26
Administrative tool
  communicating with
    creating Group Policy Objects 58
    editing existing policy 58
    overview 58
  non-timer events 60
  populating with configuration data 47
  unable to connect to domain controller - example 49
Administrative tool - abstract data model 35
Applicability 33
Applying Group Policy 24
Assumptions 28
Authoring new policy - example 48

B

Black box relationships 29

C

Capability negotiation 33
Change tracking 66
Client
  administering Group Policy 26
  applying Group Policy 24
  applying policy - example 52
  communication with server 55
  Group Policy 42
  non-timer events 60
  requesting domain scope of management 56
  requesting site scope of management 56
  timers 60
  unable to connect to domain controller when applying policy - example 54
Client abstract data model 34
Communication
  between client and server 55
  determining link state 57
  GPO search and reply 56
  locating domain controller 56
  overview 55
  policy file read operation 57
  scope of management search and response (section 6.2.1.2 56, section 6.2.1.3 56)
  with administrative tool and Group Policy server
    creating Group Policy Objects 58
    editing existing policy 58
    overview 58
  WMI filter processing 57
Concepts - system-specific
  Group Policy extensions
    client-side 18
    overview 17
    tool 20
  Group Policy Objects 16
  overview 15
  policy settings 15
Connection disconnected failure scenario 43
Context 28

D

Data model - abstract
  administrative tool 35
  client 34
  overview 34
  server 34
Disconnected connection failure scenario 43
Domain controller - locating 56

E

Environment 28
Error returns 60
Examples
  administrative tool unable to connect to domain controller 49
  authoring new policy 48
  client applying policy 52
  client unable to connect to domain controller when applying policy 54
  overview 45
  populating administrative tools with configuration data 47
  querying Active Directory for scope of management and version information 50

F

Failure scenarios
  connection disconnected 43
  history repository errors 44
  internal failures 43
  overview 43
Fields - vendor-extensible 33
Foundation 15
Functional architecture 34
Functional relationships
  groups
    Group Policy Core Protocol 39
    Group Policy Extension Protocol 39
    overview 39
  roles 37

G

Glossary 7
Group Policy
  administering 26

applying 24
extensions
client-side 18
overview 17
tool 20
objects 16
Group Policy Client 42
Group Policy Object
creating 58
search and reply 56
updating
extension settings 59
overview 58
properties 59
scope of management updates 59
Group Policy Server 42
Group Policy: Core Protocol Group 39
Group Policy: Extension Protocol Group 39
Groups
Group Policy Core Protocol 39
Group Policy Extension Protocol 39
overview 39

H

History repository error failure scenario 44

I

Informative references 10
Initialization 60
Internal architecture
Group Policy Client 42
Group Policy Server 42
Internal failure scenario 43
Introduction 7

L

Link state - determining 57

M

Member protocols 12

N

Non-timer events 60
Normative references 8

O

Overview 11

P

Policy files - reading extension information from 57
Policy settings 15
Populating administrative tools with configuration data - example 47
Preconditions 28
Product behavior 64
Purposes 21

Q

Querying Active Directory for scope of management and version information - example 50

R

References
informative 10
normative 8
overview 8
Reinitialization 60
Relationships
black box 29
dependencies 30
influences 31
overview 29
white box 35
Required knowledge
Group Policy extensions
client-side 18
overview 17
tool 20
Group Policy Objects 16
overview 15
policy settings 15
Returns - status and error 60
Roles 37

S

Scope of management
requesting domain 56
requesting site 56
Security
external 63
internal
computer startup and logon events 63
data stores 62
overview 62
timer and network events 63
overview 62
Server
communicating with
creating Group Policy Objects 58
editing existing policy 58
overview 58
communication with client 55
Group Policy 42
locating 56
Server abstract data model 34
Services 22
Stakeholders 22
Standards 13
Status returns 60
Summary 11
System purposes 21
System-specific concepts
Group Policy extensions
client-side 18

overview 17
tool 20
Group Policy Objects 16
overview 15
policy settings 15

T

Timers 60
Tracking changes 66
Transport 59

U

Use cases
descriptions
administering Group Policy 26
applying Group Policy 24
diagrams 23
stakeholders 22

V

Vendor-extensible fields 33
Versioning 33

W

White box relationships 35
WMI filter processing 57