[MS-GPAC]:
Group Policy:
Audit Configuration Extension

Intellectual Property Rights Notice for Open Specifications Documentation

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

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

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

Revision Summary

Date	Revision History	Revision Class	Comments
07/02/2009	1.0	Major	First Release.
08/14/2009	1.0.1	Editorial	Revised and edited the technical content.
09/25/2009	1.1	Minor	Updated the technical content.
11/06/2009	1.2	Minor	Updated the technical content.
12/18/2009	1.2.1	Editorial	Revised and edited the technical content.
01/29/2010	1.3	Minor	Updated the technical content.
03/12/2010	1.3.1	Editorial	Revised and edited the technical content.
04/23/2010	1.3.2	Editorial	Revised and edited the technical content.
06/04/2010	2.0	Major	Updated and revised the technical content.
07/16/2010	2.0	No change	No changes to the meaning, language, or formatting of the technical content.
08/27/2010	3.0	Major	Significantly changed the technical content.
10/08/2010	3.0	No change	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	3.0	No change	No changes to the meaning, language, or formatting of the technical content.
01/07/2011	3.0	No change	No changes to the meaning, language, or formatting of the technical content.
02/11/2011	4.0	Major	Significantly changed the technical content.
03/25/2011	5.0	Major	Significantly changed the technical content.
05/06/2011	5.1	Minor	Clarified the meaning of the technical content.
06/17/2011	5.2	Minor	Clarified the meaning of the technical content.
09/23/2011	5.3	Minor	Clarified the meaning of the technical content.
12/16/2011	5.4	Minor	Clarified the meaning of the technical content.
03/30/2012	5.4	No change	No changes to the meaning, language, or formatting of the technical content.
07/12/2012	5.4	No change	No changes to the meaning, language, or formatting of the technical content.
10/25/2012	5.4	No change	No changes to the meaning, language, or formatting of the technical content.

Date	Revision History	Revision Class	Comments
01/31/2013	6.0	Major	Significantly changed the technical content.
08/08/2013	7.0	Major	Significantly changed the technical content.

Contents

1 Introduction

This document specifies the Group Policy: Audit Policy Configuration Protocol, which provides a mechanism for an administrator to control advanced audit policies on **clients**.

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

1.1 Glossary

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

Active Directory
Active Directory Domain Services (AD DS)
Active Directory object
administrative tool
attribute
Augmented Backus-Naur Form (ABNF)
client
client-side extension GUID (CSE GUID)
computer-scoped Group Policy Object path
domain
domain controller (DC)
globally unique identifier (GUID)
Group Policy
Group Policy Object (GPO)
Lightweight Directory Access Protocol (LDAP)
policy setting
security identifier (SID)
share
system access control list (SACL)
token
tool extension GUID or administrative plug-in GUID
Universal Naming Convention (UNC)
UTF-8

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

Group Policy server

The following terms are specific to this document:

advanced audit policy: The global audit policy settings pertaining to auditing as described in this specification.

audit policy: The global audit policy settings pertaining to auditing as described in [MS-GPSB] section 2.2.4.

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

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

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

1.2.1 Normative References

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

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

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

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

[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".

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

[MS-WPO] Microsoft Corporation, "Windows Protocols Overview".

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

1.3 Overview

The Group Policy: Audit Configuration Extension to the Group Policy: Core Protocol enables advanced audit policies to be distributed to multiple client systems so that these systems can enforce the policies in accordance with the intentions of the administrator.

1.3.1 Background

The Group Policy: Core Protocol (as specified in [MS-GPOL]) allows clients to discover and retrieve **policy settings** created by administrators of a **domain**. These settings are persisted within **Group Policy Objects (GPOs)** that are assigned to Policy Target accounts in the **Active Directory**. Policy Target accounts are either computer accounts or user accounts in the Active Directory. Each client uses **Lightweight Directory Access Protocol (LDAP)** to determine what GPOs are applicable to it

by consulting the **Active Directory objects** corresponding to both its computer account and the user accounts of any users logging on to the client computer.

On each client, each GPO is interpreted and acted upon by client plug-ins. The client plug-ins responsible for a given GPO are specified using an **attribute** on the GPO. This attribute specifies a list of **globally unique identifier (GUID)** 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 GUID listed in the GPO to determine what client plug-in on the client should handle the GPO. The client then invokes the client plug-in to handle the GPO.

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

1.3.2 Audit Configuration Extension Overview

Advanced audit policies contain settings that enable the underlying audit subsystem determine which activities must be monitored and logged in the security event log. Advanced audit policies contain 3 main types of settings:

- Audit subcategory settings
- Audit options
- Global object access policy

The following major steps are involved in advanced audit policy configuration:

- Advanced audit policy authoring
- Advanced audit policy assignment
- Advanced audit policy distribution

Advanced audit policy authoring is enabled through an administrative tool for the Group Policy: Core Protocol specified in [MS-GPOL] with an administrative-side plug-in for behavior specific to this protocol. The plug-in allows an administrator to author advanced audit policies within an implementation-specific tool providing a graphical user interface. The plug-in then saves the advanced audit policies into files with a format specified in this document, and stores them on a file **share** that is accessible by remote file access sequences.

Advanced audit 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 path using the **Universal Naming Convention (UNC)** where the advanced audit policy files generated by the protocol administrative plug-in need to be fetched from using remote file access sequences.

Advanced audit 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 advanced audit policy settings. The advanced audit policy protocol client-side plug-in locates the advanced audit policy by appending "\Microsoft\Windows NT\Audit\audit.csv" to the network location specified in each GPO, transfers the advanced audit policy files by using remote file access sequences, and then uses the advanced audit policy files to configure the client's advanced audit policy, audit options, and global object access auditing settings.

1.3.2.1 Audit Subcategory Settings

The advanced audit policy allows administrators to select only the behaviors that they want to monitor and to exclude audit results for behaviors that are of little or no concern to them, or behaviors that create an excessive number of log entries. These settings are grouped in 9 main audit categories, which are divided into 53 audit subcategories:

- System
  - Security State Change
  - Security System Extension
  - System Integrity
  - IPsec Driver
  - Other System Events
- Logon/Logoff
  - Logon
  - Logoff
  - Account Lockout
  - IPsec Main Mode
  - IPsec Quick Mode
  - IPsec Extended Mode
  - Special Logon
  - Other Logon/Logoff Events
  - Network Policy Server
- Object Access
  - File System
  - Registry
  - Kernel Object
  - SAM
  - Certification Services
  - Application Generated
  - Handle Manipulation
  - File Share
  - Filtering Platform Packet Drop

- Filtering Platform Connection
- Other Object Access Events
- Detailed File Share
- Removable Storage
- Central Access Policy Staging

- Privilege Use
  - Sensitive Privilege Use
  - Non Sensitive Privilege Use
  - Other Privilege Use Events
- Detailed Tracking
  - Process Creation
  - Process Termination
  - DPAPI Activity
  - RPC Events
- Policy Change
  - Audit Policy Change
  - Authentication Policy Change
  - Authorization Policy Change
  - MPSSVC Rule-Level Policy Change
  - Filtering Platform Policy Change
  - Other Policy Change Events
- Account Management
  - User Account Management
  - Computer Account Management
  - Security Group Management
  - Distribution Group Management
  - Application Group Management
  - Other Account Management Events
- DS Access
  - Directory Service Access

- Directory Service Changes
- Directory Service Replication
- Detailed Directory Service Replication

- Account Logon
  - Credential Validation
  - Kerberos Service Ticket Operations
  - Other Account Logon Events
  - Kerberos Authentication Service

For more information about audit subcategories, see section 2.2.1.2

1.3.2.2 Audit Options

Audit options are settings that enable or disable functionality of the audit subsystem. These settings include crashing the system on audit failures, full privilege auditing, auditing of base objects, and auditing of base directories.

For more information about audit options, see section 2.2.2.

1.3.2.3 Global Object Access Policy

The global object access policy contains a set of system access control lists that are applied to whole resource managers like the File System and Registry.

For more information about global object access policy, see section 2.2.2.

1.4 Relationship to Other Protocols

This protocol depends on Group Policy: Core Protocol, as specified in [MS-GPOL], to provide a list of applicable GPOs. It also transmits Group Policy settings and instructions between the client and the **Group Policy server** by reading and writing files. See [MS-WPO] section 6.4 for an overview of Windows remote file system concepts. The following diagram illustrates these relationships.

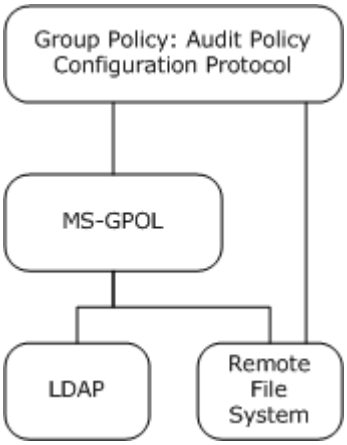

Figure 1: Group Policy: Audit Configuration Extension protocol relationship diagram

1.5 Prerequisites/Preconditions

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

1.6 Applicability Statement

Group Policy: Audit Configuration Extension is only applicable within the Group Policy framework.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

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

Parameter	Value
CSE GUID	{f3ccc681-b74c-4060-9f26-cd84525dca2a}
Tool extension GUID (computer policy settings)	{0F3F3735-573D-9804-99E4-AB2A69BA5FD4}

2 Messages

2.1 Transport

The Group Policy: Audit Configuration Extension requires remote file access as specified for use in the Group Policy: Core Protocol [MS-GPOL]. All messages MUST be exchanged over the remote file access protocols between the client and server, as specified in section 2.2.

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 Message Syntax

Messages exchanged in the Group Policy: Audit Configuration Extension correspond to advanced audit policy files transferred by using remote file access sequences. The protocol is driven through the exchange of these messages, as specified in section 3.

All advanced audit policy files processed by the Group Policy: Audit Configuration Extension are **UTF-8** encoded and based on the file syntax as follows.

```
CSVFile = Header SubcategorySettings AuditOptions GlobalObjectAccessAuditSettings
Header = "Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion
Setting,Setting Value" LineBreak
```

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
GUID                    = %x7B time-low hyphen time-mid hyphen
                          time-high-and-version hyphen
                          clock-seq-and_reserved
                          clock-seq-low hyphen node %x7D
time-low                = hexOctet hexOctet hexOctet hexOctet
time-mid                = hexOctet hexOctet
time-high-and-version   = hexOctet hexOctet
clock-seq-and-reserved = hexOctet
clock-seq-low           = hexOctet
node                    = hexOctet hexOctet hexOctet
                          hexOctet hexOctet hexOctet
hexOctet                = hexDigit hexDigit
hexDigit                = digit / a / b / c / d / e / f
digit                   = "0" / "1" | "2" / "3" / "4" / "5" / "6" / "7" /
                          "8" / "9"
hyphen                  = "-"
a                       = "a" / "A"
b                       = "b" / "B"
c                       = "c" / "C"
d                       = "d" / "D"
```

```
e                       = "e" / "E"
f                       = "f" / "F"
```

2.2.1 Subcategory Settings

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

```
SubcategorySettings = SubcategorySetting / SubcategorySetting / SubcategorySetting
SubcategorySetting = MachineName "," PolicyTarget "," Subcategory "," SubcategoryGUID ","
InclusionSetting "," ExclusionSetting "," SettingValue LineBreak
```

2.2.1.1 Policy Target

This section defines the possible values for the PolicyTarget attribute, which enables an administrator to specify whether the audit subcategory must be set for a system advanced audit policy or a specific user. The syntax for the entries in this category MUST be as follows.

```
PolicyTarget = "System" / UserSID
```

The value of PolicyTarget MUST be one of the following:

- A value of "System": Indicates that this is a system audit subcategory setting.
- A UserSID: Indicates that this is a per-user audit subcategory setting.

UserSID is the string representation of the **security identifiers (SIDs)** of a user account. The syntax for the entries in this category MUST be as follows.

```
UserSID = String
```

The UserSID string MUST use the standard S-*R*-*I*-*S*-*S*... format for SID strings, as specified in [MS-DTYP] (section 2.4.2).<1>

2.2.1.2 Subcategory and SubcategoryGUID

This section defines how the Subcategory and SubcategoryGUID values are used by the audit configuration client-side plug-in.

The Subcategory field is for user reference only and is ignored when the advanced audit policy is applied by the audit configuration client-side plug-in.

The syntax for the entries in this category MUST be as follows.

```
Subcategory = StringWithSpaces / QuotedString
SubcategoryGUID = GUID
```

The SubcategoryGUID allows administrators to identify audit subcategories to enable or disable in the client's system or per-user advanced audit policy. For more information about enabling or disabling audit subcategories, see section 2.2.1.3.

The following table provides an explanation for the valid **SubcategoryGUID** values.

SubcategoryGUID	Purpose
{0CCE9213-69AE-11D9-BED3-505054503030}	Identifies the **IPsec Driver** audit subcategory. This subcategory audits events that are generated by the IPsec filter driver.
{0CCE9212-69AE-11D9-BED3-505054503030}	Identifies the **System Integrity** audit subcategory. This subcategory audits events that violate the integrity of the security subsystem.
{0CCE9211-69AE-11D9-BED3-505054503030}	Identifies the **Security System Extension** audit subcategory. This subcategory audits events related to security system extensions or services.
{0CCE9210-69AE-11D9-BED3-505054503030}	Identifies the **Security State Change** audit subcategory. This subcategory audits events generated by changes in the security state of the computer.
{0CCE9214-69AE-11D9-BED3-505054503030}	Identifies the **Other System Events** audit subcategory. This subcategory audits any of the following events: ▪ Startup and shutdown of the Windows Firewall. ▪ Security policy processing by the Windows Firewall. ▪ Cryptography key file and migration operations.
{0CCE9243-69AE-11D9-BED3-505054503030}	Identifies the **Network Policy Server** audit subcategory. This subcategory audits events generated by RADIUS (IAS) and Network Access Protection (NAP) user access requests. These requests can be Grant, Deny, Discard, Quarantine, Lock, and Unlock.
{0CCE921C-69AE-11D9-BED3-505054503030}	Identifies the **Other Logon/Logoff** Events audit subcategory. This subcategory audits other events related to logon and logoff that are not included in the Logon/Logoff category.
{0CCE921B-69AE-11D9-BED3-505054503030}	Identifies the **Special Logon** audit subcategory. This subcategory audits events generated by special logons.
{0CCE921A-69AE-11D9-BED3-505054503030}	Identifies the **IPsec Extended Mode** audit subcategory. This subcategory audits events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Extended Mode negotiations.
{0CCE9219-69AE-11D9-BED3-505054503030}	Identifies the **IPsec Quick Mode** audit subcategory. This subcategory audits events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Quick Mode negotiations.
{0CCE9218-69AE-	Identifies the **IPsec Main Mode** audit subcategory.

SubcategoryGUID	Purpose
11D9-BED3-505054503030}	This subcategory audits events generated by Internet Key Exchange protocol (IKE) and Authenticated Internet Protocol (AuthIP) during Main Mode negotiations.
{0CCE9217-69AE-11D9-BED3-505054503030}	Identifies the **Account Lockout** audit subcategory. This subcategory audits events generated by a failed attempt to log on to an account that is locked out.
{0CCE9216-69AE-11D9-BED3-505054503030}	Identifies the **Logoff** audit subcategory. This subcategory audits events generated by closing a logon session. These events occur on the computer that was accessed. For an interactive logon, the security audit event is generated on the computer that the user account logged on to.
{0CCE9215-69AE-11D9-BED3-505054503030}	Identifies the **Logon** audit subcategory. This subcategory audits events generated by user account logon attempts on a computer.
{0CCE9223-69AE-11D9-BED3-505054503030}	Identifies the **Handle Manipulation** audit subcategory. This subcategory audits events generated when a handle to an object is opened or closed. Only objects with a matching SACL generate security audit events. Open and close handle events will be audited when both the Handle Manipulation subcategory is enabled along with the corresponding resource manager identified by other Object Access audit subcategory, like File System or Registry. Enabling Handle Manipulation causes implementation-specific security event data to be logged identifying the permissions that were used to grant or deny the access requested by the user; this is also known as "Reason for access".
{0CCE9244-69AE-11D9-BED3-505054503030}	Identifies the **Detailed File Share** audit subcategory. This subcategory audits every attempt to access objects in a shared folder.
{0CCE9227-69AE-11D9-BED3-505054503030}	Identifies the **Other Object Access** Events audit subcategory. This subcategory audits events generated by the management of Task Scheduler jobs or COM+ objects.
{0CCE9226-69AE-11D9-BED3-505054503030}	Identifies the **Filtering Platform Connection** audit subcategory. This subcategory audits connections that are allowed or blocked by WFP.
{0CCE9225-69AE-11D9-BED3-505054503030}	Identifies the **Filtering Platform Packet Drop** audit subcategory. This subcategory audits packets that are dropped by Windows Filtering Platform (WFP).
{0CCE9224-69AE-11D9-BED3-505054503030}	Identifies the **File Share** audit subcategory. This subcategory audits attempts to access a shared folder.
{0CCE9222-69AE-11D9-BED3-505054503030}	Identifies the **Application Generated** audit subcategory. This subcategory audits applications that generate events by using the Windows Auditing application programming interfaces (APIs). Applications designed to use the Windows Auditing API use this subcategory to log auditing events related to their function.
{0CCE9221-69AE-11D9-BED3-	Identifies the **Certification Services** audit subcategory. This subcategory audits Active Directory Certificate Services (AD CS)

SubcategoryGUID	Purpose
505054503030}	operations.
{0CCE9220-69AE-11D9-BED3-505054503030}	Identifies the **SAM** audit subcategory. This subcategory audits events generated by attempts to access Security Accounts Manager (SAM) objects.
{0CCE921F-69AE-11D9-BED3-505054503030}	Identifies the **Kernel Object** audit subcategory. This subcategory audits attempts to access the system kernel, which include mutexes and semaphores. Only kernel objects with a matching SACL generate security audit events. **Note:** The **Audit: Audit the access of global system objects** policy setting controls the default SACL of kernel objects.
{0CCE921E-69AE-11D9-BED3-505054503030}	Identifies the **Registry** audit subcategory. This subcategory audits attempts to access registry objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Read, Write, or Modify, and the account making the request match the settings in the SACL.
{0CCE921D-69AE-11D9-BED3-505054503030}	Identifies the **File System** audit subcategory. This subcategory audits user attempts to access file system objects. A security audit event is generated only for objects that have SACLs and only if the type of access requested, such as Write, Read, or Modify, and the account making the request match the settings in the SACL.
{0CCE9229-69AE-11D9-BED3-505054503030}	Identifies the **Non Sensitive Privilege Use** audit subcategory. This subcategory audits events generated by the use of nonsensitive privileges (user rights), such as logging on locally or with a Remote Desktop connection, changing the system time, or removing a computer from a docking station.
{0CCE922A-69AE-11D9-BED3-505054503030}	Identifies the **Other Privilege Use Events** audit subcategory.
{0CCE9228-69AE-11D9-BED3-505054503030}	Identifies the **Sensitive Privilege Use** audit subcategory. This subcategory audits events generated by the use of sensitive privileges (user rights), such as acting as part of the operating system, backing up files and directories, impersonating a client computer, or generating security audits.
{0CCE922D-69AE-11D9-BED3-505054503030}	Identifies the **DPAPI Activity** audit subcategory. This subcategory audits events generated when encryption or decryption requests are made to the Data Protection application interface (DPAPI). DPAPI is used to protect secret information such as stored password and key information.
{0CCE922C-69AE-11D9-BED3-505054503030}	Identifies the **Process Termination** audit subcategory. This subcategory audits events generated when a process ends.
{0CCE922B-69AE-11D9-BED3-505054503030}	Identifies the **Process Creation** audit subcategory. This subcategory audits events generated when a process is created or starts. The name of the application or user that created the process is also audited.
{0CCE922E-69AE-	Identifies the **RPC Events** audit subcategory.

SubcategoryGUID	Purpose
11D9-BED3-505054503030}	This subcategory audits inbound remote procedure call (RPC) connections.
{0CCE9232-69AE-11D9-BED3-505054503030}	Identifies the **MPSSVC Rule-Level Policy Change** audit subcategory. This subcategory audits events generated by changes in policy rules used by Windows Firewall.
{0CCE9234-69AE-11D9-BED3-505054503030}	Identifies the **Other Policy Change Events** audit subcategory. This subcategory audits events generated by other security policy changes that are not audited in the Policy Change category.
{0CCE9233-69AE-11D9-BED3-505054503030}	Identifies the **Filtering Platform Policy Change** audit subcategory. This subcategory audits events generated by changes to Windows Filtering Platform (WFP).
{0CCE922F-69AE-11D9-BED3-505054503030}	Identifies the **Audit Policy Change** audit subcategory. This subcategory audits changes in security **audit policy** settings.
{0CCE9231-69AE-11D9-BED3-505054503030}	Identifies the **Authorization Policy Change** audit subcategory. This subcategory audits events generated by changes to the authorization policy.
{0CCE9230-69AE-11D9-BED3-505054503030}	Identifies the **Authentication Policy Change** audit subcategory. This subcategory audits events generated by changes to the authentication policy.
{0CCE923A-69AE-11D9-BED3-505054503030}	Identifies the **Other Account Management Events** audit subcategory. This subcategory audits events generated by other user account changes that are not covered in this category.
{0CCE9239-69AE-11D9-BED3-505054503030}	Identifies the **Application Group Management** audit subcategory. This subcategory audits events generated by changes to application groups.
{0CCE9238-69AE-11D9-BED3-505054503030}	Identifies the **Distribution Group Management** audit subcategory. This subcategory audits events generated by changes to distribution groups.
{0CCE9237-69AE-11D9-BED3-505054503030}	Identifies the **Security Group Management** audit subcategory. This subcategory audits events generated by changes to security groups.
{0CCE9236-69AE-11D9-BED3-505054503030}	Identifies the **Computer Account Management** audit subcategory. This subcategory audits events generated by changes to computer accounts, such as when a computer account is created, changed, or deleted.
{0CCE9235-69AE-11D9-BED3-505054503030}	Identifies the **User Account Management** audit subcategory. This subcategory audits changes to user accounts.
{0CCE923E-69AE-11D9-BED3-505054503030}	Identifies the **Detailed Directory Service Replication** audit subcategory. This subcategory audits events generated by detailed **AD DS** replication between **domain controllers (DCs)**.
{0CCE923B-69AE-	Identifies the **Directory Service Access** audit subcategory.

SubcategoryGUID	Purpose
11D9-BED3-505054503030}	This subcategory audits events generated when an AD DS object is accessed. Only AD DS objects with a matching SACL are logged.
{0CCE923D-69AE-11D9-BED3-505054503030}	Identifies the **Directory Service Replication** audit subcategory. This subcategory audits replication between two AD DSDCs.
{0CCE923C-69AE-11D9-BED3-505054503030}	Identifies the **Directory Service Changes** audit subcategory. This subcategory audits events generated by changes to AD DS objects. Events are logged when an object is created, deleted, modified, moved, or undeleted.
{0CCE9241-69AE-11D9-BED3-505054503030}	Identifies the **Other Account Logon Events** audit subcategory. This subcategory audits events generated by responses to credential requests submitted for a user account logon that are not credential validation or Kerberos tickets.
{0CCE9240-69AE-11D9-BED3-505054503030}	Identifies the **Kerberos Service Ticket Operations** audit subcategory. This subcategory audits events generated by Kerberos service ticket requests.
{0CCE923F-69AE-11D9-BED3-505054503030}	Identifies the **Credential Validation** audit subcategory. This subcategory audits events generated by validation tests on user account logon credentials.
{0CCE9242-69AE-11D9-BED3-505054503030}	Identifies the **Kerberos Authentication Service** audit subcategory. This subcategory audits events generated by Kerberos authentication **ticket-granting ticket (TGT)** requests.
{0CCE9245-69AE-11D9-BED3-505054503030}	Identifies the **Removable Storage** audit subcategory. This subcategory audits user attempts to access file system objects on any Removable Storage device. A security audit event is generated for every read or write access to a file object on any Removable Storage device attached to the user's machine.
{0CCE9246-69AE-11D9-BED3-505054503030}	Identifies the **Central Access Policy Staging** audit subcategory. This subcategory audits access requests where the permission granted or denied by a proposed policy differs from that granted or denied by the current central access policy on an object.

2.2.1.3 Inclusion Setting, Exclusion Setting, and Setting Value

This section defines settings that enable an administrator to define whether a subcategory should be added to or removed from the client advanced audit policy.

The possible value of these attributes depends whether the subcategory audit setting policy target is "System" or a specific user or group.

2.2.1.3.1 Inclusion Setting, Exclusion Setting, and SettingValue for System Audit Subcategories

This section defines the syntax for the InclusionSetting, ExclusionSetting, and SettingValue attributes when the PolicyTarget attribute is set to "System".

The syntax for the entries in this category MUST be as follows.

```
InclusionSetting-SA = "Success" / "Failure" / "Success and Failure" / "No Auditing" / "Not
Specified"
ExclusionSetting-SA = ""
SettingValue-SA = 1*DIGIT
```

Please note that the element names above have a postfix of "-SA" to differentiate them from per-user audit settings which have a postfix of "-UA".

The value of SettingValue MUST be one of the following:

- A value of "0": Indicates that this audit subcategory setting should remain unchanged.
- A value of "1": Indicates that this audit subcategory setting is set to Success Audits Only.
- A value of "2": Indicates that this audit subcategory setting is set to Failure Audits Only.
- A value of "3": Indicates that this audit subcategory setting is set to Success and Failure Audits.
- A value of "4": Indicates that this audit subcategory setting is set to None.

Note The value of InclusionSetting is for user readability only and is ignored when the advanced audit policy is applied by the audit configuration client-side plug-in.

2.2.1.3.2 Inclusion Setting, Exclusion Setting, and SettingValue for Per-User Audit Subcategories

This section defines the syntax for the InclusionSetting, ExclusionSetting, and SettingValue attributes when the PolicyTarget attribute is set to a specific user or group SID.

The syntax for the entries in this category MUST be as follows.

```
InclusionSetting-UA = "SettingValueText"
ExclusionSetting-UA = SettingValueText
SettingValueText-UA = "Success" / "Failure" / "Success and Failure" / "No Auditing" / "Not
Specified"
SettingValue-UA = 1*DIGIT
```

Please note that the element names above have a postfix of "-UA" to differentiate them from System advanced audit policy settings, which have a postfix of "-SA".

The attribute **SettingValueText** is for user readability only and is ignored when the advanced audit policy is applied by the audit configuration client-side plug-in.

The value of SettingValue MUST be one of the following:

- A value of "0": Indicates that this audit subcategory setting should remain unchanged.
- A value of "16": Indicates that this audit subcategory setting should be set to None.
- A decimal numerical value created by combining the following bits.

Bit order	Hexadecimal value	Purpose
1	0x01	**Include Success**: This bit will cause a **Success** Audit to be generated even if not specified by the system advanced audit policy.
2	0x02	**Exclude Success**: This bit will cause a **Success** Audit to be suppressed regardless of the system advanced audit policy. This setting is not honored for users who are members of the Administrators local group.
3	0x04	**Include Failure**: This bit will cause a **Failure** Audit to be generated even if not specified by the system advanced audit policy.
4	0x08	**Exclude Failure**: This bit will cause a **Failure** Audit to be suppressed regardless of the system advanced audit policy. This setting is not honored for users who are members of the Administrators local group.

Note Include has a higher precedence than exclude:

- If **Include Success** and **Exclude Success** bits are set, **Include Success** is used and **Exclude Success** is ignored.
- If **Include Failure** and **Exclude Failure** bits are set, **Include Failure** is used and **Exclude Failure** is ignored.<2>

2.2.2 Audit Options

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

```
AuditOptions = MachineName ",,Option:" AuditOptionType ",," AuditOptionValueText ",,"
AuditOptionValue
```

2.2.2.1 Audit Option Type

This section defines the advanced audit options that are part of the audit policy. The syntax for the entries in this category MUST be as follows.

```
AuditOptionType = String
```

The value of AuditOptionType MUST be one of the following:

AuditOptionType	Purpose
CrashOnAuditFail	This audit option specifies whether the client shuts down if it is unable to log security events. If this security setting is enabled, it causes the client to stop if a security audit cannot be logged for any reason.
FullPrivilegeAuditing	This audit option specifies whether the client generates an event when one or more of these privileges are assigned to a user security **token**: ▪ AssignPrimaryTokenPrivilege

AuditOptionType	Purpose
	▪ AuditPrivilege ▪ BackupPrivilege ▪ CreateTokenPrivilege ▪ DebugPrivilege ▪ EnableDelegationPrivilege ▪ ImpersonatePrivilege ▪ LoadDriverPrivilege ▪ RestorePrivilege ▪ SecurityPrivilege ▪ SystemEnvironmentPrivilege ▪ TakeOwnershipPrivilege ▪ TcbPrivilege
AuditBaseObjects	This security setting specifies whether to audit the access of global system objects. If this audit option is enabled, it causes system objects, such as mutexes, events, semaphores, and DOS devices, to be created with a default **system access control list (SACL)**. Only named objects are given a SACLs; SACL are not given to objects without names. If the Kernel Object audit subcategory is also enabled, access to these system objects is audited.
AuditBaseDirectories	The AuditBaseDirectories option specifies that named kernel objects (such as mutexes and semaphores) are to be given SACLs when they are created. AuditBaseDirectories affects container objects while AuditBaseObjects affects objects that cannot contain other objects.

2.2.2.2 Audit Option Value

This section defines the possible values corresponding to the audit options. The syntax for the entries in this category MUST be as follows.

```
AuditOptionValueText = "Enabled" / "Disabled"
AuditOptionValue = 1*DIGIT
```

Note The AuditOptionValueText field is for user reference only and is ignored when the advanced audit policy is applied by the audit configuration client-side plug-in.

The value of AuditOptionValue MUST be one of the following:

AuditOptionValue	Purpose
"0"	The audit option is **disabled**.
"1"	The audit option is **enabled**.

2.2.3 Global Object Access Audit Settings

This section defines settings that enable an administrator to set the global object access auditing settings for an advanced audit policy.

Global object access audit settings can be used by administrators to define system access control lists (SACLs) that apply dynamically to every object in a specific resource manager. When a global object access audit setting is defined, the auditing system combines the SACL defined in the security descriptor that is being accessed with the global object access SACL for the corresponding resource manager. An event is logged if either of the two SACLs (object SACL or global SACL) determines that the activity must be audited.

The syntax for the entries in this category MUST be as follows.

```
GlobalObjectAccessAuditSettings = MachineName ",," ResourceGlobalSaclType ",,,," GlobalSACL
```

2.2.3.1 Resource Global SACL Type

This section defines the use of the ResourceGlobalSaclType attribute. The syntax for the entries in this category MUST be as follows.

```
ResourceGlobalSaclType = "FileGlobalSacl" / "RegistryGlobalSacl"
```

The value of ResourceGlobalSaclType MUST be one of the following:

ResourceGlobalSaclType	Purpose
"FileGlobalSacl"	Defines a global SACL for the **File System** resource manager.
"RegistryGlobalSacl"	Defines a global SACL for the **Registry** resource manager.

2.2.3.2 Global System Access Control List (SACL)

This section defines the use of the GlobalSACL attribute. The syntax for the entries in this category MUST be as follows.

```
GlobalSACL = SDDLString
SDDLString = String
```

The GlobalSACL attribute MUST be in the form of an SDDL encoding of a SACL of a security descriptor. For more information, see [MSDN-SDDL].

2.2.4 Machine Name

This section defines the use of the machine name, used on different sections of the advanced audit policy. The syntax for the entries in this category MUST be as follows.

```
MachineName = String / QuotedString
```

The machine name is given for user reference and is ignored when the audit configuration client-side plug-in applies an advanced audit policy.

3 Protocol Details

3.1 Audit Configuration Protocol Administrative-Side Plug-in Details

The audit configuration protocol administrative-side plug-in participates in the advanced audit policy authoring and assignment steps, as specified in section 2. The advanced audit policy MUST be stored as a text file by using a .csv format, as specified in section 2.2. The advanced audit policies MUST be stored in a location accessible by using remote file access sequences.

3.1.1 Abstract Data Model

The audit configuration protocol administrative-side plug-in maintains no state. It loads all the settings, as specified in section 2.2, in memory.

The administrative-side plug-in is used, through the implementation-specific tool providing a graphical user interface, to interact with the advanced audit policy file, as specified in [MS-GPOL]. The plug-in determines the physical location of a desired policy, 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 specified location.

3.1.2 Timers

None.

3.1.3 Initialization

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

The administrative-side plug-in is triggered when an administrator starts an **administrative tool**. The plug-in displays the current settings to the administrator, and when the administrator requests a change in settings, the plug-in updates the stored configuration appropriately as specified in section 2.2.

For both viewing and editing settings, the administrative-side plug-in MUST first open the specified GPO to fetch its network path. The plug-in MUST attempt to read an audit.csv file with the settings from the following location (for viewing) or write to the following location (for editing): <gpo path>\Microsoft\Windows NT \Audit\audit.csv (where <gpo path> is the **computer-scoped Group Policy Object path**, if the computer settings are being viewed or updated).

File reads and writes 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

The administrative-side plug-in reads extension-specific data from the remote storage location and passes that information to an implementation-specific tool that provides a graphical user interface to display the current settings to an administrator.

The administrative-side plug-in creates the advanced audit policy file in the remote location specified in section 3.1.4 if the file does not exist. The administrative-side plug-in writes the

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

After every creation, modification, or deletion that affects an audit policy file on SYSVOL, the administrative-side plug-in MUST invoke the Group Policy Extension Update task, as specified in [MS-GPOL] section 3.3.4.4.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Advanced Audit Policy Configuration Client-Side Plug-in Details

The advanced audit policy configuration client-side plug-in interacts with the Group Policy framework, as specified in [MS-GPOL] section 3.2. This plug-in MUST receive the advanced audit policy and modify the appropriate part of the Abstract Data Model (ADM) for each element in the policy as specified in this section.

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.

3.2.1.1 Policy Setting State

The client-side plug-in persistent state consists of the 4 sections below. The location where this state is stored is specific to each implementation.

- System Advanced Audit Policy:

  A list of records, each with a record identifier (subcategory GUID). In addition to the key, each record has an audit setting value that defines the audit behavior for the subcategory. For more information, see section 2.2.1.

- Per-User Advanced Audit Policy:

  A list of records, each with a user or group SID, a subcategory GUID, and an audit setting value that overrides the system audit behavior for the subcategory for the user or group. For more information, see section 2.2.1.

- Audit Options:

  A list of records, each with an audit option type and a setting value. For more information, see section 2.2.2.

- Global Object Access Auditing:

  Consists of two persistent SACL-valued data elements: FileGlobalSacl and RegistryGlobalSacl. This is used to store the global object access audit settings that can be used by administrators to

define system access control lists (SACLs) that apply dynamically to every object in a specific resource manager. For more information, see section 2.2.3.

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 audit configuration protocol client-side plug-in MUST do the following: locate all the advanced audit policy files within those GPOs, copy the policies to the local machine, read the policies, and apply them as specified in section 3.2.5.

Locating advanced audit 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 remote file access sequences.

3.2.4 Higher-Layer Triggered Events

This plug-in implements one higher-layer triggered event: Process Group Policy.

3.2.4.1 Process Group Policy

The plug-in implements the Process Group Policy abstract event interface, as specified in [MS-GPOL] section 3.2.4.1. The plug-in does not make use of the *Deleted GPOs*, the flags, or the security tokens arguments. When the event is triggered, the audit configuration protocol client-side plug-in MUST take the actions described in the section 3.2.5.

3.2.5 Message Processing Events and Sequencing Rules

The audit configuration protocol client-side extension MUST be invoked by the Group Policy framework whenever applicable GPOs need to be processed, as specified in [MS-GPOL] section 3.2.5.1. On such an event, the audit configuration protocol client-side plug-in MUST take the actions described in this section.

When invoked, the audit configuration protocol client-side plug-in expects a list of applicable GPOs in the "New or changed GPOs" parameter. It MUST then go through this list and, for each GPO, locate and retrieve the contained advanced audit policy. 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 plug-in MUST log information about the failure and continue to copy files for other GPOs.

For each GPO, the advanced audit policy configuration client-side plug-in MUST generate the following remote file access sequences to copy the file locally:

Sequence	Description
File Open from Client to Server	The plug-in MUST attempt to open the file specified by <scoped gpo path>\Microsoft\Windows NT\Audit\audit.csv.
File Read Sequences	One or more file reads MUST be done to read the entire content of the opened file or until an error occurs,
File Close	A file close operation MUST be performed.

The file MUST be parsed 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 audit parameters on the system.

After all the advanced audit policies are retrieved, each policy MUST be opened and the contained advanced audit policy settings MUST be extracted and applied for each ADM element corresponding to section 2.2.

When reading the advanced audit policy configuration file, the client-side extension follows the logical flow mentioned below.

If the "Policy Target" column value is empty AND if the "Subcategory" column value indicates FileGlobalSacl, process the "Setting Value" column value in the following way:

- Convert the "Setting Value" column value into a security descriptor based on the format defined in [MSDN-SDDL].
- For each Audit Access Control Entry (ACE) in the SACL of the security descriptor extracted in the previous step, add it to the **FileGlobalSacl** ADM variable if it doesn't already exist.

If the "Policy Target" column value is empty AND if the "Subcategory" column value indicates RegistryGlobalSacl, process the "Setting Value" column value in the following way:

- Convert the "Setting Value" column value into a security descriptor based on the format defined in [MSDN-SDDL].
- For each Audit Access Control Entry (ACE) in the SACL of the security descriptor extracted in the previous step, add it to the **RegistryGlobalSacl** ADM variable if it doesn't already exist.<3>

If the "Policy Target" column value is empty, then verify that the "Subcategory" column value is one of those specified in section 2.2.2.1, Audit Option Type. Once verified, store the "Setting Value" column value in the **AuditOptionValue** field of the corresponding AuditOptionType in the **Audit Options** ADM variable as specified in section 3.2.1.1.

If the "Exclusion Setting" column value is empty, then verify that the "Subcategory GUID" column value is one of those specified in section 2.2.1.2, Subcategory and SubcategoryGUID. Once verified, store the "Setting Value" column value in the audit setting value field of the corresponding subcategory GUID in the **System Advanced Audit Policy** ADM variable as specified in section 3.2.1.1.

If both the "Policy Target" and the "Exclusion Setting" column values are not empty, then verify that the "Subcategory GUID" column value is one of those specified in section 2.2.1.2, Subcategory and SubcategoryGUID. Once verified, for the user identified by the "Policy Target" column value, store the "Setting Value" column value in the audit setting value field of the corresponding subcategory GUID in the **Per-User Advanced Audit Policy** ADM variable as specified in section 3.2.1.1.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4 Protocol Examples

4.1 Example Involving System Audit Subcategory Settings

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

- Exclude audit attempts for IPsec Driver.
- Audit successful attempts for System Integrity.
- Audit successful and failed attempts for IPsec Extended Mode.
- Leave the File System policy unchanged.

```
Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion
Setting,Setting Value
TEST-MACHINE,System,IPsec Driver,{0CCE9213-69AE-11D9-BED3-505054503030},No Auditing,,0
TEST-MACHINE,System,System Integrity,{0CCE9212-69AE-11D9-BED3-505054503030},Success,,1
TEST-MACHINE,System,IPsec Extended Mode,{0CCE921A-69AE-11D9-BED3-505054503030},Success and
Failure,,3
TEST-MACHINE,System,File System,{0CCE921D-69AE-11D9-BED3-505054503030},Not specified,,0
```

4.2 Example Involving Per-User Audit Subcategory Settings

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

- Include made successful attempts for File System for user S-1-5-21-2127521184-1604012920-1887927527-123456.
- Exclude made failed attempts for File System for user S-1-5-21-2127521184-1604012920-1887927527-123456.

```
Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion
Setting,Setting Value
TEST-MACHINE,S-1-5-21-2127521184-1604012920-1887927527-123456,File System,{0CCE921D-69AE-
11D9-BED3-505054503030},Success,Failure,9
```

4.3 Example Involving Audit Options

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

- Enable audit option CrashOnAuditFail.
- Disable audit option FullPrivilegeAuditing.
- Disable audit option AuditBaseObjects.
- Disable audit option AuditBaseDirectories.

```
Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion
Setting,Setting Value
TEST-MACHINE,,Option:CrashOnAuditFail,,Enabled,,1
TEST-MACHINE,,Option:FullPrivilegeAuditing,,Disabled,,0
TEST-MACHINE,,Option:AuditBaseObjects,,Disabled,,0
TEST-MACHINE,,Option:AuditBaseDirectories,,Disabled,,0
```

4.4 Example Involving Global Object Access Auditing

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

- Set a registry Global SACL to log all the activity for everyone.

```
Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion
Setting,Setting Value
TEST-MACHINE,,RegistryGlobalSacl,,,,S:(AU;SA;FA;;;WD)
```

4.5 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.

```
Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion
Setting,Setting Value
TEST-MACHINE,System,IPsec Driver,{0CCE9213-69AE-11D9-BED3-505054503030},No Auditing,,0
TEST-MACHINE,System,System Integrity,{0CCE9212-69AE-11D9-BED3-505054503030},Success,,1
TEST-MACHINE,System,IPsec Extended Mode,{0CCE921A-69AE-11D9-BED3-505054503030},Success and
Failure,,3
TEST-MACHINE,System,File System,{0CCE921D-69AE-11D9-BED3-505054503030},Not specified,,0
TEST-MACHINE,S-1-5-21-2127521184-1604012920-1887927527-123456,File System,{0CCE921D-69AE-
11D9-BED3-505054503030},Success,Failure,9
TEST-MACHINE,,Option:CrashOnAuditFail,,Enabled,,1
TEST-MACHINE,,Option:FullPrivilegeAuditing,,Disabled,,0
TEST-MACHINE,,Option:AuditBaseObjects,,Disabled,,0
TEST-MACHINE,,Option:AuditBaseDirectories,,Disabled,,0
TEST-MACHINE,,RegistryGlobalSacl,,,,S:(AU;SA;FA;;;WD)
```

5 Security

5.1 Security Considerations for Implementers

Setting both the advanced audit policies (as described in this document) and the event audit policies (as described in section 2.2.4 of [MS-GPSB]) on the same client can lead to inconsistent behavior. Therefore, it is recommended that, if the advanced audit policies are being used on a client, the registry value MACHINE\System\CurrentControlSet\Control\LSA\SCENoApplyLegacyAuditPolicy be set to 1, using the mechanism described in Section 2.2.5 of [MS-GPSB]. This will avoid the conflict by preventing the event audit policies from being applied on the client.

5.2 Index of Security Parameters

5.2.1 Security Parameters Affecting Behavior of the Protocol

Security Parameter	Explanation of setting
MaxNoGPOListChangesInterval [MS-GPOL] section 3.2.1.24	When the value of the **MaxNoGPOListChangesInterval** for a particular client-side extension is set (by local implementation-specific means) to a nonzero integer value, the Group Policy Client will invoke the extension after **MaxNoGPOListChangesInterval** minutes, even if the policy has not changed since the last invocation of the extension. This setting can be used to ensure that the advanced audit policy settings created by the administrator of a domain are reapplied on the client after **MaxNoGPOListChangesInterval** minutes. This limits the amount of time that the local and central advanced audit policy settings could be out of sync because of local modifications to the policy.<4>

5.2.2 System Security Parameters Carried by the Protocol

Settings category	Comments
Subcategory settings	For more information, see section 2.2.1.
Audit options	For more information, see section 2.2.2.
Global object access audit settings	For more information, see section 2.2.3.

6 Appendix A: Product Behavior

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

- Windows 7 operating system
- Windows Server 2008 R2 operating system
- Windows 8 operating system
- Windows Server 2012 operating system
- Windows 8.1 operating system
- Windows Server 2012 R2 operating system

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

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

<1> Section 2.2.1.1: In Windows, audit settings associated with group SID strings are ignored by the client.

<2> Section 2.2.1.3.2: If any subcategory in the Per-User Advanced Audit Policy section is defined for a given user or group in Windows, the value **Include Failure** (0x4) is used as default for all the rest of the audit subcategories that are not defined for that user after all the applicable policies are processed. The **Include Failure** setting will cause a **Failure** Audit to be generated even if not specified by the system advanced audit policy.

<3> Section 3.2.5: In Windows 7 and Windows Server 2008 R2, individual Audit ACEs from different GPOs are not merged into a single SACL; instead the final value of the FileGlobalSacl, as well as the RegistryGlobalSacl ADM variables, come from the GPO with the highest precedence (as described in [MS-GPOL]) where the setting is defined.

<4> Section 5.2.1: In Windows, the value of **MaxNoGPOListChangesInterval** is 0x3c0 (960 minutes) for the advanced audit policy client-side extension.

7 Change Tracking

This section identifies changes that were made to the [MS-GPAC] protocol document between the January 2013 and August 2013 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
6 Appendix A: Product Behavior	Modified this section to include references to Windows 8.1 operating system and Windows Server 2012 R2 operating system.	Y	Content updated.

8 Index

R

S

T

V