[MS-GPSB]:
Group Policy:
Security Protocol Extension

Revision Summary

Date	Revision History	Revision Class	Comments
03/14/2007	1.0	Major	Updated and revised the technical content.
04/10/2007	1.1	Minor	Updated the technical content.
05/18/2007	2.0	Major	New format
06/08/2007	2.0.1	Editorial	Revised and edited the technical content.
07/10/2007	3.0	Major	Added normative references; updated technical content.
08/17/2007	4.0	Major	Updated and revised the technical content.
09/21/2007	4.0.1	Editorial	Revised and edited the technical content.
10/26/2007	4.0.2	Editorial	Revised and edited the technical content.
01/25/2008	4.0.3	Editorial	Revised and edited the technical content.
03/14/2008	4.0.4	Editorial	Revised and edited the technical content.
06/20/2008	5.0	Major	Updated and revised the technical content.
07/25/2008	5.0.1	Editorial	Revised and edited the technical content.
08/29/2008	5.0.2	Editorial	Revised and edited the technical content.
10/24/2008	5.0.3	Editorial	Revised and edited the technical content.
12/05/2008	5.1	Minor	Updated the technical content.
01/16/2009	5.1.1	Editorial	Revised and edited the technical content.
02/27/2009	5.1.2	Editorial	Revised and edited the technical content.
04/10/2009	5.1.3	Editorial	Revised and edited the technical content.
05/22/2009	6.0	Major	Updated and revised the technical content.
07/02/2009	6.1	Minor	Updated the technical content.
08/14/2009	6.1.1	Editorial	Revised and edited the technical content.
09/25/2009	6.2	Minor	Updated the technical content.
11/06/2009	6.3	Minor	Updated the technical content.
12/18/2009	6.3.1	Editorial	Revised and edited the technical content.
01/29/2010	6.4	Minor	Updated the technical content.
03/12/2010	7.0	Major	Updated and revised the technical content.

Date	Revision History	Revision Class	Comments
04/23/2010	7.0.1	Editorial	Revised and edited the technical content.
06/04/2010	7.0.2	Editorial	Revised and edited the technical content.
07/16/2010	8.0	Major	Significantly changed the technical content.
08/27/2010	9.0	Major	Significantly changed the technical content.
10/08/2010	10.0	Major	Significantly changed the technical content.
11/19/2010	11.0	Major	Significantly changed the technical content.
01/07/2011	11.0	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	12.0	Major	Significantly changed the technical content.

Contents

1 Introduction

This document specifies the Group Policy: Security Protocol Extension to the Group Policy: Core Protocol, as specified in [MS-GPOL].

1.1 Glossary

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

Active Directory
Active Directory object
attribute
Augmented Backus-Naur Form (ABNF)
class
client
client-side extension GUID (CSE GUID)
discretionary access control list (DACL)
domain
domain controller (DC)
globally unique identifier (GUID)
Group Policy
Group Policy object (GPO)
Lightweight Directory Access Protocol (LDAP)
security identifier (SID)
security policy
security policy settings
share
Server Message Block (SMB)
system access control list (SACL)

The following terms are specific to this document:

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

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-ADSO] Microsoft Corporation, "Active Directory System Overview", July 2009.

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

[MS-KILE] Microsoft Corporation, "Kerberos Protocol Extensions", July 2006.

[MS-LSAD] Microsoft Corporation, "Local Security Authority (Domain Policy) Remote Protocol Specification", July 2006.

[MS-SAMR] Microsoft Corporation, "Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)", July 2006.

[MS-SCMR] Microsoft Corporation, "Service Control Manager Remote Protocol Specification", May 2007.

[MS-SMB] Microsoft Corporation, "Server Message Block (SMB) Protocol Specification", July 2006.

[MS-SMB2] Microsoft Corporation, "Server Message Block (SMB) Version 2 Protocol Specification", July 2006.

[MS-RRP] Microsoft Corporation, "Windows Remote Registry Protocol Specification", July 2006.

[MS-WSO] Microsoft Corporation, "Windows System Overview", January 2010.

[RFC1510] Kohl, J., and Neuman, C., "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993, http://www.ietf.org/rfc/rfc1510.txt

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

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

[RFC4234] Crocker, D., Ed., and Overell, P., "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, October 2005, http://www.ietf.org/rfc/rfc4234.txt

1.2.2 Informative References

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

[MSDN-INF] Microsoft Corporation, "About INF Files", http://msdn.microsoft.com/en-us/library/aa376858.aspx

[MSDN-PRIVS] Microsoft Corporation, "Authorization Constants", http://msdn.microsoft.com/en-us/library/aa375728.aspx

[MSDN-SDDL] Microsoft Corporation, "Security Descriptor String Format", http://msdn.microsoft.com/en-us/library/aa379570.aspx

[TECHNET-AUDITMGMT] Microsoft Corporation, "Audit Management", http://www.microsoft.com/technet/security/prodtech/windows2000/w2kccadm/auditman/w2kadm23.mspx

1.3 Overview

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.

1.3.1 Background

The Group Policy: Core Protocol, as specified in [MS-GPOL], enables clients to discover and retrieve policy settings created by administrators of **domains**. These settings are propagated within **Group**

Policy objects (GPOs) that are assigned to policy target accounts in **Active Directory**. Policy target accounts are either computer accounts or user accounts in Active Directory. Each client uses the **Lightweight Directory Access Protocol (LDAP)** to determine what GPOs are applicable to it by consulting the **Active Directory objects** corresponding to each client's computer account and the user accounts of any users logging on to the client computer.

On each client, each GPO is interpreted and acted on by software components known as client-side plug-ins. The client-side plug-ins responsible for a given GPO are specified by using an **attribute** on the GPO. This attribute specifies a list of **GUID** pairs. The first GUID of each pair is referred to as a **client-side extension GUID (CSE GUID)**. The second GUID of each pair is referred to as a tool extension GUID.

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

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

1.3.2 Security Extension Overview

Security policies contain settings (which the protocol configures) that enable underlying security components to enforce the following:

- Password, account lockout, and Kerberos policies.
- System audit settings.
- Privilege and rights assignments.
- Application security configuration data values and security descriptors.
- Event log settings.
- Security group membership.
- Configuration information of long-running processes and programs, and security descriptors on them.
- File and folder security descriptors.

The following major steps are for security configuration:

- Security policy authoring.
- Security policy assignment.
- Security policy distribution.

Security policy authoring is enabled through an administrative tool for the Group Policy: Core Protocol with an administrative plug-in for behavior specific to this protocol. The plug-in allows an administrator to author security policies within a user interface. The plug-in then saves the security policies into .inf files with a standard format, and stores them on a network location that is accessible by using the Server Message Block (SMB) Protocol, as specified in [MS-SMB].

Security policy assignment is performed by the Group Policy: Core Protocol administrative tool, which constructs GPOs, as specified in [MS-GPOL] section 2.2.8.1. Each GPO contains a reference to the network location containing the security policy files generated by the administrative-tool plug-in.

Security policy distribution involves a corresponding protocol-specific **Group Policy** plug-in on the client machine, which is invoked to process any GPO that refers to **security policy settings**. The security protocol client-side plug-in extracts the network location specified in the GPO, transfers the security policy files by using the **SMB** protocol, and then uses the security policy files to configure the client's security settings.

1.4 Relationship to Other Protocols

This protocol depends on Group Policy: Core Protocol as specified in [MS-GPOL]. It also depends on the SMB Protocol, as specified in [MS-SMB], for transmitting Group Policy settings and instructions between the client and the GP server.

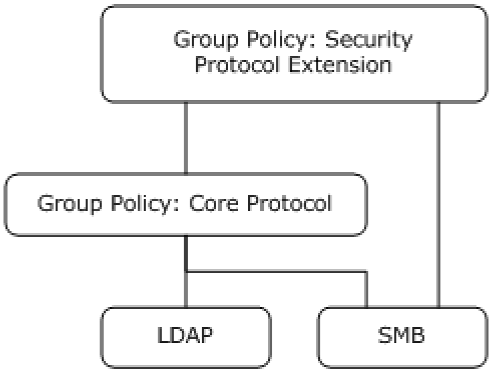
Group Policy: Security Protocol Extension
Group Policy: Core Protocol
LDAP
SMB

Figure 1: Group Policy: Host Security Configuration protocol relationship diagram

1.5 Prerequisites/Preconditions

The prerequisites for the Group Policy: Security Protocol Extension are the same as those for the Group Policy: Core Protocol.

1.6 Applicability Statement

The Group Policy: Security Protocol Extension is only applicable within the Group Policy framework.<1>

1.7 Versioning and Capability Negotiation

The Group Policy: Security Protocol Extension does not perform any explicit version checking on the received security policy.

1.8 Vendor-Extensible Fields

The Group Policy: Security Protocol Extension does not define any vendor-extensible fields.

1.9 Standards Assignments

The Group Policy: Security Protocol Extension defines CSE GUID and tool extension GUID, as specified in [MS-GPOL] section 1.8. The following table shows the assignments.

Parameter	Value
Client-side extension GUID	{827D319E-6EAC-11D2-A4EA-00C04F79F83A}
Tool extension GUID (computer policy settings)	{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}

2 Messages

2.1 Transport

The Group Policy: Security Protocol Extension MUST transport messages (in the form of files) over the Group Policy Protocol over SMB, as specified in [MS-SMB] section 1.3. The client-side plug-in MUST use this protocol's CSE GUID, and the administrative-tool plug-in MUST use the tool extension GUID.

The Group Policy: Core Protocol uses this protocol's CSE GUID and tool extension GUID values to invoke this protocol only to access GPOs that require processing by this protocol.<2>

2.2 Message Syntax

Messages exchanged in the Group Policy: Security Protocol Extension correspond to security policy files transferred by using the SMB Protocol. The protocol is driven through the exchange of these messages, as specified in section 3.

All security policy files processed by the Group Policy: Security Protocol Extension MUST be based on the .inf file syntax as follows.

```
InfFile = UnicodePreamble VersionPreamble Sections
UnicodePreamble = *("[Unicode]" LineBreak "Unicode=yes"
       LineBreak)
VersionPreamble = "[Version]" LineBreak "signature="
       DQUOTE "$CHICAGO$" DQUOTE LineBreak "Revision=1" LineBreak
Sections = Section /  Section Sections
Section = Header Settings
Header = "[" HeaderValue "]" LineBreak
HeaderValue = StringWithSpaces
Settings = Setting / Setting Settings
Setting = Key Wsp "=" Wsp ValueList LineBreak
ValueList = Value / Value Wsp "," Wsp ValueList
Key = String
Value = String / QuotedString
```

The preceding syntax is given in the **Augmented Backus-Naur Form (ABNF)** grammar, as specified in [RFC4234] and as augmented by the following rules.

```
LineBreak = CRLF
String = *(ALPHANUM / %d47 / %d45 / %d58 / %d59)
StringWithSpaces = String / String Wsp StringWithSpaces
QuotedString = DQUOTE *(%x20-21 / %x23-7E) DQUOTE
Wsp = *WSP
ALPHANUM = ALPHA / DIGIT
```

For more information about .inf files and their uses, see [MSDN-INF].

The protocol further restricts the values that can be assigned to HeaderValue. HeaderValue MUST be assigned one of the values listed in the following table.

HeaderValue	Purpose
System Access	MUST contain settings that pertain to account lockout, password policies, and local security options. For more information, see section 2.2.1.
Kerberos Policy	MUST contain settings that pertain to the Kerberos policy, as specified in [RFC1510]. For more information, see section 2.2.2.
System Log	MUST contain settings that pertain to maximum size, retention policy, and so on for the system log. For more information, see section 2.2.3.
Security Log	MUST contain settings that pertain to maximum size, retention policy, and so on for the security log. For more information, see section 2.2.3.
Application Log	MUST contain settings that pertain to maximum size, retention policy, and so on for the application log. For more information, see section 2.2.3.
Event Audit	MUST contain settings that pertain to audit policy. For more information, see section 2.2.4.
Registry Values	MUST contain registry values to be configured. For more information, see section 2.2.5.
Privilege Rights	MUST contain a list of privileges to be assigned to specific accounts. For more information, see section 2.2.6.
Service General Setting	MUST contain configuration settings that pertain to services. For more information, see section 2.2.7.
Registry Keys	MUST contain a list of registry keys and their corresponding security information to be applied. For more information, see section 2.2.8.
File Security	MUST contain a list of files, folders, and their corresponding security information to be applied. For more information, see section 2.2.9.
Group Membership	MUST contain group membership information, for example, what users should be part of what group. For more information, see section 2.2.10.

Note The plug-in that implements the client side of the protocol documented here does not understand the semantics of any of the (name, value) pairs it handles. Its operation is to set those named values in client-side stores indicated by the HeaderValue. When that client-side store is the Registry, the plug-in does not need to know the list of possible names for (name, value) pairs. This implies that new security settings stored in registry keys can be created and populated by GP. For other stores, the plug-in maintains a precompiled list of mappings from setting name to the application programming interface (API) used to apply the setting.

2.2.1 System Access

The following topics specify various types of system access settings. The ABNF for this section MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "System Access"
Settings = Setting / Setting Settings
Setting = Key Wsp "=" Wsp Value LineBreak
Key = String
Value = 1*DIGIT
```

2.2.1.1 Password Policies

This section defines settings that specify various supported password policies. The ABNF for valid keys that represent such policies MUST be as follows.

```
Key = "MinimumPasswordAge" / "MaximumPasswordAge" /
      "MinimumPasswordLength" / "PasswordComplexity" /
      "PasswordHistorySize" / "ClearTextPassword"

Value = 1*3DIGIT
```

The following table provides an explanation for each of the valid key values.

Note All numerical values are decimal unless explicitly specified otherwise or preceded by 0x.

Setting key	Explanation
MaximumPasswordAge	Maximum number of days that a password can be used before the client SHOULD require the user to change it. The value MUST be in the range 0 to 999. The value 0 indicates that a password never expires. If the maximum password age is not 0, the minimum password age MUST be less than the maximum password age.
MinimumPasswordAge	Number of days that a password can be used before the client MUST allow the user to change it from the date the password was changed or reset. This value MUST be between 0 and 998. The minimum password age MUST be less than the maximum password age, unless the maximum password age is set to 0.
MinimumPasswordLength	Minimum number of characters that a password for a user account MAY contain. This value MUST be between 0 and 14. A value of 0 indicates that no password is required.
PasswordComplexity	Flag that indicates whether the operating system MUST require that passwords meet complexity requirements. If this flag is set, it indicates that passwords MUST meet a specific minimum requirement. If this policy is enabled, passwords MUST meet the following minimum requirements: ▪ MUST NOT contain the user's account name or parts of the user's full name that exceed two consecutive characters. ▪ MUST be at least six characters in length. ▪ MUST contain characters from three of the following categories: ▪ English uppercase characters (A through Z). ▪ English lowercase characters (a through z). ▪ Base 10 digits (0 through 9). ▪ Nonalphanumeric characters (for example, !, $, #, %). Complexity requirements MUST be enforced when passwords are changed or created.
ClearTextPassword	Flag that indicates whether passwords MUST be stored by using reversible encryption.

Setting key	Explanation
	Passwords in a password database are typically stored encrypted. This encryption cannot normally be reversed. If there is a need to allow the encryption to be reversed, it is possible to enable Store password by using reversible encryption for all users in the domain. Then passwords MUST be stored with reversible encryption and can be recovered in case of emergency. Enabling this feature is not recommended. This policy provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords by using reversible encryption is essentially the same as storing plain-text versions of the passwords.
PasswordHistorySize	The number of unique new passwords that MUST be used before an old password MAY be reused in association with a user account. This value MUST be between 0 and 24. A value of 0 indicates that the password history is disabled. This policy enables administrators to enhance security by ensuring that old passwords are not reused continually.

2.2.1.2 Account Lockout Policies

This section defines settings that specify the configuration of account lockout duration. The ABNF for valid keys that represent such policies MUST be as follows.

```
Key = "LockoutBadCount" / "ResetLockoutCount" /
     "LockoutDuration"

Value = 1*5DIGIT
```

The following table provides an explanation for each of the valid key values.

Note All numerical values are decimal unless explicitly specified otherwise or preceded by 0x.

Setting key	Explanation
LockoutDuration	Number of minutes that a locked-out account MUST remain locked out before automatically becoming unlocked. The value MUST be greater than or equal to 0, and less than or equal to 99,999. If the account lockout duration is set to 0, the account MUST be locked out until an administrator explicitly unlocks it. If an account lockout threshold is defined, the account lockout duration MUST be greater than or equal to the reset time, ResetLockoutCount. This setting only has meaning when an account lockout threshold is specified.
LockoutBadCount	Number of failed logon attempts after which a user account MUST be locked out. A locked-out account MUST NOT be allowed to log on until it is reset by an administrator or until the lockout duration for the account has expired. The value MUST be between 0 and 999. A value of 0 indicates that the account is never to be locked out.
ResetLockoutCount	Number of minutes after a failed logon attempt that the account MUST be locked out. The value MUST be between 1 and 99,999. If an account lockout threshold is defined, this reset time MUST be less than or equal to the account lockout duration, LockoutDuration.

2.2.2 Kerberos Policy

This section defines settings that enable an administrator to configure user logon restrictions, as specified in [RFC1510].

The ABNF for this section MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "Kerberos Policy"
Settings = Setting /  Setting Settings
Setting = Key Wsp "=" Wsp Value LineBreak
Key = "MaxTicketAge" / "MaxRenewAge" / "MaxServiceAge" /
      "MaxClockSkew" / "TicketValidateClient"

Value = 1*3DIGIT
```

The following table provides an explanation for each of the valid key values.

Note All numerical values are decimal unless explicitly specified otherwise or preceded by 0x. The default values indicate Microsoft Windows®-specified defaults.

Setting key	Explanation
MaxServiceAge	Maximum amount of time (in minutes) that a granted session ticket MUST be valid to access a service or resource by using Kerberos before it expires. An expired ticket MUST NOT be accepted as a valid ticket for service or resource access. Details about Kerberos ticket authentication are as specified in [RFC1510]. The value MUST be greater than 10 and less than or equal to the setting for MaxTicketAge. Default: 600 minutes (10 hours).
MaxTicketAge	Maximum amount of time (in hours) that a user's ticket-granting ticket (TGT) MAY be used before it expires. An expired TGT MUST NOT be accepted as a valid TGT. Default: 10 hours.
MaxRenewAge	Period of time (in days) during which a user's TGT can be renewed. A TGT MUST NOT be renewed if it is more than MaxRenewAge days old. Default: 7 days.
MaxClockSkew	MUST be the maximum time difference (in minutes) between the client clock time and the clock time of the server that provides Kerberos v5 authentication, as specified in [RFC1510]. Default: 5 minutes.
TicketValidateClient	A flag that determines whether the Kerberos v5 Key Distribution Center (KDC) MUST validate every request for a session ticket against the user rights policy of the user account. Validation of each request for a session ticket is optional because the extra step takes time and may slow network access to services. Default: enabled.

2.2.3 Event Log Policies

There are three types of event log policies:

- System log
- Security log
- Application log

The ABNF for each of them MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "System Log" / "Security Log" / "Application Log"
Settings = Setting / Setting Settings
Setting = Key Wsp "=" Wsp Value LineBreak
Key = "MaxLogSize" / "LogRetentionPeriod"
      / "LogRetentionDays" / "LogRestrictGuest"

Value = 1*3DIGIT
```

The following table provides an explanation for each of the valid key values.

Note All numerical values are decimal unless explicitly specified otherwise, or unless preceded by 0x.

Setting key	Explanation
MaxLogSize	The log size, in kilobytes, MUST be less than or equal to this value.
LogRetentionPeriod	Specifies the type of retention period to be applied to the specific log. The retention method MUST be one of the following: ▪ A value of "0": Indicates to overwrite events as needed. ▪ A value of "1": Indicates to overwrite events as specified by the LogRetentionDays entry. ▪ A value of "2": Indicates to never overwrite events (clear log manually).
LogRetentionDays	The number of days that System, Security, and Application log events MUST be retained before being overwritten by new events. Only valid if option LogRetentionPeriod = 1. The value MUST be between 1 and 365.
LogRestrictGuest	A flag that indicates whether or not users with Guest privileges can have access to System, Security, and Application logs.

2.2.4 Event Audit Policies

This section defines settings that enable an administrator to enforce audit account logon events. The syntax for the entries in this category MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "Event Audit"
Settings = Setting / Setting Settings
Setting = Key Wsp "=" Wsp Value Linebreak
Key = "AuditSystemEvents" / "AuditLogonEvents" / "AuditPrivilegeUse" /
 "AuditPolicyChange" / "AuditAccountManage" / "AuditProcessTracking" /
 "AuditDSAccess" / "AuditObjectAccess" / "AuditAccountLogon"

Value = 1*DIGIT
```

The following table provides an explanation for the valid keys as specified in [MS-LSAD] section 2.2.4.20.

Note All numerical values are decimal unless explicitly specified otherwise, or unless preceded by 0x.

For more information about the format for the audit events, see [TECHNET-AUDITMGMT].

Setting key	Explanation
AuditAccountManage	A flag that indicates whether the operating system MUST audit each event of account management on a computer.
AuditDSAccess	A security setting that determines whether the operating system MUST audit each instance of user attempts to access an Active Directory object that has its own **system access control list (SACL)** specified, if the type of access request (such as Write, Read, or Modify) and the account making the request, match the settings in the SACL. The administrator can specify to audit only successes, only failures, both successes and failures, or to not audit these events at all (that is, neither successes nor failures). If Success auditing is enabled, an audit entry MUST be logged each time any user successfully accesses an Active Directory object that has a matching SACL specified. If Failure auditing is enabled, an audit entry MUST be logged each time any user unsuccessfully attempts to access a Active Directory object that has a matching SACL specified.
AuditAccountLogon	A security setting that determines whether the operating system MUST audit each time this computer validates the credentials of an account. Account logon events are generated whenever a computer validates the credentials of one of its local accounts. The credential validation can be in support of a local logon, or in the case of an Active Directory domain account on a **domain controller (DC)**, can be in support of a logon to another computer. Audited events for local accounts MUST be logged on the local security log of the computer. Account log off does not generate an event that can be audited. If this policy setting is defined, the administrator can specify to audit only successes, only failures, both successes and failures, or to not audit these events at all (that is, neither successes nor failures).
AuditLogonEvents	A security setting that determines whether the operating system MUST audit each instance of a user attempt to log on or log off this computer. Logoff events are generated whenever the logon session of a logged-on user account is terminated. If this policy setting is defined, the administrator can specify to audit only successes, only failures, both successes and failures, or to not audit these events at all (that is, neither successes nor failures).
AuditObjectAccess	A security setting that determines whether the operating system MUST audit each instance of user attempts to access a non-Active Directory object that has its own SACL specified, if the type of access request (such as Write, Read, or Modify) and the account making the request, match the settings in the SACL. The administrator can specify to audit only successes, only failures, both successes and failures, or to not audit these events at all (that is, neither successes nor failures). If Success auditing is enabled, an audit entry MUST be logged each time any user successfully accesses a non-Active Directory object that has a matching SACL specified. If Failure auditing is enabled, an audit entry MUST be logged each time any user unsuccessfully attempts to access a non-Active Directory object that has a matching SACL specified.
AuditPolicyChange	A security setting that determines whether the operating system MUST audit each instance of user attempts to change user rights assignment policy, audit policy, account policy, or trust policy. The administrator can specify to audit only successes, only failures, both successes and failures, or to not audit these events at all (that is, neither successes nor failures). If Success auditing is enabled, an audit entry MUST be logged when an attempted change to user rights assignment policy, audit policy, or trust policy is successful. If Failure auditing is enabled, an audit entry MAY be logged when a change to user rights assignment policy, audit policy, or trust policy is attempted by an account that is not authorized to make

Setting key	Explanation
	the requested policy change.<3>
AuditPrivilegeUse	A security setting that determines whether the operating system MUST audit each instance of user attempts to exercise a user right. If this policy setting is defined, the administrator can specify to audit only successes, only failures, both successes and failures, or to not audit these events at all (that is, neither successes nor failures). If Success auditing is enabled, an audit entry MUST be logged each time the exercise of a user right succeeds. If Failure auditing is enabled, an audit entry MUST be logged each time the exercise of a user right fails because the user account is not assigned to the user right.
AuditProcessTracking	A security setting that determines whether the operating system MUST audit process-related events such as process creation, process termination, handle duplication, and indirect object access. If this policy setting is defined, the administrator can specify to audit only successes, only failures, both successes and failures, or to not audit these events at all (that is, neither successes nor failures). If Success auditing is enabled, an audit entry MUST be logged each time the operating system performs one of these process-related activities. If Failure auditing is enabled, an audit entry MAY be logged each time the operating system fails to perform one of these process-related activities.<4>
AuditSystemEvents	A security setting that determines whether the operating system MUST audit any of the following events: ▪ Attempted system time change. ▪ Attempted security system startup or shutdown. ▪ Attempt to load extensible authentication components. ▪ Loss of audited events due to auditing system failure. ▪ Security log size exceeding a configurable warning threshold level. If this policy setting is defined, the administrator can specify to audit only successes, only failures, both successes and failures, or to not audit these events at all (that is, neither successes nor failures). If Success auditing is enabled, an audit entry MUST be logged each time the operating system performs one of these activities successfully. If Failure auditing is enabled, an audit entry MUST be logged each time the operating system attempts and fails to perform one of these activities.

The following table provides a summary of the valid values. For more details on valid values see [MS-LSAD] section 2.2.4.4.

Setting value	Explanation
0	Indicates that this setting is set to None.
1	Indicates that this setting is set to Success Audits Only.
2	Indicates that this setting is set to Failure Audits Only.
3	Indicates that this setting is set to Success and Failure Audits.

2.2.5 Registry Values

This section defines settings that enable an administrator to set registry entries. The syntax for the entries in this category MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "Registry Values"
Settings = Setting / Setting Settings
Setting = RegistryValueName "," RegistryValueType "," RegistryValue
RegistryValueType = 1*DIGIT
RegistryValueName = String
RegistryValue = String / QuotedString
```

The following table provides an explanation for each of the parameters listed.

Note All numerical values are decimal unless explicitly specified otherwise or preceded by 0x.

Setting key	Explanation
RegistryValueName	MUST be the full name of the registry value to set, for example, MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects.
RegistryValueType	The data type of the registry value MUST be one of the following values (For more details about the value types see [MS-RRP] section 3.1.1.5): ▪ A value of "1": Indicates that the data type of the registry value is String. ▪ A value of "2": Indicates that the data type of the registry value is Expand String. ▪ A value of "3": Indicates that the data type of the registry value is Binary. ▪ A value of "4": Indicates that the data type of the registry values is **DWORD**. Although other registry types exist, they are not supported by this protocol.
RegistryValue	A value to be configured. The data type of this value MUST match the type that is specified in the **RegistryValueType** field.

2.2.6 Privilege Rights

This section defines settings that enable an administrator to control what accounts have what privileges. The syntax for the entries in this category MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "Privilege Rights"
Settings = Setting / Setting Settings
Setting = RightName Wsp "=" Wsp SidList LineBreak
ValueList = SidEnt / SidEnt Wsp "," Wsp SidList
Value = USERSID

RightName = "SeNetworkLogonRight" / "SeTcbPrivilege"
      / "SeMachineAccountPrivilege" / "SeIncreaseQuotaPrivilege"
      / "SeRemoteInteractiveLogonRight" / "SeBackupPrivilege"
      / "SeChangeNotifyPrivilege" / "SeCreatePagefilePrivilege"
      / "SeSystemtimePrivilege" / "SeCreateTokenPrivilege"
      / "SeCreateGlobalPrivilege" / "SeCreatePermanentPrivilege"
```

```
         / "SeDebugPrivilege" / "SeDenyNetworkLogonRight"
         / "SeDenyBatchLogonRight" / "SeDenyServiceLogonRight"
         / "SeDenyInteractiveLogonRight"
         / "SeDenyRemoteInteractiveLogonRight"
         / "SeEnableDelegationPrivilege"
         / "SeRemoteShutdownPrivilege" / "SeAuditPrivilege"
         / "SeImpersonatePrivilege"
         / "SeIncreaseBasePriorityPrivilege"
         / "SeLoadDriverPrivilege" / "SeLockMemoryPrivilege"
         / "SeBatchLogonRight" / "SeServiceLogonRight"
         / "SeInteractiveLogonRight" / "SeSecurityPrivilege"
         / "SeSystemEnvironmentPrivilege"
         / "SeManageVolumePrivilege"
         / "SeProfileSingleProcessPrivilege"
         / "SeSystemProfilePrivilege" / "SeUndockPrivilege"
         / "SeAssignPrimaryTokenPrivilege" / "SeRestorePrivilege"
         / "SeShutdownPrivilege" / "SeSyncAgentPrivilege"
         / "SeTakeOwnershipPrivilege"

   USERSID = String
```

For information about each privilege setting, see [MSDN-PRIVS].

USERSID is the string representation of the **security identifiers (SIDs)** of accounts or groups.

2.2.7 Registry Keys

This section defines settings that enable an administrator to specify how registry keys on the client machine should be protected. The ABNF syntax for the entries in this category MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "Registry Keys"
Settings = Setting / Setting Settings
Setting = RegistryKeyName "," PermPropagationMode ","
          AclString LineBreak
RegistryKeyName = String
PermPropagationMode = DIGIT
AclString = String
```

The following table provides an explanation for each of the parameters listed.

Note All numerical values are decimal unless explicitly specified otherwise, or unless preceded by 0x.

Setting key	Explanation
RegistryKeyName	The full name of the registry key that MUST be protected.
PermPropagationMode	Controls whether and how permissions are propagated. It MUST be one of the following values: ▪ A value of "0": MUST propagate inheritable permissions to all subkeys. ▪ A value of "1": MUST replace existing permissions on all subkeys with inheritable permissions.

Setting key	Explanation
	▪ A value of "2": MUST NOT allow permissions on this key to be replaced.
AclString	A security descriptor that MUST be applied to the registry key. For more information, see [MSDN-SDDL].

2.2.8 Service General Settings

This section defines settings that enable configuration of the startup type and **discretionary access control lists (DACLs)** on services running on the client machine. The syntax for the entries in this category MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "Service General Setting"
Settings = Setting / Setting Settings
Setting = ServiceName ","  StartupMode "," AclString LineBreak
ServiceName = String
StartupMode = DIGIT
AclString = String
```

The following table explains the **ServiceName**, **StartupMode**, and **AclString** fields.

Note All numerical values are decimal unless explicitly specified otherwise, or unless preceded by 0x.

Setting key	Explanation
ServiceName	A string that represents the logical service name of the service that MUST be configured.
StartupMode	A startup mode for the process that MUST be one of the following values (the following explanations are a summary; for more details see [MS-SCMR] section 2.2.15): ▪ A value of "2": Indicates that the startup mode is Automatic. ▪ A value of "3": Indicates that the startup mode is Manual. ▪ A value of "4": Indicates that the startup mode is Disabled.
AclString	A security descriptor that MUST be applied to the service. For more information, see [MSDN-SDDL].

2.2.9 File Security

This section defines how to enable the administrator to specify how files and directories on the client machine should be protected. The ABNF syntax for the entries in this category MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "File Security"
Settings = Setting / Setting Settings
Setting = FileOrDirectoryPath ","  PermPropagationMode
          "," AclString LineBreak
FileOrDirectoryPath = String
PermPropagationMode = DIGIT
```

```
AclString = String
```

The following table explains each of the settings listed.

Note All numerical values are decimal unless explicitly specified otherwise, or unless preceded by 0x.

Setting key	Explanation
FileOrDirectoryPath	The path to the file or directory that MUST be protected.
PermPropagationMode	Controls whether and how permissions are propagated. It MUST be one of the following values: ▪ A value of "0": MUST propagate inheritable permissions to all subfolders and files. ▪ A value of "1": MUST replace existing permissions on all subfolders and files with inheritable permissions. ▪ A value of "2": MUST NOT allow permissions on this file or folder to be replaced.
AclString	A security descriptor that MUST be applied to the file or directory. For more information, see [MSDN-SDDL].

2.2.10 Group Membership

This section defines settings that enable the administrator to control the membership of various groups. The ABNF syntax for the entries in this category MUST be as follows.

```
Header = "[" HeaderValue "]" LineBreak
HeaderValue = "Group Membership"
Settings = Setting / Setting Settings
Setting = Key Wsp "=" Wsp ValueList LineBreak
Key = GroupNameMembers / GroupNameMemberOf
GroupNameMembers = GroupName "__Members"
GroupNameMemberof = GroupName "__Memberof"
ValueList = Value / Value Wsp "," Wsp ValueList
Value = SID / GroupName
GroupName = String
```

Note that in the actual security policy, the preceding "GroupName" setting MUST be replaced by the actual name of a group whose members or membership in other groups MUST be configured. For more information, see the example in section 4.3.

The following table explains each of the settings listed.

Setting key	Explanation
GroupName__Members	GroupName MUST be the name of the group that contains users represented by the SIDs specified in the value field.
GroupName__Memberof	The group, GroupName, MUST be a member of the groups listed in the value field.

Setting key	Explanation
Value	MUST be the SID of users or names of other groups.

2.2.11 User Account Control

This section defines settings that enable the administrator to configure the behavior of the User Account Control feature. For details on how the settings listed in this section SHOULD be defined, see sections 2.2.5 and 2.2.7.<5>

2.2.11.1 FilterAdministratorToken

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: "FilterAdministratorToken"

Type: REG_DWORD

Size: 2

Data: This MUST be a value in the following table.

Value	Meaning
0x00000000	Only the built-in administrator account (RID 500) MUST be placed into Full Token or Windows® XP operating system native mode.
0x00000001	Only the built-in administrator account (RID 500) MUST be placed into Admin Approval Mode. Approval is required when performing administrative tasks.

2.2.11.2 ConsentPromptBehaviorAdmin

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: "ConsentPromptBehaviorAdmin"

Type: REG_DWORD

Size: 3

Data: This MUST be a value in the following table.

Value	Meaning
0x00000000	This option SHOULD be used to allow the Consent Admin to perform an operation that requires elevation without consent or credentials.
0x00000001	This option SHOULD be used to prompt the Consent Admin to enter his or her user name and password (or another valid admin) when an operation requires elevation of privilege.
0x00000002	This option SHOULD be used to prompt the administrator in Admin Approval Mode to select either "Permit" or "Deny" an operation that requires elevation of privilege. If the Consent Admin selects Permit, the operation will continue with their highest available privilege. "Prompt for consent" removes the inconvenience of requiring that users enter their name and password to perform a privileged task.

2.2.11.3 ConsentPromptBehaviorUser

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: "ConsentPromptBehaviorUser"

Type: REG_DWORD

Size: 2

Data: This MUST be a value in the following table.

Value	Meaning
0x00000000	This option SHOULD be set to ensure that any operation that requires elevation of privilege will fail as a standard user.
0x00000001	This option SHOULD be set to ensure that a standard user that needs to perform an operation that requires elevation of privilege will be prompted for an administrative user name and password. If the user enters valid credentials, the operation will continue with the applicable privilege.

2.2.11.4 EnableInstallerDetection

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: "EnableInstallerDetection"

Type: REG_DWORD

Size: 2

Data: This MUST be a value in the following table.

Value	Meaning
0x00000000	This option SHOULD be used to disable the automatic detection of installation packages that require elevation to install.
0x00000001	This option SHOULD be used to heuristically detect applications that require an elevation of privilege to install.

2.2.11.5 ValidateAdminCodeSignatures

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: "ValidateAdminCodeSignatures"

Type: REG_DWORD

Data: This MUST be a value in the following table.

Value	Meaning
0x00000000	Do not enforce cryptographic signatures on interactive applications that require elevation of privilege.

Value	Meaning
0x00000001	Enforce cryptographic signatures on any interactive application that requests elevation of privilege.

2.2.11.6 EnableLUA

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: "EnableLUA"

Type: REG_DWORD

Data: This MUST be a value in the following table.

Value	Meaning
0x00000000	Disabling this policy disables the "administrator in Admin Approval Mode" user type.
0x00000001	This policy enables the "administrator in Admin Approval Mode" user type while also enabling all other User Account Control (UAC) policies.

2.2.11.7 PromptOnSecureDesktop

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: "PromptOnSecureDesktop"

Type: REG_DWORD

Data: This MUST be a value in the following table.

Value	Meaning
0x00000000	Disabling this policy disables secure desktop prompting. All credential or consent prompting will occur on the interactive user's desktop.
0x00000001	This policy will force all UAC prompts to happen on the user's secure desktop.

2.2.11.8 EnableVirtualization

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Value: "EnableVirtualization"

Type: REG_DWORD

Data: This MUST be a value in the following table.

Value	Meaning
0x00000000	Disables data redirection for interactive processes.
0x00000001	This policy enables the redirection of legacy application File and Registry writes that would normally fail as standard user to a user-writable data location. This setting mitigates problems with applications that historically ran as administrator and wrote

Value	Meaning
	run-time application data back to locations writable only by an administrator.

3 Protocol Details

3.1 Administrative-Side Plug-in Details

The administrative-side plug-in participates in the security policy authoring and assignment steps, as specified in section 2. The security policy MUST be stored as a text file by using an .inf format, as specified in section 2.2. The security policies MUST be stored in a location accessible over the network (such as a network **share**) by using SMB.

3.1.1 Abstract Data Model

The administrative-side plug-in maintains no state. It loads all the settings, as specified in section 2.2, in a <*name of setting, value of setting*> pair in memory.

When using the administrative UI, the administrative-side plug-in is used to interact with the Group Policy framework, as specified in [MS-GPOL]. It determines the physical location of the security policy wanted based on the abstract data model, creates a new policy or opens an existing policy as appropriate, and displays it to the administrator. After the administrator modifies the policy, the changes MUST be propagated back into the policy at the location wanted.

3.1.2 Timers

None.

3.1.3 Initialization

When the administrative-side plug-in starts up, it MUST get a scoped GPO path from the Group Policy: Core Protocol portion. The plug-in MUST attempt to retrieve any existing gpttmpl.inf file from <*gpo path*>\SecEdit\GptTmpl.inf where <*gpo path*> is the scoped GPO path. File reads MUST be performed, as specified in [MS-GPOL] section 2.2.7. If the attempt to recover the file fails, an error MUST be logged and processing stopped.

The process for reading the settings from the GPO for administrative purposes MUST be the same as those as specified in section 3.2.5, steps 1-3.

3.1.4 Higher-Layer Triggered Events

For both viewing and editing settings, the administrative-side plug-in MUST first open the specified GPO by using APIs conformant with the Group Policy: Core Protocol. The plug-in MUST attempt to copy a gpttmpl.inf file with the settings from the following location (for viewing) or to the following location (for editing): <*gpo path*>\SecEdit\GptTmpl.inf (where <*gpo path*> is the user-scoped GPO path), if the GPO user settings are being viewed/updated, or the computer-scoped GPO path, if the computer settings are being viewed/updated. File copies MUST be performed, as specified in [MS-GPOL] section 3.3. File names and paths SHOULD be regarded as case-insensitive. If the copy fails, the administrative-side plug-in MUST display to the user that the operation failed.

3.1.5 Message Processing Events and Sequencing Rules

None.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Client-Side Plug-in Details

The client-side plug-in interacts with the Group Policy framework, as specified in [MS-GPOL] section 3.2. This plug-in MUST receive the security policy and apply it in accordance with the instructions of the administrator.

3.2.1 Abstract Data Model

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

MS-GPSB sets shared Abstract Data Model variables that are defined in other protocol documents. The normative definition for each shared variable is given in the corresponding document as shown here:

MS-GPSB sets the following abstract data variables shared from [MS-SAMR] section 3.1.1.3:

- maxPwdAge ([MS-SAMR] section 3.1.1.3)
- minPwdAge ([MS-SAMR] section 3.1.1.3)
- minPwdLength ([MS-SAMR] section 3.1.1.3)
- pwdProperties ([MS-SAMR] section 3.1.1.3)
- pwdHistoryLength ([MS-SAMR] section 3.1.1.3)
- lockoutDuration ([MS-SAMR] section 3.1.1.3)
- lockoutThreshold ([MS-SAMR] section 3.1.1.3)
- lockoutObservationWindow ([MS-SAMR] section 3.1.1.3)

MS-GPSB sets the following abstract data variables shared from [MS-LSAD]:

- MaxServiceTicketAge ([MS-LSAD] section 3.1.1.1)
- MaxTicketAge ([MS-LSAD] section 3.1.1.1)
- MaxRenewAge ([MS-LSAD] section 3.1.1.1)
- MaxClockSkew ([MS-LSAD] section 3.1.1.1)
- AuthenticationOptions ([MS-LSAD] section 3.1.1.1)

MS-GPSB sets the following abstract data variables shared from [MS-EVEN6]:

- Prop 8 (MaxSize) ([MS-EVEN6] section 3.1.4.21)
- Prop 6 (Retention) ([MS-EVEN6] section 3.1.4.21)
- Prop 1 (Channel Isolation) ([MS-EVEN6] section 3.1.4.21)

3.2.2 Timers

None.

3.2.3 Initialization

When invoked by the Group Policy framework with a list of one or more applicable GPOs, the client-side plug-in MUST do the following: locate all the physical security policies within those GPOs, copy the policies to the local machine, read the policies, and apply them as specified in section 3.2.5.

Locating physical security policy files MUST be done by using the Group Policy: Core Protocol, as specified in [MS-GPOL] section 3.2.5.1, and the LDAP search protocol, as specified in [RFC2251] section 4.5. The policy files MUST be copied and read by using standard CopyFile and ReadFile functions, as specified in [MS-SMB].<6>

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

The client-side plug-in GPOs MUST be triggered by the Group Policy framework whenever applicable GPOs need to be processed, as specified in section 3.1.1. When such an event occurs, the client-side plug-in takes the appropriate actions.

When triggered, the client-side plug-in expects a list of applicable GPOs. It MUST then go through this list and, for each GPO, locate and retrieve the contained security policy.

After all the security policies are retrieved, each policy MUST be opened and the contained security policy settings MUST be extracted and applied.

When the policy application step is completed, an appropriate error code MUST be returned to the Group Policy framework, as specified in [MS-GPOL], to indicate the success or failure of the operation.

The Group Policy: Core Protocol MUST invoke the client-side plug-in for each GPO that it identifies as containing Group Policy: Security Protocol Extension protocol settings. For each of those GPOs, one file with the format (as specified in section 2.2) MUST be copied from the Group Policy: Core Protocol server. If any file cannot be read, the client-side plug-in MUST ignore the failure and continue to copy files for other GPOs.

The Group Policy: Core Protocol client MUST determine a list of GPOs for which this protocol MUST be executed, as specified in [MS-GPOL] section 3.3.5.

For each GPO, the client-side plug-in MUST do the following:

1. Perform an SMB File Open on the file specified by <*gpo path*>\SecEdit\GptTmpl.inf (where <*gpo path*> is the scoped GPO path in the GPO). If an error is encountered while opening the file, an error MUST be indicated to the Group Policy system (as specified in [MS-GPOL] section 2.2.7) on the client machine and processing MUST be stopped.

2. Perform a series of SMB File Reads to read the entire contents of the opened file until the entire file has been read or an error in reading occurs. If an error is encountered while reading the file, an error MUST be indicated to the Group Policy system (as specified in [MS-GPOL]) on the client machine and processing MUST be aborted.

3. Perform an SMB File Close to close the file.

When using SMB to open or read files as described in the preceding steps, the client-side plug-in MUST be prepared to handle error codes returned by the SMB protocol as specified in [MS-SMB] section 2.2.2.4 or [MS-SMB2].

The client-side plug-in MUST parse the file according to the format specified in section 2.2. If the file does not conform to that format, the entire configuration operation MUST be ignored. If the file does conform to that format, the settings MUST be applied to the corresponding security parameters on the system.

In applying security policies, several MS-GPSB setting names correspond to Abstract Data Model shared variables for which the normative definition is provided in other documents (see the "Abstract Data Model" section 3.2.1.) The MS-GPSB setting name and the corresponding Abstract Data Model shared variable are provided in the following tables. For each such setting that is read from a GPO .inf file, the client-side plug-in MUST set the value of the ADM variable in the right-hand column of the table to the value for the setting in the left-hand column.

3.2.5.1 Password Policies

The settings in Password Policies (section 2.2.1.1) correspond to the ADM in [MS-SAMR] section 3.1.1.3 according to the following table. For the **PasswordComplexity** and **ClearTextPassword** settings, if the setting in the GPO .inf file has a value of "true", then the client-side plug-in MUST set the named bit in the ADM variable named in the right-hand column.

MS-GPSB	MS-SAMR
MaximumPasswordAge	maxPwdAge
MinimumPasswordAge	minPwdAge
MinimumPasswordLength	minPwdLength
PasswordComplexity	pwdProperties bit DOMAIN_PASSWORD_COMPLEX
ClearTextPassword	pwdProperties bit DOMAIN_PASSWORD_STORE_CLEARTEXT
PasswordHistorySize	pwdHistoryLength

3.2.5.2 Account Lockout Policies

The settings in Account Lockout Policies (section 2.2.1.2) correspond to the ADM in [MS-SAMR] section 3.1.1.3 according to the following table.

MS-GPSB	MS-SAMR
LockoutDuration	lockoutDuration
LockoutBadCount	lockoutThreshold
ResetLockoutCount	lockoutObservationWindow

3.2.5.3 Kerberos Policy

Settings in Kerberos Policy (section 2.2.2) correspond to the Abstract Data Model as specified in [MS-LSAD] section 3.1.1.1, according to the following table. For the **TicketValidateClient** setting, if the setting in the GPO .inf file has a value of "true", then the client-side plug-in MUST set the named bit in the ADM variable in the right-hand column.

MS-GPSB	MS-LSAD
MaxServiceAge	MaxServiceTicketAge
MaxTicketAge	MaxTicketAge
MaxRenewAge	MaxRenewAge
MaxClockSkew	MaxClockSkew
TicketValidateClient	AuthenticationOptions bit POLICY_KERBEROS_VALIDATE_CLIENT

3.2.5.4 Event Log Policies

Settings in Event Log Policies (section 2.2.3) are mapped to the Abstract Data Model as specified in [MS-EVEN6] section 3.1.4.21, according to the following table.

MS-GPSB	MS-EVEN6
MaxLogSize	Prop 8 - MaxSize
LogRetentionPeriod	Prop 6 – Retention
LogRestrictGuest	Prop 1 - Channel Isolation

3.2.5.5 Event Audit Policies

Settings in Event Audit Policies (section 2.2.4) MUST be set by performing the external behavior consistent with locally invoking **LsarSetInformationPolicy (section 3.1.4.4.6)** ([MS-LSAD] section 3.1.4.4.6).

- The *PolicyHandle* MUST be set to a policy handle opened by performing external behavior consistent with locally invoking **LsarOpenPolicy (section 3.1.4.4.2)** ([MS-LSAD] section 3.1.4.4.2).
- The InformationClass MUST be set to PolicyAuditEventsInformation.
- The *Buffers* MUST be set with the settings in Event Audit Policies where the keys are mapped to the enumeration ([MS-LSAD] section 2.2.4.20) according to the following table.

MS-GPSB	MS-LSAD
AuditAccountManage	AuditCategoryAccountManagement
AuditDSAccess	AuditCategoryDirectoryServiceAccess
AuditAccountLogon	AuditCategoryAccountLogon
AuditLogonEvents	AuditCategoryLogon
AuditObjectAccess	AuditCategoryObjectAccess
AuditPolicyChange	AuditCategoryPolicyChange

MS-GPSB	MS-LSAD
AuditPrivilegeUse	AuditCategoryPrivilegeUse
AuditProcessTracking	AuditCategoryDetailedTracking
AuditSystemEvents	AuditCategorySystem

In addition, the values of the settings (section 2.2.4) are mapped to the values of the EventAuditingOptions array ([MS-LSAD] section 2.2.4.4) according to the following table.

MS-GPSB	MS-LSAD
0	POLICY_AUDIT_EVENT_NONE
1	POLICY_AUDIT_EVENT_SUCCESS | POLICY_AUDIT_EVENT_NONE
2	POLICY_AUDIT_EVENT_FAILURE | POLICY_AUDIT_EVENT_NONE
3	POLICY_AUDIT_EVENT_SUCCESS | POLICY_AUDIT_EVENT_FAILURE |POLICY_AUDIT_EVENT_NONE

3.2.5.6 Registry Values

Settings in Registry Values (section 2.2.5) MUST be set by adding registry values.

Registry values MUST be added by performing the external behavior consistent with locally invoking **BaseRegSetValue (section 3.1.5.22)** ([MS-RRP] section 3.1.5.22) for each setting.

- The *hKey* MUST be set to a registry key handle opened by performing external behavior consistent with locally invoking **BaseRegCreateKey (section 3.1.5.7)** ([MS-RRP] section 3.1.5.7) using the portion of the RegistryValueName of the Setting prior to the last '\'.
- The *lpValueName* MUST be set to the final portion of the RegistryValueName of the setting after the last '\'.
- The *dwType* MUST be set to the RegistryValueType of the setting.
- The *lpData* MUST be set to the RegistryValue of the setting.
- The *cbData* MUST be set to the length in bytes of the RegistryValue of the setting.

3.2.5.7 Privilege Rights

Settings in Privilege Rights (section 2.2.6) MUST be set by adding privilege rights.

Privilege rights are added by performing the external behavior consistent with locally invoking LsarAddAccountRights [MS-LSAD] section 3.1.4.5.12) for each SidEnt in a setting.

- The *PolicyHandle* MUST be set to a policy handle opened by performing external behavior consistent with locally invoking LsarOpenPolicy ([MS-LSAD] section 3.1.4.4.2.
- The *AccountSid* MUST be set to the value of SidEnt for the setting.
- The *UserRights* MUST be set to the value of a RightName in Privilege Rights (section 2.2.6) where the values are mapped to the constants according to the following table (provided here for

convenience, the normative description of these mappings is described in the Privilege Data Model ([MS-LSAD] section 3.1.1.2.1) and the System Access Rights Data Model ([MS-LSAD] section 3.1.1.2.2).

MS-GPSB RightName	UserRights Parameter Value
SeNetworkLogonRight	SeNetworkLogonRight
SeTcbPrivilege	SE_TCB_NAME
SeMachineAccountPrivilege	SE_MACHINE_ACCOUNT_NAME
SeIncreaseQuotaPrivilege	SE_INCREASE_QUOTA_NAME
SeRemoteInteractiveLogonRight	SeRemoteInteractiveLogonRight
SeBackupPrivilege	SE_BACKUP_NAME
SeChangeNotifyPrivilege	SE_CHANGE_NOTIFY_NAME
SeCreatePagefilePrivilege	SE_CREATE_PAGEFILE_NAME
SeSystemtimePrivilege	SE_SYSTEMTIME_NAME
SeCreateTokenPrivilege	SE_CREATE_TOKEN_NAME
SeCreateGlobalPrivilege	SE_CREATE_GLOBAL_NAME
SeCreatePermanentPrivilege	SE_CREATE_PERMANENT_NAME
SeDebugPrivilege	SE_DEBUG_NAME
SeDenyNetworkLogonRight	SeDenyNetworkLogonRight
SeDenyBatchLogonRight	SeDenyBatchLogonRight
SeDenyServiceLogonRight	SeDenyServiceLogonRight
SeDenyInteractiveLogonRight	SeDenyInteractiveLogonRight
SeDenyRemoteInteractiveLogonRight	SeDenyRemoteInteractiveLogonRight
SeEnableDelegationPrivilege	SE_ENABLE_DELEGATION_NAME
SeRemoteShutdownPrivilege	SE_REMOTE_SHUTDOWN_NAME
SeAuditPrivilege	SE_AUDIT_NAME
SeImpersonatePrivilege	SE_IMPERSONATE_NAME
SeIncreaseBasePriorityPrivilege	SE_INC_BASE_PRIORITY_NAME
SeLoadDriverPrivilege	SE_LOAD_DRIVER_NAME
SeLockMemoryPrivilege	SE_LOCK_MEMORY_NAME
SeBatchLogonRight	SeBatchLogonRight
SeServiceLogonRight	SeServiceLogonRight

MS-GPSB RightName	UserRights Parameter Value
SeInteractiveLogonRight	SeInteractiveLogonRight
SeSecurityPrivilege	SE_SECURITY_NAME
SeSystemEnvironmentPrivilege	SE_SYSTEM_ENVIRONMENT_NAME
SeManageVolumePrivilege	SE_MANAGE_VOLUME_NAME
SeProfileSingleProcessPrivilege	SE_PROF_SINGLE_PROCESS_NAME
SeSystemProfilePrivilege	SE_SYSTEM_PROFILE_NAME
SeUndockPrivilege	SE_UNDOCK_NAME
SeAssignPrimaryTokenPrivilege	SE_ASSIGNPRIMARYTOKEN_NAME
SeRestorePrivilege	SE_RESTORE_NAME
SeShutdownPrivilege	SE_SHUTDOWN_NAME
SeSyncAgentPrivilege	SE_SYNC_AGENT_NAME
SeTakeOwnershipPrivilege	SE_TAKE_OWNERSHIP_NAME

3.2.5.8 Registry Keys

Settings in Registry Keys (section 2.2.7) MUST be set by applying security descriptors on registry keys for each setting.

Security descriptors MUST be applied to registry keys by performing the external behavior consistent with locally invoking **BaseRegSetKeySecurity (section 3.1.5.21)** ([MS-RRP] section 3.1.5.21) for each Setting.

- The *hKey* MUST be set to a registry key handle opened by performing external behavior consistent with locally invoking **BaseRegOpenKey (section 3.1.5.15)** ([MS-RRP] section 3.1.5.15) using the RegistryKeyName of the setting.
- The *SecurityInformation* MUST be set to OWNER_SECURITY_INFORMATION | GROUP_SECURITY_INFORMATION | DACL_SECURITY_INFORMATION | SACL_SECURITY_INFORMATION ([MS-RRP] section 2.2.10).
- The *pRpcSecurityDescriptor* MUST be set to the security descriptor provided in the "ACLString" setting in the form of a **RPC_SECURITY_DESCRIPTOR (section 2.2.9)** ([MS-RRP] section 2.2.9).

3.2.5.9 Service General Settings

Settings in Service General Settings (section 2.2.8) MUST be set by applying start up configuration and security descriptors on services for each setting.

Start up configuration MUST be applied to services by performing external behavior consistent with locally invoking RChangeServiceConfigW ([MS-SCMR] section 3.1.4.11) for each setting.

- The *hService* MUST be set to service handle opened by performing external behavior consistent with locally invoking ROpenServiceW ([MS-SCMR] section 3.1.4.16) using the ServiceName of the setting.

- The *dwServiceType* MUST be set to the service type retrieved by performing external behavior consistent with locally invoking RQueryServiceConfigW ([MS-SCMR] section 3.1.4.17).

- The *dwStartType* MUST be set to the StartupMode of a setting in Service General Settings where the StartupMode are mapped to the dwStartType ([MS-SCMR] section 2.2.15) according to the following table.

[MS-GPSB]	[MS-SCMR]
Value of "2"	SERVICE_AUTO_START ([MS-SCMR] section 2.2.15)
Value of "3"	SERVICE_DEMAND_START ([MS-SCMR] section 2.2.15)
Value of "4"	SERVICE_DISABLED ([MS-SCMR] section 2.2.15)

- The *dwErrorControl* MUST be set to the error control retrieved by performing external behavior consistent with locally invoking RQueryServiceConfigW ([MS-SCMR] section 3.1.4.17).

- The *lpBinaryPathName* MUST be set to the path name retrieved by performing external behavior consistent with locally invoking RQueryServiceConfigW ([MS-SCMR] section 3.1.4.17).

- The *lpLoadOrderGroup* MUST be set to the service group for load ordering retrieved by performing external behavior consistent with locally invoking RQueryServiceConfigW ([MS-SCMR] section 3.1.4.17).

- The *lpdwTagId* MUST be set to NULL.

- The *lpDependencies* MUST be set to the dependencies retrieved by performing external behavior consistent with locally invoking RQueryServiceConfigW ([MS-SCMR] section 3.1.4.17).

- The *dwDependSize* MUST be set to the number of dependencies retrieved by performing external behavior consistent with locally invoking RQueryServiceConfigW ([MS-SCMR] section 3.1.4.17).

- The *lpServiceStartName* MUST be set to NULL.

- The *lpPassword* MUST be set to NULL.

- The *dwPwSize* MUST be set to 0.

- The *lpDisplayName* MUST be set to the display name retrieved by performing external behavior consistent with locally invoking RQueryServiceConfigW ([MS-SCMR] section 3.1.4.17).

Security descriptors MUST be applied to services by performing the external behavior consistent with locally invoking RSetServiceObjectSecurity ([MS-SCMR] section 3.1.4.6) for each setting.

- The *hService* MUST be set to a service handle opened by performing external behavior consistent with locally invoking ROpenServiceW ([MS-SCMR] section 3.1.4.16) using the ServiceName of the setting.

- The *dwSecurityInformation* MUST be set to DACL_SECURITY_INFORMATION ([MS-SCMR] section 2.2.1.

- The *lpSecurityInformation* MUST be set to the security descriptor in the AclString of the setting in the form specified in [MS-WSO] sections 3.1.2.3.2 and 3.1.2.3.3.

3.2.5.10 File Security

The security descriptor on a file or subdirectory MUST be applied by performing external behavior consistent with locally invoking the "Application Requests Applying File Security" task [MS-SMB2] section 3.2.4.13) with the following parameters:

- The Open MUST be set to an open returned by performing external behavior consistent with locally invoking the "Application Requests Opening a File" task ([MS-SMB2] section 3.2.4.3) using the FileOrDirectoryPath of the setting.
- The security information MUST be set to the security descriptor provided in the "ACLString" setting. This security descriptor must be in the self-relative form specified in [MS_DTYP] section 2.4.6.
- The security attributes MUST be set to DACL_SECURITY_INFORMATION [MS-SMB2] section 2.2.37).

3.2.5.11 Group Membership

Settings in Group Membership MUST be set by applying members and membership on a group for each setting.

The members and membership of global and universal groups MUST be applied by performing external behavior consistent with locally invoking "Perform an LDAP Operation on an ADConnection" task ([MS-ADSO] section 6.2.6.1.6) with the following parameters for each of the values in a setting:

- TaskInputADConnection: An ADConnection handle ([MS-ADSO] section 6.2.2) based on the client's domain name.
- TaskInputRequestMessage: An LDAP ModifyRequest ([RFC2251] section 4.6) as follows:
  - **object**: Distinguished name for the group specified by the GroupName of the setting.
  - The modification sequence has one entry, as follows:
    - operation: add.
    - modification:
      - **type**: member or memberOf.
      - **vals**:Distinguished name for the object specified by a Value of the setting.

The members and membership of local domain groups and local groups MUST be applied by performing external behavior consistent with locally invoking SamrAddMemberToGroup ([MS-SAMR] section 3.1.5.8.1) for each of the Values in a setting:

- The *GroupHandle* MUST be set to group handle opened by performing external behavior consistent with locally invoking SamrOpenGroup [MS-SAMR] section 3.1.5.1.7) using the SID of the group specified by the GroupName of the setting.
- The *MemberId* MUST be set to the RID of the object specified by the SID Value of the setting.

- The *Attributes* MUST be set to 0.

3.2.5.12 User Account Control

Settings in User Account Control (section 2.2.11) MUST be set by adding registry values as specified in section 2.2.5.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4 Protocol Examples

4.1 Example Involving Password Policy

In the following example, an administrator specifies that, for computers to which a certain GPO applies, a specified password policy is enforced:

- Minimum password length is 8 characters.
- Password complexity checks are turned on.
- Password history of 10 passwords should be remembered and enforced.

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[System Access]
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 10
```

4.2 Example Involving Audit Settings

In the following example, an administrator specifies that the designated audit settings be applied for computers to which a certain GPO applies:

1. Audit made successful attempts for account logon.
2. Audit failed attempts for account management.
3. Audit made successful and failed attempts for object access.
4. Audit made successful and failed attempts for process tracking.

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Event Audit]
AuditObjectAccess = 3
AuditAccountManage = 2
AuditProcessTracking = 3
AuditAccountLogon = 1
```

4.3 Example of Configuring Group Membership

In the following example, an administrator specifies that, for computers to which a certain GPO applies, the group memberships are configured as assigned:

1. Group1 should contain the following members: member1, member2, and member3.
2. Group2 should contain the following members: member1 and member3.

3. Group3 should contain the following member: member4.

4. Group1 should be part of Group3.

5. Group2 should be part of Group1.

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Group Membership]
Group1__Memberof = Group3
Group1__Members = member3,member2,member1
Group2__Memberof = Group3
Group2__Members = member3,member1
Group3__Memberof =
Group3__Members = member4
```

4.4 Example of Configuring Multiple Types of Settings

In the following example, an administrator specifies that for computers to which a certain GPO applies, all the settings specified in the previous sections should be configured as designated.

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[System Access]
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 10
[Event Audit]
AuditObjectAccess = 3
AuditAccountManage = 2
AuditProcessTracking = 3
AuditAccountLogon = 1
[Group Membership]
Group1__Memberof = Group3
Group1__Members = member3,member2,member1
Group2__Memberof = Group3
Group2__Members = member3,member1
Group3__Memberof =
Group3__Members = member4
```

5 Security

5.1 Security Considerations for Implementers

The ClearTextPassword flag, as specified in section 2.2.1.1, indicates whether passwords are to be stored by using reversible encryption. This policy provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords by using reversible encryption is essentially the same as storing plain-text versions of the passwords. For this reason, this policy SHOULD never be enabled unless application requirements outweigh the need to protect password information.

5.2 Index of Security Parameters

5.2.1 Security Parameters Affecting Behavior of the Protocol

Name of setting	Default value	Explanation of setting
MaxNoGPOListChangesInterval Details are as specified in [MS-GPOL].	960	Time interval (in minutes) that sets a maximum limit of how long a client can function without reapplying nonchanged GPOs.

5.2.2 System Security Parameters Carried by the Protocol

Settings category	Comments
System Access	For more information, see section 2.2.1.
Kerberos Policy	For more information, see section 2.2.2.
System Log	For more information, see section 2.2.3.
Security Log	For more information, see section 2.2.3.
Application Log	For more information, see section 2.2.3.
Event Audit	For more information, see section 2.2.4.
Registry Values	For more information, see section 2.2.5.
Privilege Rights	For more information, see section 2.2.6.
Registry Key	For more information, see section 2.2.7.
Service General Setting	For more information, see section 2.2.8.
File Security	For more information, see section 2.2.9.
Group Membership	For more information, see section 2.2.10.

6 Appendix A: Product Behavior

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

- Microsoft Windows® 2000 Server operating system
- Windows® XP operating system
- Windows Server® 2003 operating system
- Windows Vista® operating system
- Windows Server® 2008 operating system
- Windows® 7 operating system
- Windows Server® 2008 R2 operating system

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

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

<1> Section 1.6: This protocol is supported on Windows 2000 Server, Windows XP Professional, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

<2> Section 2.1: If enabled on Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2, the files can also be transported by using the Server Message Block (SMB) Version 2 Protocol, as specified in [MS-SMB2].

<3> Section 2.2.4: Windows does not generate security audit event records for policy change failures.

<4> Section 2.2.4: Windows does not generate security audit event records for process tracking failures.

<5> Section 2.2.11: The settings are supported in Windows Vista, Windows 7, and Windows Server 2008 R2.

<6> Section 3.2.3: If enabled on Windows Vista, Windows Server 2008, Windows 7 or Windows Server 2008 R2, the files can also be transported by using the SMB Version 2.0 Protocol, as specified in [MS-SMB2].

7 Change Tracking

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

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

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

- A document revision that incorporates changes to interoperability requirements or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- The removal of a document from the documentation set.
- Changes made for template compliance.

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

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

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

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

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.

- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- New content added for template compliance.
- Content updated for template compliance.
- Content removed for template compliance.
- Obsolete document removed.

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

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

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

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

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
2.2.6 Privilege Rights	31362 Updated content regarding Privilege Rights Key settings.	Y	Content updated.
3.2.5 Message Processing Events and Sequencing Rules	59005 Changed "GptTmpl.ini" to "GptTmpl.inf" and changed "GPO .ini" to "GPO .inf".	Y	Content updated.
3.2.5.1 Password Policies	59005 Changed "GPO .ini" to "GPO .inf".	Y	Content updated.
3.2.5.3 Kerberos Policy	59005 Changed "GPO .ini" to "GPO .inf".	Y	Content updated.
3.2.5.7 Privilege Rights	31362 Updated content regarding SidENt, Value, RightName, and UserRights Parameter Value	Y	Content updated.

8 Index