Quest

# Quest® Change Auditor for Active Directory® 7.4

# Event Reference Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

**Patents**

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

**Trademarks**

Quest Software, Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

**Legend**

**CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

**IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Change Auditor for Active Directory Event Reference Guide
Updated - November 2023
Software Version - 7.4

# Contents

# 1

# Introduction

Change Auditor for Active Directory drives the security and control of Microsoft Active Directory by proactively tracking vital Active Directory configuration changes in real time. From GPO and Schema to critical group and operational changes, Change Auditor for Active Directory tracks, audits, reports, and alerts on changes that impact your directory — without the overhead costs of native auditing.

You can also track, audit, and report on Azure Active Directory changes. For more information, see the Change Auditor for Office 365 and Azure Active Directory Auditing User Guide.

In addition to real-time event auditing, you can enable event logging to capture Active Directory or ADAM (AD LDS) events locally in a Windows event log. These event logs can then be collected using InTrust to satisfy long-term storage requirements.

**NOTE:** Active Directory and ADAM (AD LDS) auditing and event logging are only available when you have licensed Change Auditor for Active Directory. Contact your Sales Representative for more information about obtaining Change Auditor for Active Directory.

This guide lists the events that can be captured by Change Auditor for Active Directory. Separate event reference guides are provided that list the core Change Auditor events (when any Change Auditor license is applied) and the events captured when the different auditing modules are licensed.

# 2

# Change Auditor for Active Directory Events

This section lists the audited events specific to Change Auditor for Active Directory and each event's corresponding severity setting. Audited events are listed in alphabetical order by facility:

- Active Directory Database
- Active Directory Federation Services - Authentication Methods
- Active Directory Federation Services - Claims Provider Trusts
- Active Directory Federation Services - Endpoints
- Active Directory Federation Services - Relying Party Trusts
- Active Directory Federation Services - Relying Party Trusts
- Dynamic Access Control
- Connection Object
- Custom AD Object Monitoring
- Custom Computer Monitoring
- Custom Group Monitoring
- Custom User Monitoring
- DNS Service
- DNS Zone
- Domain Configuration
- Dynamic Access Control
- Forest Configuration
- FRS Service
- Group Policy Item
- Group Policy Object
- IP Security
- NETLOGON Service
- NTDS Service
- Organizational Unit (OU)
- Replication Transport
- Schema Configuration
- Site Configuration
- Site Link Bridge Configuration
- Site Link Configuration

- Subnets
- SYSVOL

**NOTE:** To view a complete list of all the Change Auditor for Active Directory events, open the Audit Events page on the Administration Tasks tab in the Change Auditor client. This page contains a list of all the events available for auditing by Change Auditor for Active Directory. It also displays the facility to which the event belongs, the severity assigned to each event, if the event is enabled or disabled, and the type of Change Auditor for Active Directory license that is required to capture each event.

**IMPORTANT:** When expecting large numbers of events, it may be necessary to increase the Max Events per Connection setting in the Change Auditor client (Agent Configuration on the Administration Tasks tab) to avoid an ever-increasing backlog of events waiting to be sent from the agent to the coordinator database.

# Active Directory Database

**Table 1. Active Directory Database events**

| Event | Description | Severity |
|---|---|---|
| Active Directory database file access rights changed | Created when access to the NTDS.dit file has been changed through Access Control Settings. | High |
| Active Directory database file accessed | Created when the NTDS.dit file has been accessed. | High |
| Active Directory database file attribute changed | Created when NTDS.dit file attributes have been changed. | High |
| Active Directory database file auditing changed | Created when changes are made to the NTDS.dit auditing list on the domain controller. | High |
| Active Directory database file central access policy changed | Created when the NTDS.dit file central access policy is changed on the domain controller. | High |
| Active Directory database file classification changed | Created when the NTDS.dit file classification is changed on the domain controller. | High |
| Active Directory database file created | Created when the NTDS.dit file is created on a domain controller. | High |
| Active Directory database file deleted | Created when the NTDS.dit file is deleted on a domain controller. | High |
| Active Directory database file last write changed | Created when the contents of the NTDS.dit file are written on a domain controller. | High |
| Active Directory database file moved | Created when the NTDS.dit file is moved on a domain controller. | High |
| Active Directory database file ownership changed | Created when ownership of the NTDS.dit file has been changed. | High |
| Active Directory database file renamed | Created when the NTDS.dit file is renamed on a domain controller. | High |
| Failed Active Directory database access (Change Auditor Protection) | Created when access attempt fails on the NTDS.dit file due to Change Auditor protection. | High |
| Failed Active Directory database access (NTFS permissions) | Created when access attempt fails on the NTDS.dit file due to NTFS permission. | High |
| Failed Active Directory database access (Sharing violation) | Created when access attempt fails on the NTDS.dit file due to sharing violation. | High |

# Active Directory Federation Services - Authentication Methods

**Table 2. Active Directory Federation Services - Authentication Methods events**

| Event | Description | Severity |
|---|---|---|
| Additional authentication methods changed | Created when authentication methods are changed. | Medium |
| Additional authentication method registered | Created when authentication methods are registered. | Medium |
| Additional authentication method unregistered | Created when authentication methods are unregistered. | Medium |
| Allow additional authentication providers as primary setting changed | Created when additional authentication providers as primary setting is changed. | Medium |
| Extranet authentication methods changed | Created when extranet authentication methods are changed. | Medium |
| Intranet authentication methods changed | Created when intranet authentication methods are changed. | Medium |

# Active Directory Federation Services - Claims Provider Trusts

**Table 3. Active Directory Federation Services - Claims Provider Trusts events**

| Event | Description | Severity |
|---|---|---|
| Claims Provider Trust added | Created when the claims provider trust is added. | Medium |
| Claims Provider Trust changed | Created when the claims provider trust is changed. | Medium |
| Claims Provider Trust deleted | Created when the claims provider trust is deleted. | Medium |
| Claims Provider Trust disabled | Created when the claims provider trust is enabled. | Medium |
| Claims Provider Trust enabled | Created when the claims provider trust is disabled. | Medium |

# Active Directory Federation Services - Endpoints

**Table 4. Active Directory Federation Services - Endpoints events**

| Event | Description | Severity |
|---|---|---|
| Endpoint enabled | Created when an endpoint was enabled. | Medium |
| Endpoint disabled | Created when an endpoint was disabled. | Medium |
| Endpoint Proxy enabled | Created when an endpoint was enabled through a proxy. | Medium |
| Endpoint Proxy disabled | Created when an endpoint was disabled through a proxy. | Medium |

# Active Directory Federation Services - Relying Party Trusts

**Table 5. Active Directory Federation Services - Relying Party Trusts**

| Event | Description | Severity |
|---|---|---|
| Relying Party Trust added | Created when a relying party trust is added. | Medium |
| Relying Party Trust changed | Created when a relying party trust is changed. | Medium |
| Relying Party Trust deleted | Created when a relying party trust is deleted. | Medium |
| Relying Party Trust disabled | Created when a relying party trust is disabled. | Medium |
| Relying Party Trust enabled | Created when a relying party trust is enabled. | Medium |

# Active Directory Federation Services - Server Farm

**Table 6. Active Directory Federation Services - Server Farm**

| Event | Description | Severity |
|---|---|---|
| Server Farm Node added | Created when a server farm node is added to an Active Directory Federation Services server. | Medium |
| Server Farm Node Primary Computer Name changed | Created when a server farm node primary computer name is changed. | Medium |
| Server Farm Node Primary Computer port changed | Created when a server farm node primary computer port is changed | Medium |
| Server Farm Node removed | Created when a server farm node is removed from an Active Directory Federation Services server. | Medium |
| Server Farm Node Role changed | Created when an Active Directory Federation Services computer is changed from a primary computer to a secondary computer or a secondary computer to primary computer. | Medium |
| Server Farm Node Synchronization Frequency changed | Created when a server farm node synchronization frequency is changed. | Medium |

# Configuration Monitoring

**Table 7. Configuration Monitoring events**

| Event | Description | Severity |
|---|---|---|
| Active Directory Share Added | Created when an Active Directory share has been added to a server. | Medium |
| Active Directory Share Removed | Created when an Active Directory share has been removed from a server. | High |
| Append Parent Suffixes Option Changed | Created when the append parent suffixes of the primary DNS suffix option is changed. | Medium |
| Application Partition Replica Added | Created when a DN for an application partition is added to the msDS-hasMasterNCs attribute of an nTDSDSA object. | Medium |
| Application Partition Replica Removed | Created when a DN for an application partition is removed from the msDS-hasMasterNCs attribute of an nTDSDSA object. | High |
| Connection DNS Registration Option Changed | Created when the register connection in DNS option on a network connection is changed. | Medium |
| Connection Object Added | Created when an nTDSConnection object is added to the NTDS Settings container. | Medium |
| Connection Object Removed | Created when an nTDSConnection object is removed from the NTDS Settings container. | Medium |
| Connection-specific DNS Suffix Changed | Created when the connection-specific DNS suffix changes. | Medium |
| Contents of DNS Server List Changed | Created when a DNS server is added or removed from the DNS server list. | Medium |
| Contents of DNS Suffix List Changed | Created when a suffix is added or removed from the DNS suffix list. | Medium |
| Contents of WINS Server List Changed | Created when a server is added or removed from the WINS server list. | Medium |
| Critical Link Failures Allowed Parameter Changed | Created when the CriticalLinkFailuresAllowed parameter on a DC is changed. | Medium |
| Default Gateway Changed | Created when the default gateway changes on a network connection. | Low |
| DHCP Disabled | Created when DHCP is disabled on a network connection. | Low |
| DHCP Enabled | Created when DHCP is enabled on a network connection. | Low |
| DIT Location Changed | Created when the directory path of the DIT is changed. | Low |
| Domain Controller Added as Preferred Bridgehead Server | Created when a domain controller is configured as a preferred bridgehead server for a particular replication transport. | Medium |
| Domain Controller Moved to Another OU | Created when a domain controller is moved to another OU. | Medium |
| Domain Controller Removed as Preferred Bridgehead Server | Created when a domain controller is removed as a preferred bridgehead server for a particular replication transport. | Medium |
| Domain Controller Service Pack Applied | Created when a service pack is applied to a domain controller. | Medium |
| Domain Controller Service Pack Rolled Back | Created when a service pack is removed from a domain controller. | Medium |

**Table 7. Configuration Monitoring events**

| Event | Description | Severity |
|---|---|---|
| DS Database Logging and Recover Option Changed | Created when the logging and recovery option of Active Directory is changed. | Low |
| DS Hierarchy Table Evaluation Interval Changed | Created when the hierarchy table evaluation interval on the DC is changed. | Medium |
| DS Log File Location Changed | Created when the directory path of the DS log file is changed. | Low |
| Hotfix Applied | Created when a hot fix is applied. | Medium |
| Hotfix Rolled Back | Created when a hot fix is removed. (Disabled by Default) | Medium |
| Intersite Failures Allowed Parameter Changed | Created when the IntersiteFailuresAllowed parameter is changed on a DC. | Medium |
| IP Deny List Entry Added | Created when an entry is added to the IP deny list of an LDAP query policy object. | Medium |
| IP Deny List Entry Removed | Created when an entry is removed from the IP deny list of an LDAP query policy object. | Low |
| IPSEC Settings Changed | Created when the IPSEC settings for a network connection are changed. | Medium |
| KCC Delay After Startup Changed | Created when the amount of time the KCC delays after startup before re-computing the replication topology is changed. | Medium |
| KCC Site Generator Failover Interval Changed | Created when the interval after which a new Intersite Topology Generator (ISTG) is nominated if no ISTG identity is updated in the directory is changed. | Medium |
| KCC Site Generator Renewal Interval Changed | Created when the interval at which the Intersite Topology Generator (ISTG) publishes its identity in the directory is changed. | Medium |
| KCC Update Interval Changed | Created when the interval at which the KCC on the domain controller runs is changed. | Medium |
| Kerberos Diagnostic Log Level Changed | Created when the diagnostic log level for the Kerberos service is changed. | Medium |
| Linked Query Policy for Domain Controller Changed | Created when the lDAPAdminLimits attribute of a query policy object referred to by the querypolicyObject attribute of the nTDSDSA object for the domain controller was changed. | Low |
| Max Failure Time for Intersite Link Parameter Changed | Created when the MaxFailureTimeForIntersiteLink value is changed on a domain controller. | Medium |
| Max Failure Time for Non-critical Link Parameter Changed | Created when the Maximum Failure Time value for non-critical links is changed on a domain controller. | Medium |
| MaxFailureTimeForCritical Link Parameter Changed | Created when the MaxFailureTimeForCriticalLink parameter is changed on a domain controller. | Medium |
| Maximum Number of DS Threads Changed | Created when the number of threads used by the DS service is changed. | Medium |
| NetBIOS Setting Changed | Created when the NETBIOS setting on a network connection is changed. | Medium |
| NIC Added | Created when a NIC is added to the host computer. | Low |
| NIC Disabled | Created when a NIC is disabled on the host computer. | Medium |
| NIC Enabled | Created when a NIC is enabled on the host computer. | Medium |
| NIC Removed | Created when a NIC is removed from the host computer. | Low |

**Table 7. Configuration Monitoring events**

| Event | Description | Severity |
|---|---|---|
| Non-critical Link Failures Allowed Flag Changed | Created when the Non-critical Link Failures value is changed on a domain controller. | Low |
| Preferred Bridgehead Setting Changed | Created when the bridgeheadTransportList attribute of a server is changed. | Medium |
| Processor Speed Changed | Created when the processor speed of the DC is changed. | Low |
| Query Policy Link for Domain Controller Changed | Created when the queryPolicyObject attribute of the nTDSDSA is changed. | Low |
| Query Policy Setting Changed | Created when query policy settings of an existing query policy object have changed. | Low |
| Raw IP Allowed Protocols List Changed | Created when the contents of the Raw IP Allowed Protocols list are changed. | Medium |
| Replicator Notify Pause After Modify Delay Changed | Created when the notify pause value is changed on a domain controller. | Medium |
| Schema Modifications Allowed Flag Changed | Created when a domain controller is configured to allow schema modifications. | High |
| Static IP Address Changed | Created when the static IP address changes on a network connection. | Low |
| Subnet Mask Changed | Created when the subnet mask changes on a network connection. | Low |
| SYSVOL Location Changed | Created when the SYSVOL location is changed on a domain controller. | Low |
| TCP Allowed Port List Changed | Created when the contents of the TCP Allowed Port list are changed. | Medium |
| TCP/IP Filtering Changed | Created when the TCP/IP Filtering option is changed on a network connection. | Medium |
| UDP Allowed Port List Changed | Created when the contents of the UDP Allowed Port list are changed. | Medium |
| Update DNS on All Adapters Setting Changed | Created when Active Directory's setting that controls the adapters on which a DC updates DNS is changed. | Medium |
| Use Connection Suffix in DNS Registration Option Changed | Created when the use this connection's DNS suffix in DNS registration option is changed. | Medium |
| Use LMHOSTS Option Changed | Created when the LMHOSTS option on a network connection is changed. | Low |
| Use of Dynamic DNS Changed | Created when Active Directory's use of dynamic DNS has been changed. | Medium |
| Use Primary and Connection Specific Suffixes Flag Changed | Created when the primary and connection-specific suffixes flag changes on a domain controller. | Medium |

# Connection Object

**Table 8. Connection Object events**

| Event | Description | Severity |
|---|---|---|
| Connection Object From-server Changed | Created when the from-server of a connection object is changed. | Medium |
| Connection Object Schedule Changed | Created when a change is detected in the schedule attribute of a connection object. | Medium |
| Connection Object Transport Changed | Created when the transport type of a connection object is changed. | Medium |

# Custom AD Object Monitoring

**Table 9. Custom AD Object Monitoring events**

| Event | Description | Severity |
|---|---|---|
| <*Object*> <*Attribute*> Changed | Created when an attribute changes on an object that the user has opted to audit using the Active Directory Attribute Auditing page on the Administration Tasks tab in the Change Auditor client.<br>**NOTE:** Starting with Change Auditor 5.6, the attributes that can be set using the User Properties dialog in Active Directory Users and Computers (ADUC) are audited by default. If you have added custom attribute auditing for any of these attributes, you receive two events when changes to these user attributes are made:<br>• A Custom User Monitoring event for the built-in user attribute event.<br>• A Custom AD Object Monitoring event for the custom attribute event (user attribute specified on Active Directory Attribute Auditing page).<br>To eliminate duplicate events, you can remove the user attribute from the Active Directory Attribute Auditing page which prevents the custom attribute event from being generated. | Medium |
| Computer Changed | Created when an object is added, moved, removed, or renamed in a computer object. | Medium |
| Group Changed | Created when an object is added, moved, removed, or renamed in a group object. | Medium |
| User Changed | Created when an object is added, moved, removed, or renamed in a user object. | Medium |

# Custom Computer Monitoring

**Table 10. Custom Computer Monitoring events**

| Event | Description | Severity |
|---|---|---|
| AdminCount attribute changed on computer object | Created when the adminCount attribute is changed on a computer. | Medium |
| Computer Account Disabled | Created when the computer account is disabled. | Medium |
| Computer Account Enabled | Created when the computer account is enabled. | Medium |
| Computer Added | Created when a computer account object is added to the domain. | Medium |
| Computer Moved | Created when a computer account object is moved within the domain. | Medium |
| Computer Removed | Created when a computer account object is removed from the domain. | Medium |
| Computer Renamed | Created when a computer account object is renamed. | Medium |
| Computer Service Pack Applied | Created when a service pack is applied to the computer. | Medium |
| Computer Service Pack Rolled Back | Created when a service pack is uninstalled from the computer. | Medium |
| DACL Changed on Computer Object | Created when the DACL is changed for the computer object.<br>**NOTE:** Change Auditor access control list (ACL) events (discretionary access control list (DACL) and system access control list (SACL) changes), will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes. | Medium |
| Dynamic Computer Object Added | Created when a dynamic computer object is added to a container. | Medium |
| Dynamic Computer Object Changed | Created when a dynamic computer object is modified. | Medium |
| Dynamic Computer Object Removed | Created when a dynamic computer object is removed from a container. | Medium |
| Inheritance Setting Changed on Computer Object | Created when the inheritance setting of a computer object is changed. | Medium |

Table 10. Custom Computer Monitoring events

| Event | Description | Severity |
|---|---|---|
| Irregular domain controller registration activity detected | Created when irregular domain controller registration activity detected on a computer.<br>**NOTE:** This event indicates the addition of a replication specific servicePrincipalName attribute value to a computer object that is not a child of the domain controllers organizational unit and could identify a possible DCShadow threat.<br>DCShadow is a command within Mimikatz that simulates the behavior of a domain controller to push changes to an Active Directory domain through replication, bypassing most of the common security controls.<br>The following SPN serviceclass values are considered suspicious, and the event is generated when they are added to the servicePrincipalName attribute:<br>• GC/<br>• E3514235-4B06-11D1-AB04-00C04FC2DCD2/ | High |
| Owner Changed on Computer Object | Created when the owner of a computer object is changed. | Medium |

# Custom Group Monitoring

Table 11. Custom Group Monitoring events

| Event | Description | Severity |
|---|---|---|
| AdminCount attribute changed on group object | Created when the adminCount attribute is changed on a group. | Medium |
| DACL Changed on Group Object | Created when the DACL is changed for the group object.<br>**NOTE:** Change Auditor access control list (ACL) events (discretionary access control list (DACL) and system access control list (SACL) changes), do not report inherited access control entry (ACE) changes. This event does not report inherited ACL changes. | High |
| Different domain SID added to group object sIDHistory | Created when a SID from a different domain is added to the sIDHistory attribute of a group. | Medium |
| Different domain SID removed from group object sIDHistory | Created when a SID from a different domain is removed from the sIDHistory attribute of a group. | Medium |
| Dynamic Group Object Added | Created when a dynamic group object is added to a container. | Medium |
| Dynamic Group Object Changed | Created when a dynamic group object is modified. | Medium |
| Dynamic Group Object Removed | Created when a dynamic group object is removed from a container. | Medium |
| Inheritance Setting Changed on Group Object | Created when the inheritance setting of a group object is changed. | High |
| Group Member-Of Added | Created when a group is added to another group. | Medium |
| Group Member-Of Removed | Created when a group is removed from another group. | Medium |
| Group Object Added | Created when a new group is added to a container. | Medium |

**Table 11. Custom Group Monitoring events**

| Event | Description | Severity |
|---|---|---|
| Group Object Moved | Created when a group is moved to or from a container. | Medium |
| Group Object Removed | Created when a group is removed from a container. | Medium |
| Group Renamed | Created when a group is renamed. | Medium |
| Group samAccountName Changed | Created when the samAccountName attribute for a group is changed. | Medium |
| Group Type Changed | Created when the group type for a group is changed. | Medium |
| Member Added to Group | Created when a new member is added to a group. | Medium |
| Member Removed from Group | Created when a member is removed from a group. | Medium |
| Nested Member Added to Group | Created when a member is added to a nested group within a monitored group. | Medium |
| Nested Member Removed from Group | Created when a member is removed from a nested group within a monitored group. | Medium |
| Owner Changed on Group Object | Created when the owner of a group object is changed. | Medium |
| Same domain SID added to group object sIDHistory | Created when a SID from the same domain is added to the sIDHistory attribute of a group. | High |
| Same domain SID removed from group object sIDHistory | Created when a SID from the same domain is removed from the sIDHistory attribute of a group. | Medium |
| Well-known SID added to group object sIDHistory | Created when a well-known SID is added to the sIDHistory attribute of a group. | High |
| Well-known SID removed from group object sIDHistory | Created when a well-known SID is removed from the sIDHistory attribute of a group. | Medium |

# Custom User Monitoring

**Table 12. Custom User Monitoring events**

| Event | Description | Severity |
|---|---|---|
| AdminCount attribute changed on user object | Created when the adminCount attribute is changed on a user. | Medium |
| Active Session Limit Changed for User Object | Created when the Active session limit setting is changed in the Sessions settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Allow Reconnection Changed for User Object | Created when the Allow reconnection option is changed in the Sessions settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| City Changed on User Object | Created when the City field is changed in the Address settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Company Changed for User Object | Created when the Company field is changed in the Organization settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Connect Client Drives at Logon Changed for User Object | Created when the Connect Client Drives at Logon option is changed in the Environment settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |

**Table 12. Custom User Monitoring events**

| Event | Description | Severity |
|---|---|---|
| Connect Client Printers at Logon Changed for User Object | Created when the Connect Client Printers at Logon option is changed in the Environment settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Country/Region Changed on User Object | Created when the Country/Region field is changed in the Address settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| DACL Changed on User Object | Created when the DACL is changed for a user object.<br>**NOTE:** Change Auditor access control list (ACL) events (discretionary access control list (DACL) and system access control list (SACL) changes), do not report inherited access control entry (ACE) changes. This event does not report inherited ACL changes. | High |
| Default to Main Client Printer Changed for User Object | Created when the Default to Main Client Printer at Logon option is changed in the Environment settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Delegation Authentication Protocol Changed for User Object | Created when the Delegation protocol is changed in the Delegation settings for a user object in the Active Directory Users and Computers administrative tool.<br>**NOTE:** The Delegation settings tab only appears when the AD User and Computers 'Advanced Features' option is enabled, and only on accounts with registered SPNs in domains with Windows Server® 2003 (or higher) Functional Level. | Medium |
| Department Changed for User Object | Created when the Department field is changed in the Organization settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Description Changed on User Object | Created when the Description field is changed in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Different domain SID added to user object sIDHistory | Created when a SID from a different domain is added to the sIDHistory attribute of a user. | Medium |
| Different domain SID removed from user object sIDHistory | Created when a SID from a different domain is removed from the sIDHistory attribute of a user. | Medium |
| Direct Report Added to User Object | Created when the user is added as the 'Manager' in the Organization settings for another user object in the Active Directory Users and Computers administrative tool. | Medium |
| Direct Report Removed from User Object | Created when the user is removed as the 'Manager' in the Organization settings for another user object in the Active Directory Users and Computers administrative tool. | Medium |
| Display Name Changed on User Object | Created when the Display Name field is changed in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Domain User Renamed | Created when a user's domain user name is changed. | Medium |
| Dynamic User Object Added | Created when a dynamic user object is added to a container. | Medium |
| Dynamic User Object Changed | Created when a dynamic user object is modified. | Medium |
| Dynamic User Object Removed | Created when a dynamic user object is removed from a container. | Medium |

**Table 12. Custom User Monitoring events**

| Event | Description | Severity |
|---|---|---|
| Enable Remote Control Changed for User Object | Created when the Enable remote control option is changed in the Remote Control settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| End a Disconnected Session Changed for User Object | Created when the End a disconnected session setting is changed in the Sessions settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Fax Number Changed on User Object | Created when the Fax field is changed in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| First Name Changed on User Object | Created when the First Name field is changed in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Home Folder Changed on User Object | Created when the contents of either of the Home Folder fields (local or connect) are changed in the Profile settings for user in the Active Directory Users and Computers. | Medium |
| Home Folder Mapped Drive Changed on User Object | Created when the Home Folder: Connect mapped drive field is changed in the Profile settings for a user in Active Directory Users and Computers. | Medium |
| Home Telephone Number Changed on User Object | Created when the Home field is changed in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Idle Session Limit Changed for User Object | Created when the Idle session limit setting is changed in the Sessions settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Inheritance Setting Changed on User Object | Created when the inheritance setting of a user object is changed. | High |
| Initials Changed on User Object | Created when the Initials field is changed in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| IP Phone Number Changed on User Object | Created when the IP Phone field is changed in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Last Name Changed on User Object | Created when the Last Name field is changed in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Level of Control Changed on User Object | Created when the Level of control option is changed in the Remote Control settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Logon Script Changed on User Object | Created when the Logon Script field is changed in the Profile settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Manager Changed for User Object | Created when the Manager field is changed in the Organization settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Mobile Number Changed on User Object | Created when the Mobile field is changed in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |

**Table 12. Custom User Monitoring events**

| Event | Description | Severity |
|---|---|---|
| Office Changed on User Object | Created when the Office field is changed in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Fax Number Added to User Object | Created when a number is added to the Fax: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Fax Number Removed from User Object | Created when a number is removed from the Fax: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Home Telephone Number Added to User Object | Created when a number is added to the Home: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Home Telephone Number Removed from User Object | Created when a number is removed from the Home: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other IP Phone Number Added to User Object | Created when a number is added to the IP Phone: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other IP Phone Number Removed from User Object | Created when a number is removed from the IP Phone: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Mobile Number Added to User Object | Created when a number is added to the Mobile: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Mobile Number Removed from User Object | Created when a number is removed from the Mobile: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Pager Number Added to User Object | Created when a number is added to the Pager: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Pager Number Removed from User Object | Created when a number is removed from the Pager: Other list in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Telephone Number Added to User Object | Created when a number is added to the Telephone Number: Other list in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Telephone Number Removed from User Object | Created when a number is removed from the Telephone Number: Other list in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |

**Table 12. Custom User Monitoring events**

| Event | Description | Severity |
|---|---|---|
| Other Web Page Added to User Object | Created when a web page is added to the Web Page: Other list in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Other Web Page Removed from User Object | Created when a web page is removed from the Web Page: Other list in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Owner Changed on User Object | Created when the owner of a user object is changed. | Medium |
| P.O. Box Changed on User Object | Created when the P.O. Box field is changed in the Address settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Pager Number Changed on User Object | Created when the Pager field is changed in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Partition Set Changed for User Object | Created when the Partition set setting is changed in the COM+ settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Primary Group ID Changed for User Object | Created when the Primary group setting is changed in the Member Of settings for a user object in the Active Directory Users and Computers administrative tool.<br>**NOTE:** This setting is only available when a global or universal security group in the user's domain, different than the current primary group, is selected in the Member Of list. | Medium |
| Profile Path Changed on User Object | Created when the Profile Path field is changed in the Profile settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Published Certificate Added to User Object | Created when a certificate is added to the List of X509 certificates published for the user account field in the Published Certificate settings for a user in Active Directory User and Computers. | Medium |
| Published Certificate Removed from User Object | Created when a certificate is removed from the List of X509 certificates published for the user account field in the Published Certificate settings for a user in the Active Directory User and Computers administrative tool. | Medium |
| Require User's Permission Changed for User Object | Created when the Require user's permission option is changed in the Remote Control settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Service Added to Delegation List of User Object | Created when a service is added to the Services list in the Delegation settings for a user object in the Active Directory Users and Computers administrative tool.<br>**NOTE:** The Delegation settings tab only appears when the AD User and Computers 'Advanced Features' option is enabled, and only on accounts with registered SPNs in domains with Windows Server 2003 (or higher) Functional Level. | Medium |

**Table 12. Custom User Monitoring events**

| Event | Description | Severity |
|---|---|---|
| Service Removed from Delegation List of User Object | Created when a service is removed from the Services list in the Delegation settings for a user object in the Active Directory Users and Computers administrative tool.<br>**NOTE:** The Delegation settings tab only appears when the AD User and Computers 'Advanced Features' option is enabled, and only on accounts with registered SPNs in domains with Windows Server 2003 (or higher) Functional Level. | Medium |
| Same domain SID added to user object sIDHistory | Created when a SID from the same domain is added to the sIDHistory attribute of a user. | High |
| Same domain SID removed from user object sIDHistory | Created when a SID from the same domain is removed from the sIDHistory attribute of a user. | Medium |
| Starting Directory Changed for User Object | Created when the Start In field is changed in the Environment settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Starting Program Changed for User Object | Created when the Program File Name field is changed in the Environment settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| State/Province Changed on User Object | Created when the State/Province field is changed in the Address settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Street Address Changed on User Object | Created when the Street field is changed in the Address settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Telephone Notes Changed on User Object | Created when the Notes field is changed in the Telephone settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Telephone Number Changed on User Object | Created when the Telephone number field is changed in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Terminal Services Home Folder Drive Changed | Created when the Terminal Services home folder drive is changed in the Terminal Services Profile settings for an Active Directory® user object. | Medium |
| Terminal Services Home Folder Path Changed | Created when the Terminal Services home folder path is changed in the Terminal Services Profile settings for an Active Directory user object. | Medium |
| Terminal Services Home Folder Type Changed | Created when the Terminal Services home folder type is changed in the Terminal Services Profile settings for an Active Directory user object. | Medium |
| Terminal Services Logon Permission Changed | Created when the Deny this user permission to log on to any Terminal Server option is changed in the Terminal Services Profile settings for an Active Directory® user object. | Medium |
| Terminal Services User Profile Path Changed | Created when the Terminal Services user profile path is changed in the Terminal Services Profile settings for an Active Directory user object. | Medium |
| Title Changed for User Object | Created when the Title field is changed in the Organization settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| User Account Disabled | Created when a user account is disabled. | Medium |

**Table 12. Custom User Monitoring events**

| Event | Description | Severity |
|---|---|---|
| User Account Enabled | Created by default when a user account is enabled, including when the account is created. | Medium |
| User Account is Sensitive and Cannot be Delegated Option Changed | Created when the User Account is Sensitive and Cannot be Delegated option is changed on the user object account options. | Medium |
| User Account is Trusted for Delegation Option Changed | Created when the User Account is Trusted for Delegation option is changed on the user object account options. | Medium |
| User Account Locked | Created when a user's account is locked. | Medium |
| User Account Re-enabled | Created when an existing user account is enabled after having been disabled. (Disabled by default)<br>**NOTE:** This event is intended for users that prefer to turn off the 'User Account Enabled' event so it is not generated when a user account is created. | Medium |
| User Account Type Changed | Created when a user object account option is changed. | Medium |
| User Account Unlocked | Created when a user's account is unlocked. | Medium |
| User accountExpires Changed | Created when the accountExpires attribute for a user object is changed. | Medium |
| User Dial-in Callback Options Changed | Created when the user Dial-In callback options user attribute has changed. | Medium |
| User Dial-in Remote Access Permission Changed | Created when the Dial-in Remote Access Permission attribute for the user object has changed. | Medium |
| User Dial-in Static IP Address Changed | Created when User Dial-in Static Address user attribute has changed. | Medium |
| User Dial-in Static Route Added | Created when the User Dial-in Static Route added attribute has been changed | Medium |
| User Dial-in Static Route Removed | Created when the User Dial-in Static Route removed attribute has been changed. | Medium |
| User Dial-in Verify Caller-ID Changed | Created when the user Dial-in verify caller-ID user attribute has been changed. | Medium |
| User Do Not Require Kerberos Preauthentication Option Changed | Created when the User Do Not Require Kerberos Preauthentication option is changed on the user object account options. | Medium |
| User logonHours Changed | Created when the logonHours attribute for a user object is changed. | Medium |
| User Member-Of Added | Created when a user is added to a group. | Medium |
| User Member-Of Removed | Created when a user is removed from a group. | Medium |
| User Must Change Password at Next Logon Option Changed | Created when the User Must Change Password at the Next Logon option is changed in the Account settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| User Object Added | Created when a user is added to a container. | Medium |
| User Object Moved | Created when a user is moved to or from a container. | Medium |
| User Object Removed | Created when a user is removed from a container. | Medium |
| User Password Changed | Created when a user's password is changed. | Medium |
| User Password Changed by Non-owner | Created when a user's password is changed by someone other than the account owner. | Medium |
| User Password Never Expires Option Changed | Created when the Password Never Expires option is changed on the user object account options. | Medium |

**Table 12. Custom User Monitoring events**

| Event | Description | Severity |
|---|---|---|
| User samAccountName Changed | Created when the User log on name (pre-Windows® 2000) field (sAMAccountname attribute) is changed in the Account settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| User Smart Card is Required for Interactive Logon Option Changed | Created when the User Smart Card is Required for Interactive Logon option is changed on the user object account options. | Medium |
| User Store Password Using Reversible Encryption Option Changed | Created when the User Store Password Using Reversible Encryption option is changed on the user object account options. | Medium |
| User Use DES Encryption Types for This Account Option Changed | Created when the User Use DES Encryption Types for this Account option is changed on the user object account options. | Medium |
| User userPrincipalName Changed | Created when the userPrincipalName attribute for a user object is changed. | Medium |
| User userWorkstations Added | Created when a computer is added to the userWorkstations attribute of a user object. | Medium |
| User userWorkstations Removed | Created when a computer is removed from the userWorkstations attribute of a user object. | Medium |
| ServicePrincipalName added to user object | Created when servicePrincipalName added to a user object. | Medium |
| ServicePrincipalName removed from user object | Created when servicePrincipalName removed from a user object. | Medium |
| User's ability to update their password has changed | Created when the user’s ability to update their password has changed. | High |
| User's home folder requirement has changed | Created when the UserAccountControl attribute property flag (ADS_UF_HOMEDIR_REQUIRED) has changed. This flag determines whether a user must have a home folder. This value can be set to:<br>• Required<br>• Not required | Medium |
| User's requirement for a password has changed | Created when the UserAccountControl attribute property flag (ADS_UF_PASSWD_NOTREQD) has changed. This flag determines whether a user must have a password. This value can be set to:<br>• Required<br>• Not required | High |
| Web Page Changed on User Object | Created when the Web Page field is changed in the General settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Well-known SID added to user object sIDHistory | Created when a well-known SID is added to the sIDHistory attribute of a user. | High |
| Well-known SID removed from user object sIDHistory | Created when a well-known SID is removed from the sIDHistory attribute of a user. | Medium |
| When Session Limit is Reached Changed for User Object | Created when the When a session limit is reached or connection is broken option is changed for a user object in the Active Directory Users and Computers administrative tool. | Medium |
| Zip/Postal Code Changed on User Object | Created when the Zip/Postal Code field is changed in the Address settings for a user object in the Active Directory Users and Computers administrative tool. | Medium |

# DNS Service

**Table 13. DNS Service events**

| Event | Description | Severity |
|---|---|---|
| Address Answer Limit Changed | Created when the Answer section address limit of the DNS service is changed. | Medium |
| AutoConfigFileZones Setting Changed | Created when the Automatic Configuration of Standard Primary Zones setting of the DNS service is changed. | Medium |
| BIND Secondaries Flag Changed | Created when the Bind secondaries setting of the DNS server is changed. | Medium |
| Database Directory Setting Changed | Created when the Database Directory setting of the DNS service is changed. | Medium |
| Default Aging State Setting Changed | Created when the Default Aging State of the DNS service is changed. | Medium |
| Disable Auto Reverse Zones Setting Changed | Created when the Disable Auto Reverse Zones setting of the DNS service is changed. | Medium |
| DisableNSRecordsAutoCreation | Created when the DisableNSRecordsAutoCreation registry entry is added, removed, or changed. | Medium |
| DNS Service Added | Created when a DNS service is added to a domain controller. | Medium |
| DNS Service Removed | Created when a DNS service is removed from a domain controller. | Medium |
| Enable Netmask Ordering Flag Changed | Created when the Netmask ordering setting of the DNS server is changed. | Medium |
| Enable Scavenging of Stale Resource Record Setting Changed | Created when the Automatic scavenging of stale resource records setting of the DNS server is changed. | Medium |
| Event Log Level Changed | Created when the Event Log Level setting of the DNS service is changed. | Medium |
| Fail On Load Flag Changed | Created when the Fail on load if bad zone data setting of the DNS server is changed. | Medium |
| Forward Delegations Setting Changed | Created when the Forward Delegations setting of the DNS service is changed. | Medium |
| Forwarder Timeout Changed | Created when the Number of seconds before forward queries time out setting of the DNS server is changed. | Medium |
| Forwarders List Changed | Created whenever an entry is added or removed from the Forwarders list. | Medium |
| IsSlave Setting Changed | Created when the IsSlave setting of the DNS service is changed. | Medium |
| Listen-on Interfaces Changed | Created whenever an entry is added or removed from the listen on interfaces list. | Medium |
| Log File Path Changed | Created when the Log File Path of the DNS service is changed. | Low |
| LogFileMaxSize Setting Changed | Created when the LogFileMaxSize setting of the DNS service is changed. | Low |
| Loose Wildcarding Setting Changed | Created when the Loose Wildcarding setting of the DNS service is changed. | Medium |
| Max Cache TTL Setting Changed | Created when the Max Cache TTL setting of the DNS service is changed. | Medium |
| Name Checking Option Changed | Created when the name checking option of the DNS server is changed. | Medium |

**Table 13. DNS Service events**

| Event | Description | Severity |
|---|---|---|
| No-refresh Interval Changed | Created when the No-refresh interval setting of the DNS server is changed. | Medium |
| Publish Addresses List Changed | Created when the Publish Addresses list of the DNS service is changed. | Medium |
| Publish Autonet Setting Changed | Created when the Publish Autonet setting of the DNS service is changed. | Medium |
| Recursion Flag Changed | Created when the Disable recursion setting of the DNS server is changed. | Medium |
| Recursion Retry Setting Changed | Created when the Recursion Retry setting of the DNS service is changed. | Medium |
| Recursion Timeout Setting Changed | Created when the Recursion Timeout setting of the DNS service is changed. | Medium |
| Refresh Interval Changed | Created when the Refresh interval setting of the DNS server is changed. | Medium |
| Round-robin Flag Changed | Created when the Enable round robin setting of the DNS server is changed. | Medium |
| RPC Protocol Setting Changed | Created when the RPC Protocol setting of the DNS service is changed. | Medium |
| Scavenging Period Changed | Created when the scavenging period setting of the DNS server is changed. | Medium |
| Secure Cache Against Pollution Flag Changed | Created when the Secure cache against pollution setting of the DNS server is changed. | Medium |
| Send Port Setting Changed | Created when the Send Port setting of the DNS service is changed. | Medium |
| Service Log Level Changed | Created when the diagnostic log level for a DNS service is changed. | Medium |
| Transfer Connect Timeout Setting Changed | Created when the Transfer Connect Timeout setting of the DNS service is changed. | Medium |
| Update Options Setting Changed | Created when the Update Options setting of the DNS service is changed. | Medium |
| WriteAuthorityNS Setting Changed | Created when the WriteAuthorityNS setting of the DNS service is changed. | Medium |
| Zone Added | Created when a new zone is added. | Medium |
| Zone Deleted | Created when a zone is deleted. | Medium |
| Zone Load Mode Changed | Created when the Load zone data on startup setting of the DNS server is changed. | Medium |

# DNS Zone

**Table 14. DNS Zone events**

| Event | Description | Severity |
|---|---|---|
| Aging No-refresh Interval Changed | Created when the aging no-refresh interval of the zone is changed. | Medium |
| Aging Refresh Interval Changed | Created when the aging refresh interval of the zone is changed. | Medium |

Table 14. DNS Zone events

| Event | Description | Severity |
|---|---|---|
| DNS AAAA Record Added | Created when the DNS host (AAAA) record is added to a zone. (Disabled by default)<br>**NOTE:** This event is captured for Active Directory® integrated DNS zones only. | Low |
| DNS AAAA Record Modified | Created when the DNS host (AAAA) record in a zone is modified. (Disabled by default)<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS AAAA Record Removed | Created when the DNS host (AAAA) record is removed from a zone. (Disabled by default)<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS A Record Added | Created when the DNS host (A) record is added to a zone. (Disabled by default)<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS A Record Modified | Created when the DNS host (A) record in a zone is modified. (Disabled by default)<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS A Record Removed | Created when the DNS host (A) record is removed from a zone. (Disabled by default)<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS CNAME Record Added | Created when the DNS CNAME (Alias) record is added to a zone.<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS CNAME Record Removed | Created when the DNS CNAME (Alias) record is removed from a zone.<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS MX Record Added | Created when the DNS MX (Mail Exchange) record is added to a zone.<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS MX Record Removed | Created when the DNS MX (Mail Exchange) record is removed from a zone.<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS PTR Record Added | Created when the DNS PTR (Pointer) record is added to a zone. (Disabled by default)<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS PTR Record Removed | Created when the DNS PTR (Pointer) record is removed from a zone. (Disabled by default)<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |

Table 14. DNS Zone events

| Event | Description | Severity |
|---|---|---|
| DNS SRV Record Added | Created when the DNS SRV (Service Locator) record is added to a zone.<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| DNS SRV Record Removed | Created when the DNS SRV (Service Locator) record is removed from a zone.<br>**NOTE:** This event is captured for Active Directory integrated DNS zones only. | Low |
| Expires After Period Changed | Created when the expires-after period has changed in the zone.<br>Disabled by default. | Medium |
| Name Server Added | Created when a name server is added to the zone.<br>Disabled by default. | Medium |
| Name Server Removed | Created when a name server is removed from the zone.<br>Disabled by default. | Medium |
| Primary Server Changed | Created when the primary server in the SOA has changed in the zone.<br>Disabled by default. | Medium |
| Retry Interval Changed | Created when the retry interval has changed in the zone.<br>Disabled by default. | Medium |
| WINS Forwarding Flag Disabled | Created when WINS forwarding flag is disabled in the zone.<br>Disabled by default. | Low |
| WINS Forwarding Flag Enabled | Created when WINS forwarding flag is enabled in the zone.<br>Disabled by default. | Low |
| WINS Forwarding Host List Changed | Created when the WINS forwarding host list has changed in the zone.<br>Disabled by default. | Low |
| Zone Allow Dynamic Updates Flag Changed | Created when the allow dynamic updates flag is changed in the zone. | Medium |
| Zone Default TTL Changed | Created when the default TTL has changed in the zone.<br>Disabled by default. | Medium |
| Zone Delegation Added | Created when a zone is delegated.<br>Disabled by default. | Medium |
| Zone Delegation Removed | Created when a zone delegation is removed.<br>Disabled by default. | Medium |
| Zone Refresh Interval Changed | Created when the refresh interval has changed in the zone.<br>Disabled by default. | Medium |
| Zone Replication Scope Changed | Created when the zone replication scope is changed. | Medium |
| Zone Scavenging Flag Changed | Created when scavenging is enabled or disabled in the zone. | Medium |
| Zone Storage Changed | Created when the zone storage is changed. | Medium |
| Zone Transfer Flag Changed | Created when the zone transfer flag of the zone is changed. | Medium |

Table 14. DNS Zone events

| Event | Description | Severity |
|---|---|---|
| Zone Transfer Host List Changed | Created when the zone transfer host list of the zone is changed. | Medium |
| Zone Type Changed | Created when the zone type is changed. | Medium |

# Domain Configuration

Table 15. Domain Configuration events

| Event | Description | Severity |
|---|---|---|
| Allowed DNS Suffix List Changed for Domain | Created when a new value is added to or removed from the list of allowed DNS suffixes for a domain. | Medium |
| DACL Changed on AdminSDHolder Object | Created when the DACL is changed for an object located at CN=AdminSDHolder,CN=System, DC=<*Domain Name*>.<br>**NOTE:** Change Auditor access control list (ACL) events (discretionary access control list (DACL) and system access control list (SACL) changes), will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes. | High |
| DACL Changed on Domain Object | Created when the DACL is changed on a domain object.<br>**NOTE:** Change Auditor access control list (ACL) events (discretionary access control list (DACL) and system access control list (SACL) changes), will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes. | High |
| Default Quota for Partition Changed | Created when the default object quota for the Configuration NC, a domain NC, or an application partition is changed. | Medium |
| Domain Controller Added to Domain | Created when a new domain controller is promoted into the domain. | Medium |
| Domain Controller Removed from Domain | Created when a domain controller is demoted from the domain. | Medium |
| Domain Controller Renamed | Created when a domain controller is renamed. | Medium |
| Domain Functional Level Changed | Created when the domain functional level is changed. | Medium |
| Domain Group Policy Order Changed | Created when the list of group policies linked to a domain is re-ordered. | Medium |
| Guest Account Disabled | Created when the Guest account is disabled in a domain. | Medium |
| Guest Account Enabled | Created when the Guest account is enabled in a domain. | Medium |
| Infrastructure FSMO Role Owner Moved | Created when the infrastructure FSMO role owner is changed from one DC to another. | High |
| Inheritance Setting Changed on AdminSDHolder Object | Created when the inheritance setting of an AdminSDHolder object is changed. | High |
| Object Quota Added | Created when a new object quota is added to an NC. | Medium |
| Object Quota Removed | Created when an object quota is removed from an NC. | Medium |

Table 15. Domain Configuration events

| Event | Description | Severity |
|---|---|---|
| PDC FSMO Role Owner Moved | Created when the PDC FSMO role owner is changed from one DC to another. | High |
| Quota Security Principal Changed | Created when the security principal for an existing quota is changed. | Medium |
| Quota Value Changed | Created when the quota value for an existing quota is changed. | Medium |
| Read-Only Domain Controller Added to Domain | Created when a Read-Only Domain Controller is added to a domain. | Medium |
| Read-Only Domain Controller Removed from Domain | Created when a Read-Only Domain Controller is demoted. | Medium |
| Read-Only Domain Controller Renamed | Created when a Read-Only Domain Controller is renamed. | Medium |
| RID FSMO Role Owner Moved | Created when the RID FSMO role owner is changed from one DC to another. | High |
| Tombstone Quota Factor for Partition Changed | Created when the quota factor for tombstone objects is changed for the Configuration NC, a domain NC, or an application partition. | Medium |
| Trust Added | Created when a Trust is created between 2 domains. | Medium |
| Trust Removed | Created when a Trust is removed. | High |

# Dynamic Access Control

**NOTE:** Dynamic Access Control is available in Windows® Server 2012; therefore, the events in this facility do not apply to earlier versions of Windows Server.

Table 16. Dynamic Access Control events

| Event | Description | Severity |
|---|---|---|
| Central Access Policy Created | Created when a Central Access Policy is created. | Medium |
| Central Access Policy Description Changed | Created when the description of a Central Access policy is changed. | Medium |
| Central Access Policy Deleted | Created when a Central Access Policy is deleted. | Medium |
| Central Access Policy Permission Changed | Created when the permission of a Central Access Policy is changed. | High |
| Central Access Policy Rule Added | Created when a rule is added to a Central Access Policy. | Medium |
| Central Access Policy Rule Changed | Created when a rule for a Central Access Policy is changed. | Medium |
| Central Access Policy Rule Removed | Created when a rule is removed from a Central Access Policy. | Medium |
| Central Access Rule Created | Created when a central access rule is created. | Medium |
| Central Access Rule Description Changed | Created when the description of a central access rule is changed. | Medium |
| Central Access Rule Deleted | Created when a central access rule is deleted. | Medium |
| Central Access Rule Effective Permission Changed | Created when the effective permission of a central access rule is changed. | High |

**Table 16. Dynamic Access Control events**

| Event | Description | Severity |
|---|---|---|
| Central Access Rule Permission Changed | Created when the permission of a central access rule is changed. | High |
| Central Access Rule Proposed Permission Changed | Created when the proposed permission of a central access rule is changed. | High |
| Central Access Rule Target Resource Changed | Created when the target resource of a central access rule is changed. | Medium |
| Claim Type AD Attribute Changed | Created when an AD attribute for a claim type is changed. | Medium |
| Claim Type Class Added | Created when a claim type class is added. | Medium |
| Claim Type Class Changed | Created when a claim type class is changed. | Medium |
| Claim Type Class Removed | Created when a claim type class is removed. | Medium |
| Claim Type Created | Created when a claim type is created. | Medium |
| Claim Type Deleted | Created when a claim type is deleted. | Medium |
| Claim Type Description Changed | Created when the description of a claim type is changed. | Medium |
| Claim Type Disabled | Created when a claim type is disabled. | Medium |
| Claim Type Display Name Changed | Created when the display name of a claim type is changed. | Medium |
| Claim Type Enabled | Created when a claim type is enabled. | Medium |
| Claim Type Permission Changed | Created when the permission of a claim type is changed. | High |
| Claim Type Suggested Values Changed | Created when the suggested values of a claim type are changed. | Medium |
| Reference Resource Property Created | Created when a reference resource property is created. | Medium |
| Reference Resource Property Deleted | Created when a reference resource property is deleted. | Medium |
| Reference Resource Property Description Changed | Created when the description of a reference resource property is changed. | Medium |
| Reference Resource Property Disabled | Created when a reference resource property is disabled. | Medium |
| Reference Resource Property Display Name Changed | Created when the display name of a reference resource property is changed. | Medium |
| Reference Resource Property Enabled | Created when a reference resource policy is enabled. | Medium |
| Reference Resource Property Permission Changed | Created when the permission of a reference resource policy is changed. | High |
| Resource Property Created | Created when a resource property is created. | Medium |
| Resource Property Deleted | Created when a resource property is deleted. | Medium |
| Resource Property Description Changed | Created when the description for a resource property is changed. | Medium |
| Resource Property Disabled | Created when a resource property is disabled. | Medium |
| Resource Property Display Name Changed | Created when the display name for a resource property is changed. | Medium |
| Resource Property Enabled | Created when a resource property is enabled. | Medium |
| Resource Property Permission Changed | Created when the permission for a resource property is changed. | High |
| Resource Property Suggested Values Changed | Created when the suggested values for a resource property are changed. | Medium |
| Resource Property List Created | Created when a resource property list is created. | Medium |

Table 16. Dynamic Access Control events

| Event | Description | Severity |
|---|---|---|
| Resource Property List Deleted | Created when a resource property list is deleted. | Medium |
| Resource Property List Description Changed | Created when the description of a resource property list is changed. | Medium |
| Resource Property List Member Added | Created when a member is added to a resource property list. | Medium |
| Resource Property List Member Changed | Created when a member of a resource property list is changed. | Medium |
| Resource Property List Member Removed | Created when a member is removed from a resource property list. | Medium |
| Resource Property List Permission Changed | Created when the permission of a resource property list is changed. | High |

# Forest Configuration

Table 17. Forest Configuration events

| Event | Description | Severity |
|---|---|---|
| Alternate UPN Suffix Added to Enterprise | Created when an entry is added to the list of alternate UPN suffixes available for user names. | Medium |
| Alternate UPN Suffix Removed from Enterprise | Created when an entry is removed from the list of alternate UPN suffixes available for user names. | Medium |
| Cross-forest Trust Added | Created when a trust is created between 2 forests. | Medium |
| Cross-forest Trust Removed | Created when a trust is removed between 2 forests. | High |
| Domain Added | Created when a domain is added to the partitions container. | High |
| Domain FSMO Role Owner Moved | Created when the domain naming FSMO role owner is changed from one DC to another. | High |
| Domain Removed | Created when a domain is removed from the partitions container. | High |
| Extended Access Right Added | Created when a new extended access right object is added to the system. | Medium |
| Extended Access Right Removed | Created when an extended access right object is removed from the system. | Medium |
| Forest Functional Level Changed | Created when the forest functional level is changed. | High |
| GC Added | Created when a domain controller is promoted from a non-GC to a GC. | Medium |
| GC Removed | Created when a domain controller is demoted from a GC to a non-GC. | High |

**Table 17. Forest Configuration events**

| Event | Description | Severity |
|---|---|---|
| Member Added to Critical Enterprise Group | Created when a new member is added to one of the critical enterprise groups. Critical enterprise groups include:<br>• Server Operators<br>• Print Operators<br>• Network Configuration Operators<br>• Incoming Forest Trust Builders<br>• Backup Operators<br>• Administrators<br>• Account Operators<br>• Cert Publishers<br>• DHCP Administrators<br>• Domain Admins<br>• Domain Controllers<br>• Enterprise Admins<br>• Group Policy Creator Owners<br>• RAS and IAS Servers<br>• Schema Admins | High |
| Member Removed from Critical Enterprise Group | Created when a new member is removed from one of the critical enterprise groups. Critical enterprise groups include:<br>• Server Operators<br>• Print Operators<br>• Network Configuration Operators<br>• Incoming Forest Trust Builders<br>• Backup Operators<br>• Administrators<br>• Account Operators<br>• Cert Publishers<br>• DHCP Administrators<br>• Domain Admins<br>• Domain Controllers<br>• Enterprise Admins<br>• Group Policy Creator Owners<br>• RAS and IAS Servers<br>• Schema Admins | High |
| Nested Member Added to Critical Enterprise Group | Created when a member is added to a nested group in a critical enterprise group. | High |
| Nested Member Removed from Critical Enterprise Group | Created when a member is removed from a nested group in a critical enterprise group. | Medium |
| Query Policy Added | Created when a new domain controller query policy is added. | Low |
| Query Policy Removed | Created when a domain controller query policy object is removed. | Low |
| Schema FSMO Role Owner Moved | Created when the schema FSMO role owner is changed from one DC to another. | High |
| Site Added | Created when a new site is added to the forest. | Medium |

Table 17. Forest Configuration events

| Event | Description | Severity |
|---|---|---|
| Site Link Added | Created when a site link is added to either the IP or SMTP containers. | Medium |
| Site Link Bridge Added | Created when a site link bridge is added to either the IP or SMTP containers. | Medium |
| Site Link Bridge Removed | Created when a site link bridge is removed from either the IP or SMTP containers. | High |
| Site Link Removed | Created when a site link is removed from either the IP or SMTP containers. | High |
| Site Removed | Created when a site is removed from the forest. | High |
| Site Renamed | Created when an existing site is renamed. | Medium |
| Subnet Added | Created when a new subnet is added. | Medium |
| Subnet Removed | Created when a subnet is removed. | High |

# FRS Service

Table 18. FRS Service events

| Event | Description | Severity |
|---|---|---|
| FRS Access Check Changed | Created when an FRS access check is changed. | Low |
| FRS Directory Exclusion Filter List Changed on Domain Controller | Created when the FRS directory exclusion filter list on a domain controller is changed. | Low |
| FRS Directory Exclusion Filter List Changed on Replica Set | Created when the FRS directory exclusion filter list on a Replica Set is changed. | Low |
| FRS File Exclusion Filter List Changed for Replica Set | Created when the FRS file exclusion filter list on a Replica Set is changed. | Low |
| FRS File Exclusion Filter List Changed on Domain Controller | Created when the FRS file exclusion filter list on a Domain controller is changed. | Low |
| FRS Mutual Authentication Setting Changed | Created when the FRS mutual authentication is changed. | Low |
| FRS RPC TCP/IP Port Assignment Changed | Created when the FRS TCP/IP port assignment is changed. | Low |
| FRS Staging Space Limit Changed | Created when the FRS Staging space limit is changed. | Low |
| FRS Working Directory Changed | Created when the FRS working directory is changed. | Low |

# Group Policy Item

Table 19. Group Policy Item events

| Event | Description | Severity |
|---|---|---|
| Access Credential Manager as a Trusted Caller | Created when the Access Credential Manager as a Trusted Caller policy is changed in a Group Policy Object. | Medium |
| Access This Computer From The Network Policy Changed | Created when the Computer policy Access This Computer From The Network setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Account Lockout Duration Policy Changed | Created when the Computer policy Account Lockout Duration setting is changed in a Group Policy Object. | Medium |
| Account Lockout Threshold Policy Changed | Created when the Computer policy Account Lockout Threshold setting is changed in a Group Policy Object. | Medium |
| Account Logon: Audit Credential Validation Changed | Created when the Account Logon: Audit Credential Validation policy setting changed in a Group Policy Object. | Medium |
| Account Logon: Audit Kerberos Authentication Service Changed | Created when the Account Logon: Audit Kerberos Authentication Service policy setting changed in a Group Policy Object. | Medium |
| Account Logon: Audit Kerberos Service Ticket Operations Changed | Created when the Account Logon: Audit Kerberos Service Ticket Operations policy setting is changed in a Group Policy Object. | Medium |
| Account Logon: Audit Other Account Logon Events Changed | Created when the Account Logon: Audit Other Application Logon Events policy setting is changed in a Group Policy Object. | Medium |
| Account Management: Audit Application Group Management Changed | Created when the Account Management: Audit Application Group Management policy setting is changed in a Group Policy Object. | Medium |
| Account Management: Audit Computer Account Management Changed | Created when the Account Management: Audit Computer Account Management policy setting is changed in a Group Policy Object. | Medium |
| Account Management: Audit Distribution Group Management Changed | Created when the Account Management: Audit Distribution Group Management policy setting is changed in a Group Policy Object. | Medium |
| Account Management: Audit Other Account Management Events Changed | Created when the Account Management: Audit Other Account Management Events policy setting is changed in a Group Policy Object. | Medium |
| Account Management: Audit Security Group Management Changed | Created when the Account Management: Audit Security Group Management policy setting is changed in a Group Policy Object. | Medium |
| Account Management: Audit User Account Management Changed | Created when the Account Management: Audit User Account Management policy setting is changed in a Group Policy Object. | Medium |
| Accounts: Administrator Account Status Policy Changed | Created when the Accounts: Administrator Account Status setting is changed in a Group Policy Object. | Medium |
| Accounts: Guest Account Status Policy Changed | Created when the Accounts: Guest Account Status setting is changed in a Group Policy Object. | Medium |
| Accounts: Limit Local Account Use Of Blank Passwords To Console Logon Only Policy Changed | Created when the Accounts: Limit Local Account Use Of Blank Passwords To Console Logon Only setting is changed in a Group Policy Object. | Medium |
| Accounts: Rename Administrator Account Policy Changed | Created when the Accounts: Rename Administrator Account is changed in a Group Policy Object. | Medium |
| Accounts: Rename Guest Account Policy Changed | Created when the Accounts: Rename Guest Account is changed in a Group Policy Object. | Medium |
| Act As Part Of The Operating System Policy Changed | Created when the Computer policy Act As Part Of The Operating System setting is changed in a Group Policy Object. | Medium |
| Add Workstations to Domain Policy Changed | Created when the Computer policy Add Workstations to Domain setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Adjust Memory Quotas for a Process Policy Changed | Created when the Computer policy Adjust Memory Quotas for a Process setting is changed in a Group Policy Object. | Medium |
| Allow Log On Locally Policy Changed | Created when the Computer policy Allow Log On Locally setting is changed in a Group Policy Object. | Medium |
| Allow Log On Through Terminal Services Policy Changed | Created when the Computer policy Allow Log On Through Terminal Services setting is changed in a Group Policy Object. | Medium |
| Audit Account Logon Events Policy Changed | Created when the Computer policy Audit Account Logon Events setting is changed in a Group Policy Object. | Medium |
| Audit Account Management Policy Changed | Created when the Computer policy Audit Account Management setting is changed in a Group Policy Object. | Medium |
| Audit Directory Service Access Policy Changed | Created when the Computer policy Audit Directory Service Access setting is changed in a Group Policy Object. | Medium |
| Audit Logon Events Policy Changed | Created when the Computer policy Audit Logon Events setting is changed in a Group Policy Object. | Medium |
| Audit Object Access Policy Changed | Created when the Computer policy Audit Object Access setting is changed in a Group Policy Object. | Medium |
| Audit Policy Change Policy Changed | Created when the Computer policy Audit Policy Change setting is changed in a Group Policy Object. | Medium |
| Audit Privilege Use Policy Changed | Created when the Computer policy Audit Privilege Use setting is changed in a Group Policy Object. | Medium |
| Audit Process Tracking Policy Changed | Created when the Computer policy Audit Process Tracking setting is changed in a Group Policy Object. | Medium |
| Audit System Events Policy Changed | Created when the Computer policy Audit System Events setting is changed in a Group Policy Object. | Medium |
| Audit: Audit the Access of Global System Objects Policy Changed | Created when the Audit: Audit the Access of Global System Objects setting is changed in a Group Policy Object. | Medium |
| Audit: Audit the Use of Backup and Restore Privilege Policy Changed | Created when the Audit: Audit the Use of Backup and Restore Privilege setting is changed in a Group Policy Object. | Medium |
| Audit: Force Audit Policy Subcategory Settings (Windows Vista or later) to Override Audit Policy Category Settings | Created when the Audit: Force Audit Policy Subcategory Settings (Windows Vista or later) to Override Audit Policy Category Settings policy is changed in a Group Policy Object. | Medium |
| Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed | Created when the Audit: Shut Down System Immediately if Unable to Log Security Audits setting is changed in a Group Policy Object. | Medium |
| Back Up Files and Directories Policy Changed | Created when the Computer policy Back Up Files And Directories setting is changed in a Group Policy Object. | Medium |
| BitLocker Drive Encryption Added | Created when the BitLocker Drive Encryption security feature is added to a Group Policy Object. | Medium |
| BitLocker Drive Encryption Changed | Created when the BitLocker Drive Encryption settings are changed on a Group Policy Object. | Medium |
| BitLocker Drive Encryption Removed | Created when the BitLocker Drive Encryption security feature is removed from a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Bypass Traverse Checking Policy Changed | Created when the Computer policy Bypass Traverse Checking setting is changed in a Group Policy Object. | Medium |
| Central Access Policy Added to Group Policy | Created when a Central Access Policy is added to a Group Policy.<br>**NOTE:** Central Access Policy is available in Windows Server 2012; therefore, this event does not apply to earlier versions of Windows Server. | Medium |
| Central Access Policy Removed From Group Policy | Created when a Central Access Policy is removed from a Group Policy.<br>**NOTE:** Central Access Policy is available in Windows Server 2012; therefore, this event does not apply to earlier versions of Windows Server. | Medium |
| Change the System Time Policy Changed | Created when the Computer policy Change The System Time setting is changed in a Group Policy Object. | Medium |
| Change the Time Zone | Created when the Change the Time Zone policy is changed in a Group Policy Object. | Medium |
| Computer Administrative Template Setting Changed | Created when a setting associated with a Computer Administrative Template is enabled, changed, or disabled. | Medium |
| Computer Group Policy Preference Setting Changed | Created when a computer preference in a group policy is enabled, changed, or disabled.<br>**NOTE:** Group policy preferences are available in Windows® 2008 Group Policy Editor.<br>**NOTE:** This event is not available in earlier versions of Windows server. | Medium |
| Computer Group Policy Script setting changed | Created when a computer startup/shutdown script in a group policy is added, changed, or removed. | Medium |
| Computer Public Key Policies Autoenrollment Settings Changed | Created when any properties of Autoenrollment Settings in the Computer Configuration Public Key Policies Enterprise Trust list are changed. | Medium |
| Computer Public Key Policies Automatic Certificate Request Added | Created when an Automated Certificate Request is added to the Computer Configuration Public Key Policies Automated Certificate Request Settings. | Medium |
| Computer Public Key Policies Automatic Certificate Request Changed | Created when an Automated Certificate Request setting is changed in the Computer Configuration Public Key Policies Automated Certificate Request list. | Medium |
| Computer Public Key Policies Automatic Certificate Request Removed | Created when an Automated Certificate Request is removed from the Computer Configuration Public Key Policies Automated Certificate Request list. | Medium |
| Computer Public Key Policies Encrypting File System DRA Added | Created when a Data Recovery Agent (DRA) is added to the Computer Configuration Public Key Policies Encrypting File System list. | Medium |
| Computer Public Key Policies Encrypting File System DRA Changed | Created when a Data Recovery Agent (DRA) is changed in the Computer Configuration Public Key Policies Encrypting File System list. | Medium |
| Computer Public Key Policies Encrypting File System DRA Removed | Created when a Data Recovery Agent (DRA) is removed from the Computer Configuration Public Key Policies Encrypting File System list. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Computer Public Key Policies Enterprise Trust List Added | Created when a certificate is imported into the Computer Configuration Public Key Policies Enterprise Trust. | Medium |
| Computer Public Key Policies Enterprise Trust List Changed | Created when a certificate in the Computer Configuration Public Key Policies Enterprise Trust list is changed. | Medium |
| Computer Public Key Policies Enterprise Trust List Removed | Created when a certificate in the Computer Configuration Public Key Policies Enterprise Trust list is removed. | Medium |
| Computer Public Key Policies Trusted Root Certification Authority Added | Created when a certificate is imported into the Computer Configuration Public Key Policies Trusted Root Certification Authorities. | Medium |
| Computer Public Key Policies Trusted Root Certification Authority Changed | Created when a certificate in the Computer Configuration Public Key Policies Trusted Root Certification Authorities is changed. | Medium |
| Computer Public Key Policies Trusted Root Certification Authority Removed | Created when a certificate in the Computer Configuration Public Key Policies Trusted Root Certification Authorities is removed. | Medium |
| Computer Software Installation Policy Added | Created when a Software Installation is added to the Computer Configuration Group Policy. | Medium |
| Computer Software Installation Policy Changed | Created when a Software Installation is changed in the Computer Configuration Group Policy. | Medium |
| Computer Software Installation Policy Removed | Created when a Software Installation is removed from the Computer Configuration Group Policy. | Medium |
| Computer Software Restriction Basic User Hash Rule Added | Created when a Basic User Hash Rule has been added to Computer Configuration Software Restriction policies. | Medium |
| Computer Software Restriction Basic User Hash Rule Changed | Created when a Basic User Hash Rule has changed in Computer Configuration Software Restriction policies. | Medium |
| Computer Software Restriction Basic User Hash Rule Removed | Created when a Basic User Hash Rule removed from Computer Configuration Software Restriction policies. | Medium |
| Computer Software Restriction Basic User Path Rule Added | Created when a Basic User Path Rule has been added to Computer Configuration Software Restriction policies. | Medium |
| Computer Software Restriction Basic User Path Rule Changed | Created when a Basic User Path Rule has changed in Computer Configuration Software Restriction policies. | Medium |
| Computer Software Restriction Basic User Path Rule Removed | Created when a Basic User Path Rule has been removed from Computer Configuration Software Restriction policies. | Medium |
| Computer Software Restriction Basic User Zone Rule Added | Created when a Basic User Zone Rule added to Computer Configuration Software Restriction policies. | Medium |
| Computer Software Restriction Basic User Zone Rule Changed | Created when a Basic User Zone Rule changed in Computer Configuration Software Restriction policies. | Medium |
| Computer Software Restriction Basic User Zone Rule Removed | Created when a Basic User Zone Rule removed from Computer Configuration Software Restriction policies. | Medium |
| Computer Software Restriction Designated File Types Changed | Created when the Designated File Types policy is changed in the Software Restriction Policies. | Medium |
| Computer Software Restriction Disallowed Certificate Rule Added | Created when a Disallowed level Certificate Rule is added to the Software Restriction Policies Additional Rules. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Computer Software Restriction Disallowed Certificate Rule Changed | Created when a Disallowed level Certificate Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Certificate Rule Removed | Created when a Disallowed level Certificate Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Hash Rule Added | Created when a Disallowed level Hash Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Hash Rule Changed | Created when a Disallowed level Hash Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Hash Rule Removed | Created when a Disallowed level Hash Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Path Rule Added | Created when a Disallowed level Path Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Path Rule Changed | Created when a Disallowed level Path Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Path Rule Removed | Created when a Disallowed level Path Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Zone Rule Added | Created when a Disallowed level Zone Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Zone Rule Changed | Created when a Disallowed level Zone Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Disallowed Zone Rule Removed | Created when a Disallowed level Zone Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Enforcement Files Changed | Created when an Enforcement Policy Applicable Files option is changed in the Software Restriction Policies. | Medium |
| Computer Software Restriction Enforcement Users Changed | Created when an Enforcement Policy Applicable Users option is changed in the Software Restriction Policies. | Medium |
| Computer Software Restriction Policies Default Security Level Changed | Created when the default security level in the Computer Configuration Software Restriction Policies Security Levels folder is changed. | Medium |
| Computer Software Restriction Trusted Publishers Changed | Created when the Trusted Publisher policy is changed in the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Certificate Rule Added | Created when an Unrestricted level Certificate Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Certificate Rule Changed | Created when an Unrestricted level Certificate Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Certificate Rule Removed | Created when an Unrestricted level Certificate Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Hash Rule Added | Created when an Unrestricted level Hash Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Hash Rule Changed | Created when an Unrestricted level Hash Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Hash Rule Removed | Created when an Unrestricted level Hash Rule is removed from the Software Restriction Policies Additional Rules. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Computer Software Restriction Unrestricted Path Rule Added | Created when an Unrestricted level Path Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Path Rule Changed | Created when an Unrestricted level Path Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Path Rule Removed | Created when an Unrestricted level Path Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Zone Rule Added | Created when an Unrestricted level Zone Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Zone Rule Changed | Created when an Unrestricted level Zone Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| Computer Software Restriction Unrestricted Zone Rule Removed | Created when an Unrestricted level Zone Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| Create a Pagefile Policy Changed | Created when the Computer policy Create A Pagefile setting is changed in a Group Policy Object. | Medium |
| Create a Token Object Policy Changed | Created when the Computer policy Create A Token Object setting is changed in a Group Policy Object. | Medium |
| Create Global Objects Policy Changed | Created when the Computer policy Create Global Objects setting is changed in a Group Policy Object. | Medium |
| Create Permanent Shared Objects Policy Changed | Created when the Computer policy Create Permanent Shared Objects setting is changed in a Group Policy Object. | Medium |
| Create Symbolic Links | Created when the Create Symbolic Links policy is changed in a Group Policy Object. | Medium |
| DCOM: Machine Access Restrictions Policy Defined | Created when the DCOM: Machine Access Restrictions policy setting is defined on a Group Policy Object. | Medium |
| DCOM: Machine Access Restrictions Policy Undefined | Created when the DCOM: Machine Access Restrictions policy setting is undefined on a Group Policy Object. | Medium |
| DCOM: Machine Access Restrictions Security Settings Changed | Created when the DCOM: Machine Access Restrictions in Security Descriptor Definition (SDDL) Syntax security setting is changed in a Group Policy Object. | Medium |
| DCOM: Machine Launch Restrictions Policy Defined | Created when the DCOM: Machine Launch Restrictions policy setting is defined on a Group Policy Object. | Medium |
| DCOM: Machine Launch Restrictions Policy Undefined | Created when the DCOM: Machine Launch Restrictions policy setting is undefined on a Group Policy Object. | Medium |
| DCOM: Machine Launch Restrictions Security Settings Changed | Created when the DCOM: Machine Launch Restrictions in Security Descriptor Definition (SDDL) Syntax security setting is changed in a Group Policy Object. | Medium |
| Debug Programs Policy Changed | Created when the Computer policy Debug Programs setting is changed in a Group Policy Object. | Medium |
| Deny Access to this Computer from the Network Policy Changed | Created when the Computer policy Deny Access to this Computer from the Network setting is changed in a Group Policy Object. | Medium |
| Deny Log On as a Batch Job Policy Changed | Created when the Computer policy Deny Log On as a Batch Job setting is changed in a Group Policy Object. | Medium |
| Deny Log On as a Service Policy Changed | Created when the Computer policy Deny Log On As A Service setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Deny Log On Locally Policy Changed | Created when the Computer policy Deny Log On Locally setting is changed in a Group Policy Object. | Medium |
| Deny Log On Through Terminal Services /Remote Desktop Service Policy Changed | Created when the Computer policy Deny Log On Through Terminal Services setting is changed in a Group Policy Object. | Medium |
| Detailed Tracking: Audit DPAPI Activity Changed | Created when the Detailed Tracking: Audit DPAPI Activity policy setting is changed in a Group Policy Object. | Medium |
| Detailed Tracking: Audit Process Creation Changed | Created when the Detailed Tracking: Audit Process Creation policy setting is changed in a Group Policy Object. | Medium |
| Detailed Tracking: Audit Process Termination Changed | Created when the Detailed Tracking: Audit Process Termination policy setting is changed in a Group Policy Object. | Medium |
| Detailed Tracking: Audit RPC Events Changed | Created when the Detailed Tracking: Audit RPC Events policy setting is changed in a Group Policy Object. | Medium |
| Devices: Allow Undock Without Having to Logon Policy Changed | Created when the Devices: Allow Undock Without Having To Logon setting is changed in a Group Policy Object. | Medium |
| Devices: Allowed to Format and Eject Removable Media Policy Changed | Created when the Devices: Allowed To Format And Eject Removable Media setting is changed in a Group Policy Object. | Medium |
| Devices: Prevent Users from Installing Printer Drivers Policy Changed | Created when the Devices: Prevent Users From Installing Printer Drivers setting is changed in a Group Policy Object. | Medium |
| Devices: Restrict CD-ROM Access to Locally Logged-On User Only Policy Changed | Created when the Devices: Restrict CD-ROM Access To Locally Logged-On User Only setting is changed in a Group Policy Object. | Medium |
| Devices: Restrict Floppy Access to Locally Logged-On User Only Policy Changed | Created when the Devices: Restrict Floppy Access To Locally Logged-On User Only setting is changed in a Group Policy Object. | Medium |
| Devices: Unsigned Driver Installation Behavior Policy Changed | Created when the Devices: Unsigned Driver Installation Behavior setting is changed in a Group Policy Object. | Medium |
| Domain Controller: Allow Server Operators to Schedule Tasks Policy Changed | Created when the Domain controllers: Allow Server Operators To Schedule Tasks setting is changed in a Group Policy Object. | Medium |
| Domain Controller: LDAP Server Signing Requirements Policy Changed | Created when the Domain controllers: LDAP Server Signing Requirements setting is changed in a Group Policy Object. | Medium |
| Domain Controller: Refuse Machine Account Password Changes Policy Changed | Created when the Domain controllers: Refuse Machine Account Password Changes setting is changed in a Group Policy Object. | Medium |
| Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always) Policy Changed | Created when the Domain Member: Digitally Encrypt Or Sign Secure Channel Data (Always) setting is changed in a Group Policy Object. | Medium |
| Domain Member: Digitally Encrypt Secure Channel Data (When Possible) Policy Changed | Created when the Domain Member: Digitally Encrypt Secure Channel Data (When Possible) setting is changed in a Group Policy Object. | Medium |
| Domain Member: Digitally Sign Secure Channel Data (When Possible) Policy Changed | Created when the Domain Member: Digitally Sign Secure Channel Data (When Possible) setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Domain Member: Disable Machine Account Password Changes Policy Changed | Created when the Domain Member: Disable Machine Account Password Changes setting is changed in a Group Policy Object. | Medium |
| Domain Member: Maximum Machine Account Password Age Policy Changed | Created when the Domain Member: Maximum Machine Account Password Age setting is changed in a Group Policy Object. | Medium |
| Domain Member: Require Strong (Windows 2000 or Later) Session Key Policy Changed | Created when the Domain Member: Require Strong (Windows 2000 Or Later) Session Key setting is changed in a Group Policy Object. | Medium |
| DS Access: Audit Detailed Directory Service Replication Changed | Created when the DS Access: Audit Detailed Directory Service Replication policy setting is changed in a Group Policy Object. | Medium |
| DS Access: Audit Directory Service Access Changed | Created when the DS Access: Audit Directory Service Access policy setting is changed in a Group Policy Object. | Medium |
| DS Access: Audit Directory Service Changes Changed | Created when the DS Access: Audit Directory Service Changes policy setting is changed in a Group Policy Object. | Medium |
| DS Access: Audit Directory Service Replication Changed | Created when the DS Access: Audit Directory Service Replication policy setting is changed in a Group Policy Object. | Medium |
| Enable Computer and User Accounts to be Trusted for Delegation Changed | Created when the Computer policy Enable Computer And User Accounts To Be Trusted For Delegation Policy setting is changed in a Group Policy Object. | Medium |
| Enforce Password History Policy Changed | Created when the Computer policy Enforce Password History setting is changed in a Group Policy Object. | Medium |
| Enforce User Logon Restrictions Policy Changed | Created when the Computer policy Enforce User Logon Restrictions setting is changed in a Group Policy Object. | Medium |
| File or Folder Added to File System Policy | Created when a registry key is added to the File System policy. | Medium |
| File or Folder Changed in File System Policy | Created when a file or folder is changed in the File System policy. | Medium |
| File or Folder Removed from File System Policy | Created when a file or folder is removed from the File System policy. | Medium |
| Force Shutdown from a Remote System Policy Changed | Created when the Computer policy Force Shutdown From A Remote System setting is changed in a Group Policy Object. | Medium |
| Generate Security Audits Policy Changed | Created when the Computer policy Generate Security Audits setting is changed in a Group Policy Object. | Medium |
| Global Object Access Auditing: File System Changed | Created when the Global Object Auditing: File System security policy is changed. | Medium |
| Global Object Access Auditing: Registry Changed | Create when the Global Object Auditing: Registry security policy is changed. | Medium |
| Group Added To Restricted Group Policy | Created when a group is added to the Restricted Group policy in a Group Policy Object. | Medium |
| Group Removed from Restricted Group Policy | Created when a group is removed from the Restricted Group policy in a Group Policy Object. | Medium |
| Impersonate a Client after Authentication Policy Changed | Created when the Computer policy Impersonate A Client After Authentication setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Increase a Process Working Set | Created when the Increase a Process Working Set policy is change in a Group Policy Object. | Medium |
| Increase Scheduling Priority Policy Changed | Created when the Computer policy Increase Scheduling Priority setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Display User Information When the Session is Locked Policy Changed | Created when the Interactive Logon: Display User Information When the Session is Locked setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Do Not Display Last User Name Policy Changed | Created when the Interactive Logon: Do Not Display Last User Name setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Do Not Require CTRL+ALT+DEL Policy Changed | Created when the Interactive Logon: Do Not Require CTRL+ALT+DEL setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Message Text for Users Attempting to Log On Policy Changed | Created when the Interactive Logon: Message Text For Users Attempting To Log On setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Message Title for Users Attempting to Log On Policy Changed | Created when the Interactive Logon: Message Title For Users Attempting To Log On setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Number Of Previous Logons To Cache (In Case Domain Controller is Not Available) Policy Changed | Created when the Interactive Logon: Number Of Previous Logons To Cache setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Prompt User to Change Password Before Expiration Policy Changed | Created when the Interactive Logon: Prompt User To Change Password Before Expiration setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Require Domain Controller Authentication to Unlock Workstation Policy Changed | Created when the Interactive Logon: Require Domain controller Authentication to Unlock Workstation setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Require Smart Card Policy Changed | Created when the Interactive Logon: Require Smart Card setting is changed in a Group Policy Object. | Medium |
| Interactive Logon: Smart Card Removal Behavior Policy Changed | Created when the Interactive Logon: Smart Card Removal Behavior setting is changed in a Group Policy Object. | Medium |
| Intermediate Certificate Authorities Added | Created when an Intermediate Certification Authorities (CA) certificate is added to a Group Policy Object. | Medium |
| Intermediate Certificate Authorities Changed | Created when the Intermediate Certification Authorities certificate is changed on a Group Policy Object. | Medium |
| Intermediate Certificate Authorities Removed | Created when an Intermediate Certification Authorities (CA) certificate is removed from a Group Policy Object. | Medium |
| IP Security Policy Assigned | Created when an IP Security Policy is assigned in the Computer Configuration Group Policy. | Medium |
| IP Security Policy Un-assigned | Created when an IP Security Policy is un-assigned in the Computer Configuration Group Policy. | Medium |
| Load and Unload Device Drivers Policy Changed | Created when the Computer policy Load And Unload Device Drivers setting is changed in a Group Policy Object. | Medium |
| Lock Pages in Memory Policy Changed | Created when the Computer policy Lock Pages In Memory setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Log On as a Batch Job Policy Changed | Created when the Computer policy Log On As A Batch Job setting is changed in a Group Policy Object. | Medium |
| Log On as a Service Policy Changed | Created when the Computer policy Log On As A Service setting is changed in a Group Policy Object. | Medium |
| Logon/Logoff: Audit Account Lockout Changed | Created when the Logon/Logoff: Audit Account Lockout policy setting is changed in a Group Policy Object. | Medium |
| Logon/Logoff: Audit IPsec Extended Mode Changed | Created when the Logon/Logoff: Audit IPsec Extended Mode policy setting is changed in a Group Policy Object. | Medium |
| Logon/Logoff: Audit IPsec Main Mode Changed | Created when the Logon/Logoff: Audit IPsec Main Mode policy setting is changed in a Group Policy Object. | Medium |
| Logon/Logoff: Audit IPsec Quick Mode Changed | Created when the Logon/Logoff: Audit IPsec Quick Mode policy setting is changed in a Group Policy Object. | Medium |
| Logon/Logoff: Audit Logoff Changed | Created when the Logon/Logoff: Audit Logoff policy setting is changed in a Group Policy Object. | Medium |
| Logon/Logoff: Audit Logon Changed | Created when the Logon/Logoff: Audit Logon policy setting is changed in a Group Policy Object. | Medium |
| Logon/Logoff: Audit Network Policy Server Changed | Created when the Logon/Logoff: Audit Network Policy Server policy setting is changed in a Group Policy Object. | Medium |
| Logon/Logoff: Audit Other Logon/Logoff Events Changed | Created when the Logon/Logoff: Audit Other Logon/Logoff Events policy setting is changed in a Group Policy Object. | Medium |
| Logon/Logoff: Audit Special Logon Changed | Created when the Logon/Logoff: Audit Special Logon policy setting is changed in a Group Policy Object. | Medium |
| Manage Auditing and Security Log Policy Changed | Created when the Manage Auditing And Security Log setting is changed in a Group Policy Object. | Medium |
| Maximum Application Log Size Policy Changed | Created when the Maximum Application Log Size setting is changed in a Group Policy Object. | Medium |
| Maximum Lifetime for Service Ticket Policy Changed | Created when the Computer policy Maximum Lifetime for Service Ticket setting is changed in a Group Policy Object. | Medium |
| Maximum Lifetime for User Ticket Policy Changed | Created when the Computer policy Maximum Lifetime for User Ticket setting is changed in a Group Policy Object. | Medium |
| Maximum Lifetime for User Ticket Renewal Policy Changed | Created when the Computer policy Maximum Lifetime for User Ticket Renewal setting is changed in a Group Policy Object. | Medium |
| Maximum Password Age Policy Changed | Created when the Computer policy Maximum Password Age setting is changed in a Group Policy Object. | Medium |
| Maximum Security Log Size Policy Changed | Created when the Maximum Security Log Size setting is changed in a Group Policy Object. | Medium |
| Maximum System Log Size Policy Changed | Created when the Maximum System Log Size setting is changed in a Group Policy Object. | Medium |
| Maximum Tolerance for Computer Clock Synchronization Policy Changed | Created when the Computer policy Maximum Tolerance for Computer Clock Synchronization setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Member Added to Group in the Restricted Group Policy | Created when a member is added to a group in the Restricted Group policy of a Group Policy Object. | Medium |
| Member Removed from Group in the Restricted Group Policy | Created when a member is removed from a group in the Restricted Group policy of a Group Policy Object. | Medium |
| Membership Added to Group in the Restricted Group Policy | Created when a membership is added to a group in the Restricted Group policy of a Group Policy Object. | Medium |
| Membership Removed from Group in the Restricted Group Policy | Created when a membership is removed from a group in the Restricted Group policy of a Group Policy Object. | Medium |
| Microsoft Network Client: Digitally Sign Communications (Always) Policy Changed | Created when the Microsoft® Network Client: Digitally Sign Communications (Always) setting is changed in a Group Policy Object. | Medium |
| Microsoft Network Client: Digitally Sign Communications (If Server Agrees) Policy Changed | Created when the Microsoft Network Client: Digitally Sign Communications (If Server Agrees) setting is changed in a Group Policy Object. | Medium |
| Microsoft Network Client: Send Unencrypted Password to Connect to Third-Party SMB Servers Policy Changed | Created when the Microsoft Network Client: Send Unencrypted Password to Connect to Third-Party SMB Servers setting is changed in a Group Policy Object. | Medium |
| Microsoft Network Server: Amount of Idle Time Required Before Suspending Sessions Policy Changed | Created when the Microsoft Network Server: Amount of Idle Time Required Before Suspending Sessions setting is changed in a Group Policy Object. | Medium |
| Microsoft Network Server: Digitally Sign Communications (Always) Policy Changed | Created when the Microsoft Network Server: Digitally Sign Communications (Always) setting is changed in a Group Policy Object. | Medium |
| Microsoft Network Server: Digitally Sign Communications (If Client Agrees) Policy Changed | Created when the Microsoft Network Server: Digitally Sign Communications (If Client Agrees) setting is changed in a Group Policy Object. | Medium |
| Microsoft Network Server: Disconnect Clients When Logon Hours Expire Policy Changed | Created when the Microsoft Network Server: Disconnect Clients When Logon Hours Expire setting is changed in a Group Policy Object. | Medium |
| Microsoft Network Server: Server SPN Target Name Validation Level | Created when the Microsoft Network Server: Server SPN Target Name Validation Level policy is changed in a Group Policy Object. | Medium |
| Minimum Password Age Policy Changed | Created when the Computer policy Minimum Password Age setting is changed in a Group Policy Object. | Medium |
| Minimum Password Length Policy Changed | Created when the Computer policy Minimum Password Length setting is changed in a Group Policy Object. | Medium |
| Modify an Object Label | Created when the Modify an Object Label policy is changed in a Group Policy Object. | Medium |
| Modify Firmware Environment Policy Changed | Created when the Modify Firmware Environment setting is changed in a Group Policy Object. | Medium |
| NAP Client Health Registration Settings: CSP Changed | Created when the Cryptographic Service Provider (CSP) is changed in a NAP client request policy. | Medium |
| NAP Client Health Registration Settings: CSP Key Length Changed | Created when the CSP asymmetric key length is changed in a NAP client request policy. | Medium |
| NAP Client Health Registration Settings: Hash Algorithm Changed | Created when the hash algorithm is changed in a NAP client request policy. | Medium |
| NAP Client Health Registration Settings: Require Server Verification Changed | Created when the server verification (HTTP) setting is enabled or disabled in a NAP client configuration. | Medium |
| NAP Client Health Registration Settings: Trusted Server Group Added | Created when a new trusted server group is created in a NAP client configuration. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| NAP Client Health Registration Settings: Trusted Server Group Removed | Created when a trusted server group is removed from a NAP client configuration. | Medium |
| NAP Client Health Registration Settings: Trusted Server URL Added | Created when a new URL for a HRA server is added to the trusted server group in a NAP client configuration. | Medium |
| NAP Client Health Registration Settings: Trusted Server URL Changed | Created when an existing URL for a HRA server is modified in a NAP client configuration. | Medium |
| NAP Client Health Registration Settings: Trusted Server URL Removed | Created when a URL for a HRA server is removed from the trusted server group in a NAP client configuration. | Medium |
| NAP User Interface Description Changed | Created when the description field on the NAP Status User Interface properties dialog is changed for an NAP client configuration. | Medium |
| NAP User Interface Image File Changed | Created when the image file is changed on the NAP Status User Interface properties dialog for an NAP client configuration. | Medium |
| NAP User Interface Image File Name Changed | Created when the image file name is changed on the NAP Status User Interface properties dialog for an NAP client configuration. | Medium |
| NAP User Interface Title Changed | Created when the title field on the NAP Status User Interface properties dialog is changed for an NAP client configuration. | Medium |
| NAP: DHCP Quarantine Enforcement Client Changed | Created when the DHCP Quarantine Enforcement Client setting is enabled or disabled for an NAP client configuration. | Medium |
| NAP: EAP Quarantine Enforcement Client Changed | Created when the EAP Quarantine Enforcement Client setting is enabled or disabled for an NAP client configuration. | Medium |
| NAP: IPsec Relying Party Changed | Create when the IPsec Relying Party setting is enabled or disabled for an NAP client configuration. | Medium |
| NAP: RD Gateway Quarantine Enforcement Client Changed | Created when the RD Gateway Quarantine Enforcement Client setting is enabled or disabled for an NAP client configuration. | Medium |
| NAP: Remote Access Enforcement Client for Windows XP and Windows Vista Changed | Created when the Remote Access Enforcement Client for Windows XP and Windows Vista setting is enabled or disabled for an NAP client configuration. | Medium |
| NAP: Wireless EAPOL Enforcement Client for Windows XP Changed | Created when the Wireless EAPOL Enforcement Client for Windows XP setting is enabled or disabled for an NAP client configuration. | Medium |
| Network Access: Allow Anonymous SID/Name Translation Policy Changed | Created when the Network Access: Allow Anonymous SID/Name Translation setting is changed in a Group Policy Object. | Medium |
| Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts And Shares Policy Changed | Created when the Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts and Shares setting is changed in a Group Policy Object. | Medium |
| Network Access: Do Not Allow Anonymous Enumeration of SAM Accounts Policy Changed | Created when the Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts setting is changed in a Group Policy Object. | Medium |
| Network Access: Do Not Allow Storage of Credentials or .NET Passports for Network Authentication Policy Changed | Created when the Network Access: Do Not Allow Storage of Credentials or .NET Passports for Network Authentication setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Network Access: Let Everyone Permissions Apply to Anonymous Users Policy Changed | Created when the Network Access: Let Everyone Permissions Apply to Anonymous Users setting is changed in a Group Policy Object. | Medium |
| Network Access: Named Pipes that can be Accessed Anonymously Policy Changed | Created when the Network Access: Named Pipes that can be Accessed Anonymously setting is changed in a Group Policy Object. | Medium |
| Network Access: Remotely Accessible Registry Paths and Sub-Paths Changed | Created when the Network Access: Remotely Accessible Registry Paths And Sub-Paths setting is changed in a Group Policy Object. | Medium |
| Network Access: Remotely Accessible Registry Paths Policy Changed | Created when the Network Access: Remotely Accessible Registry Paths setting is changed in a Group Policy Object. | Medium |
| Network Access: Restrict Anonymous Access to Named Pipes and Shares Policy Changed | Created when the Network Access: Restrict Anonymous Access To Named Pipes and Shares setting is changed in a Group Policy Object. | Medium |
| Network Access: Shares that can be Accessed Anonymously Policy Changed | Created when the Network Access: Shares that can be Accessed Anonymously setting is changed in a Group Policy Object. | Medium |
| Network Access: Sharing and Security Model for Local Accounts Changed | Created when the Network Access: Sharing and Security Model for Local Accounts setting is changed in a Group Policy Object. | Medium |
| Network Security: Allow Local System to Use Computer Identity for NTLM | Created when the Network Security: Allow Local System to Use Computer Identity for NTLM setting is changed in a Group Policy Object. | Medium |
| Network Security: Allow LocalSystem NULL Session Fallback | Created when the Network Security: Allow LocalSystem NULL Session Fallback setting is changed in a Group Policy Object. | Medium |
| Network Security: Allow PKU2U Authentication Requests to this Computer to use Online Identities | Created when the Network Security: Allow PKU2U Authentication Requests to this Computer to use Online Identities setting is changed in a Group Policy Object. | Medium |
| Network Security: Configure Encryption Types Allowed for Kerberos | Created when the Network Security: Configure Encryption Types Allowed for Kerberos setting is changed in a Group Policy Object. | Medium |
| Network Security: Do Not Store LAN Manager Hash Value on Next Password Change Policy Changed | Created when the Network Security: Do Not Store LAN Manager Hash Value on Next Password Change setting is changed in a Group Policy Object. | Medium |
| Network Security: Force Logoff When Logon Hours Expire Policy Changed | Created when the Network Security: Force Logoff When Logon Hours Expire setting is changed in a Group Policy Object. | Medium |
| Network Security: LAN Manager Authentication Level Policy Changed | Created when the Network Security: LAN Manager Authentication Level setting is changed in a Group Policy Object. | Medium |
| Network Security: LDAP Client Signing Requirements Policy Changed | Created when the Network Security: LDAP Client Signing Requirements setting is changed in a Group Policy Object. | Medium |
| Network Security: Minimum Session Security for NTLM SSP Based (Including Secure RPC) Clients Policy Changed | Created when the Network Security: Minimum Session Security for NTLM SSP Based (Including Secure RPC) Clients setting is changed in a Group Policy Object. | Medium |
| Network Security: Minimum Session Security for NTLM SSP Based (Including Secure RPC) Servers Policy Changed | Created when the Network Security: Minimum Session Security for NTLM SSP Based (Including Secure RPC) Servers setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Network Security: Restrict NTLM: Add Remote Server Exceptions for NTLM Authentication | Created when the Network Security: Restrict NTLM: Add Remote Server Exceptions for NTLM Authentication policy setting is changed in a Group Policy Object. | Medium |
| Network Security: Restrict NTLM: Add Server Exceptions in This Domain | Created when the Network Security: Restrict NTLM: Add Server Exceptions in This Domain policy setting is changed in a Group Policy Object. | Medium |
| Network Security: Restrict NTLM: Audit Incoming NTLM Traffic | Created when the Network Security: Restrict NTLM: Audit Incoming NTLM Traffic policy setting is changed in a Group Policy Object. | Medium |
| Network Security: Restrict NTLM: Audit NTLM Authentication in This Domain | Created when the Network Security: Restrict NTLM: Audit NTLM Authentication in This Domain policy setting is changed in a Group Policy Object. | Medium |
| Network Security: Restrict NTLM: Incoming NTLM Traffic | Created when the Network Security: Restrict NTLM: Incoming NTLM Traffic policy setting is changed in a Group Policy Object. | Medium |
| Network Security: Restrict NTLM: NTLM Authentication in This Domain | Created when the Network Security: Restrict NTLM: NTLM Authentication in This Domain policy setting is changed in a Group Policy Object. | Medium |
| Network Security: Restrict NTLM: Outgoing NTLM Traffic to Remote Servers | Created when the Network Security: Restrict NTLM: Outgoing NTLM Traffic to Remote Servers policy setting is changed in a Group Policy Object. | Medium |
| NLM: Location Type Added | Created when an NLM: Location Type is added to a Group Policy Object. | Medium |
| NLM: Location Type Changed | Created when an NLM: Location Type is changed in a Group Policy Object. | Medium |
| NLM: Location Type Permissions Added | Created when an NLM: Location Type Permission is added to a Group Policy Object. | Medium |
| NLM: Location Type Permissions Changed | Created when an NLM: Location Type Permission is changed in a Group Policy Object. | Medium |
| NLM: Location Type Permissions Removed | Created when an NLM: Location Type Permission is removed from a Group Policy Object. | Medium |
| NLM: Location Type Removed | Created when an NLM: Location Type is removed from a Group Policy Object. | Medium |
| NLM: Network Icon Added | Created when an NLM: Network Icon is added to a Group Policy Object. | Medium |
| NLM: Network Icon Changed | Created when an NLM: Network Icon is changed in a Group Policy Object. | Medium |
| NLM: Network Icon Permissions Added | Created when an NLM: Network Icon Permission is added to a Group Policy Object. | Medium |
| NLM: Network Icon Permissions Changed | Created when an NLM: Network Icon Permission is changed in a Group Policy Object. | Medium |
| NLM: Network Icon Permissions Removed | Created when an NLM: Network Icon Permission is removed from a Group Policy Object. | Medium |
| NLM: Network Icon Removed | Created when an NLM: Network Icon is removed from a Group Policy Object. | Medium |
| NLM: Network Name Added | Created when an NLM: Network Name is added to a Group Policy Object. | Medium |
| NLM: Network Name Changed | Created when an NLM: Network Name is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| NLM: Network Name Permissions Added | Created when an NLM: Network Name Permission is added to a Group Policy Object. | Medium |
| NLM: Network Name Permissions Changed | Created when an NLM: Network Name Permission is changed in a Group Policy Object. | Medium |
| NLM: Network Name Permissions Removed | Created when an NLM: Network Name Permission is removed from a Group Policy Object. | Medium |
| NLM: Network Name Removed | Created when an NLM: Network Name is removed from a Group Policy Object. | Medium |
| Object Access: Audit Application Generated Changed | Created when the Object Access: Audit Application Generated policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit Certification Services Changed | Created when the Object Access: Audit Certification Services policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit File Share Changed | Created when the Object Access: Audit File Share policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit File System Changed | Created when the Object Access: Audit File System policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit Filtering Platform Connection Changed | Created when the Object Access: Audit Filtering Platform Connection policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit Filtering Platform Packet Drop Changed | Created when the Object Access: Audit Filtering Platform Packet Drop policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit Handle Manipulation Changed | Created when the Object Access: Audit Handle Manipulation policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit Kernel Object Changed | Created when the Object Access: Audit Kernel Object policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit Other Object Access Events Changed | Created when the Object Access: Audit Other Object Access Events policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit Registry Changed | Created when the Object Access: Audit Registry policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Audit SAM Changed | Created when the Object Access: Audit SAM policy setting is changed in a Group Policy Object. | Medium |
| Object Access: Detailed File Share Changed | Created when the Object Access: Audit Detailed File Share policy setting is changed in a Group Policy Object. | Medium |
| Password Must Meet Complexity Requirements Policy Changed | Created when the Computer policy Password Must Meet Complexity Requirements setting is changed in a Group Policy Object. | Medium |
| Perform Volume Maintenance Tasks Policy Changed | Created when the Perform Volume Maintenance Tasks setting is changed in a Group Policy Object. | Medium |
| Permissions Changed on a System Services Policy | Created when permissions change in a System Services Policy in a Group Policy Object. | Medium |
| Policy Change: Audit Audit Policy Change Changed | Created when the Policy Change: Audit Audit Policy Change security setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Policy Change: Audit Authentication Policy Change Changed | Created when the Policy Change: Audit Authentication Policy Change security setting is changed in a Group Policy Object. | Medium |
| Policy Change: Audit Authorization Policy Change Changed | Created when the Policy Change: Audit Authorization Policy Change security setting is changed in a Group Policy Object. | Medium |
| Policy Change: Audit Filtering Platform Policy Change Changed | Created when the Policy Change: Audit Filtering Platform Policy Change security setting is changed in a Group Policy Object. | Medium |
| Policy Change: Audit MPSSVC Rule-Level Policy Change Changed | Created when the Policy Change: Audit MPSSVC Rule-Level Policy Change security setting is changed in a Group Policy Object. | Medium |
| Policy Change: Audit Other Policy Change Events Changed | Created when the Policy Change: Audit Other Policy Change Events security setting is changed in a Group Policy Object. | Medium |
| Prevent Local Guests Group from Accessing Application Log Policy Change | Created when the Prevent Local Guests Group from Accessing Application Log setting is changed in a Group Policy Object. | Medium |
| Prevent Local Guests Group from Accessing Security Log Policy Changed | Created when the Prevent Local Guests Group from Accessing Security Log setting is changed in a Group Policy Object. | Medium |
| Prevent Local Guests Group From Accessing System Log Policy Changed | Created when the Prevent Local Guests Group From Accessing System Log setting is changed in a Group Policy Object. | Medium |
| Privilege Use: Audit Non Sensitive Privilege Use Changed | Created when the Privilege Use: Audit Non Sensitive Privilege Use security setting is changed in a Group Policy Object. | Medium |
| Privilege Use: Audit Other Privilege Use Events Changed | Created when the Privilege Use: Audit Other Privilege Use Events security setting is changed in a Group Policy Object. | Medium |
| Privilege Use: Audit Sensitive Privilege Use Changed | Created when the Privilege Use: Audit Sensitive Privilege Use security setting is changed in a Group Policy Object. | Medium |
| Profile Single Process Policy Changed | Created when the Profile Single Process setting is changed in a Group Policy Object. | Medium |
| Profile System Performance Policy Changed | Created when the Profile System Performance setting is changed in a Group Policy Object. | Medium |
| QoS Policy: Application Name Changed | Created when the application name specified in a QoS policy is changed. | Medium |
| QoS Policy: DSCP Value Changed | Created when the DSCP value specified in a QoS policy is changed. | Medium |
| QoS Policy: Local IP Changed | Created when the source IP address specified in a QoS policy is changed. | Medium |
| QoS Policy: Local IP Prefix Length Changed | Created when the prefix length of the source IP address specified in a QoS policy is changed. | Medium |
| QoS Policy: Local Port Changed | Created when the source port specified in a Qos policy is changed. | Medium |
| QoS Policy: Protocol Changed | Created when the protocol to which a QoS policy applies is changed. | Medium |
| QoS Policy: Remote IP Changed | Created when the destination IP address specified in a QoS policy is changed. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| QoS Policy: Remote IP Prefix Length Changed | Created when the prefix length of the destination IP address specified in a QoS policy is changed. | Medium |
| QoS Policy: Remote Port Changed | Created when the destination port specified in a QoS policy is changed. | Medium |
| QoS Policy: Throttle Rate Changed | Created when the traffic throttle rate setting or value is modified in a QoS policy. | Medium |
| QoS Policy: URL Changed | Created when HTTP or HTTPS URL specified in a QoS policy is changed. | Medium |
| QoS Policy: URL Recursive Changed | Created when the Include subdirectories and files option is enabled or disabled for a QoS policy. | Medium |
| QoS Policy: Version Changed | Created when the version specified in a QoS policy is changed. | Medium |
| Recovery Console: Allow Automatic Administrative Logon Policy Changed | Created when the Recovery Console: Allow Automatic Administrative Logon setting is changed in a Group Policy Object. | Medium |
| Recovery Console: Allow Floppy Copy And Access Policy Changed | Created when the Recovery Console: Allow Floppy Copy And Access To All Drives And All Folders setting is changed in a Group Policy Object. | Medium |
| Registry Key Added to Registry Policy | Created when a registry key is added to the Registry policy. | Medium |
| Registry Key Changed in Registry Policy | Created when a registry key is changed in the Registry policy. | Medium |
| Registry Key Removed from Registry Policy | Created when a registry key is removed from the Registry policy. | Medium |
| Remove Computer from Docking Station Policy Changed | Created when the Remove Computer From Docking Station setting is changed in a Group Policy Object. | Medium |
| Replace a Process Level Token Policy Changed | Created when the Replace a Process Level Token setting is changed in a Group Policy Object. | Medium |
| Reset Account Lockout Counter After Change Policy Changed | Created when the Computer policy Reset Account Lockout Counter After Change setting is changed in a Group Policy Object. | Medium |
| Restore Files and Directories Policy Changed | Created when the Restore Files and Directories setting is changed in a Group Policy Object. | Medium |
| Retain Application Log Policy Changed | Created when the Retain Application Log setting is changed in a Group Policy Object. | Medium |
| Retain Security Log Policy Changed | Created when the Retain Security Log setting is changed in a Group Policy Object. | Medium |
| Retain System Log Policy Changed | Created when the Retain System Log setting is changed in a Group Policy Object. | Medium |
| Retention Method for Application Log Policy Changed | Created when the Retention Method For Application Log setting is changed in a Group Policy Object. | Medium |
| Retention Method for Security Log Policy Changed | Created when the Retention Method For Security Log setting is changed in a Group Policy Object. | Medium |
| Retention Method for System Log Policy Changed | Created when the Retention Method For System Log setting is changed in a Group Policy Object. | Medium |
| Secure System Partition (For RISC Platforms only) Policy Changed | Created when the Secure System Partition (For RISC Platforms Only) setting is changed in a Group Policy Object. | Medium |
| Service Defined in System Services Policy | Created when a service is marked as defined in the System Services policy. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| Service Startup Changed in System Services Policy | Created when a service startup is marked as changed in the System Services policy. | Medium |
| Service Undefined in System Services Policy | Created when a service is undefined from the System Services policy. | Medium |
| Shut Down the Computer When the Security Audit Log is Full Policy Changed | Created when the Shut Down the Computer When the Security Audit Log is Full setting is changed in a Group Policy Object. | Medium |
| Shut Down the System Policy Changed | Created when the Shut Down the System setting is changed in a Group Policy Object. | Medium |
| Shutdown: Allow System to be Shut Down Without Having to Log On Policy Changed | Created when the Allow System to be Shut Down Without Having to Log On setting is changed in a Group Policy Object. | Medium |
| Shutdown: Clear Virtual Memory Pagefile Policy Changed | Created when the Clear Virtual Memory Pagefile When System Shuts Down setting is changed in a Group Policy Object. | Medium |
| Starter GPO Computer Setting Changed | Created when a Computer Configuration policy setting is changed for a Starter GPO. | Medium |
| Starter GPO User Setting Changed | Created when a User Configuration policy setting is changed for a Starter GPO. | Medium |
| Store Passwords Using Reversible Encryption Policy Changed | Created when the Computer policy Store Passwords Using Reversible Encryption setting is changed in a Group Policy Object. | Medium |
| Synchronize Directory Service Data Policy Changed | Created when the Synchronize Directory Service Data setting is changed in a Group Policy Object. | Medium |
| System Cryptography: Force Strong Key Protection for User Keys Stored on the Computer Policy Changed | Created when the System Cryptography: Force Strong Key Protection For User Keys Stored On The Computer setting is changed in a Group Policy Object. | Medium |
| System Cryptography: Use FIPS Compliant Algorithms for Encryption, Hashing, and Signing Policy Changed | Created when the System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing, and Signing setting is changed in a Group Policy Object. | Medium |
| System Objects: Default Owner for Objects Created by Members of the Administrators Group Policy Changed | Created when the System Objects: Default Owner For Objects Created By Members Of The Administrators Group setting is changed in a Group Policy Object. | Medium |
| System Objects: Require Case Insensitivity for Non-Windows Subsystems Policy Changed | Created when the System Objects: Require Case Insensitivity For Non-Windows Subsystems setting is changed in a Group Policy Object. | Medium |
| System Objects: Strengthen Default Permissions of Global System Objects (e.g. Symbolic Links) Policy Changed | Created when the System Objects: Strengthen Default Permissions Of Global System Objects setting is changed in a Group Policy Object. | Medium |
| System Objects: Strengthen Default Permissions of Internal System Objects (e.g. Symbolic Links) Policy Changed | Created when the System Objects: Strengthen Default Permissions Of Internal System Objects setting is changed in a Group Policy Object. | Medium |
| System Settings: Optional Subsystems Policy Changed | Created when the System Settings: Optional Subsystems setting is changed in a Group Policy Object. | Medium |
| System Settings: Use Certificate Rules on Windows Executables for Software Restriction Policies Policy Changed | Created when the System Settings: Use Certificate Rules on Windows Executables for Software Restriction Policies setting is changed in a Group Policy Object. | Medium |
| System: Audit IPsec Driver Changed | Created when the System: Audit IPsec Driver security setting is changed in a Group Policy Object. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| System: Audit Other System Events Changed | Created when the System: Audit Other System Events security setting is changed in a Group Policy Object. | Medium |
| System: Audit Security State Change Changed | Created when the System: Audit Security State Change security setting is changed in a Group Policy Object. | Medium |
| System: Audit Security System Extension Changed | Created when the System: Audit Security System Extension security setting is changed in a Group Policy Object. | Medium |
| System: Audit System Integrity Changed | Created when the System: Audit System Integrity security setting is changed in a Group Policy Object. | Medium |
| Take Ownership of Files or Other Objects Policy Changed | Created when the Take Ownership of Files or Other Objects setting is changed in a Group Policy Object. | Medium |
| Trusted People Added | Created when a Trusted People certificate is added to a Group Policy Object. | Medium |
| Trusted People Changed | Created when a Trusted People certificate is changed in a Group Policy Object. | Medium |
| Trusted People Removed | Created when a Trusted People certificate is removed from a Group Policy Object. | Medium |
| Unsigned Non-Driver Installation Behavior Policy Changed | Created when the Unsigned Non-Driver Installation Behavior setting is changed in a Group Policy Object. | Low |
| User Account Control: Admin Approval Mode for the Built-in Administrator Account | Created when the User Account Control: Admin Approval Mode for the Built-in Administration Account policy is changed in a Group Policy Object. | Medium |
| User Account Control: Allow UIAccess Applications to Prompt for Evaluation Without Using the Secure Desktop | Created when the User Account Control: Allow UIAccess Applications to Prompt for Evaluation Without Using the Secure Desktop policy is changed in a Group Policy Object. | Medium |
| User Account Control: Behavior of the Elevation Prompt for Administrators in Admin Approval Mode | Created when the User Account Control: Behavior of the Elevation Prompt for Administrators in Admin Approval Mode policy is changed in a Group Policy Object. | Medium |
| User Account Control: Behavior of the Elevation Prompt for Standard Users | Created when the User Account Control: Behavior of the Elevation Prompt for Standard Users policy is changed in a Group Policy Object. | Medium |
| User Account Control: Detect Application Installations and Prompt for Elevation | Created when the User Account Control: Detect Application Installations and Prompt for Elevation policy is changed in a Group Policy Object. | Medium |
| User Account Control: Only Elevate Executables that are Signed and Validated | Created when the User Account Control: Only Elevate Executables that are Signed and Validated policy is changed in a Group Policy Object. | Medium |
| User Account Control: Only Elevate UIAccess Applications that are Installed in Secure Locations | Created when the User Account Control: Only Elevate UIAccess Applications that are Installed in Secure Locations policy is changed in a Group Policy Object. | Medium |
| User Account Control: Run All Administrators in Admin Approval Mode | Created when the User Account Control: Run All Administrators in Admin Approval Mode policy is changed in a Group Policy Object. | Medium |
| User Account Control: Switch to the Secure Desktop When Prompting for Elevation | Created when the User Account Control: Switch to the Secure Desktop When Prompting for Elevation policy is changed in a Group Policy Object. | Medium |
| User Account Control: Virtualize File and Registry Write Failures to Per-User Locations | Created when the User Account Control: Virtualize File and Registry Write Failures to Per-User Locations policy is changed in a Group Policy Object. | Medium |

Table 19. Group Policy Item events

| Event | Description | Severity |
|---|---|---|
| User Administrative Template Setting Changed | Created when a setting associated with a User Administrative Template is enabled, changed, or disabled. | Medium |
| User Application Data Folder Redirection Options Changed | Created when Settings properties of the Application Data policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Application Data Folder Redirection Target Path Changed | Created when Target properties of the Application Data policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Contacts Folder Redirection Options Changed | Created when Settings properties of the Contacts policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Contacts Folder Redirection Target Path Changed | Created when Target properties of the Contacts policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Credential Roaming Added | Created when user credential roaming is added to a Group Policy Object. | Medium |
| User Credential Roaming Changed | Created when changes are made to user credential roaming in a Group Policy Object. | Medium |
| User Credential Roaming Options Changed | Created when the user credential roaming options are changed in a Group Policy Object. | Medium |
| User Credential Roaming Removed | Created when user credential roaming is removed from a Group Policy Object. | Medium |
| User Desktop Folder Redirection Options Changed | Created when Settings properties of the Desktop policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Desktop Folder Redirection Target Path Changed | Created when Target properties of the Desktop policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Downloads Folder Redirection Options Changed | Created when Settings properties of the Downloads policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Downloads Folder Redirection Target Path Changed | Created when Target properties of the Downloads policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Favorites Folder Redirection Options Changed | Created when Settings properties of the Favorites policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Favorites Folder Redirection Target Path Changed | Created when Target properties of the Favorites policy are changed in the Windows Settings Folder Redirection Policies. | Medium |
| User Group Policy Preference Setting Changed | Created when a user preference in a group policy is enabled, changed, or disabled.<br>**NOTE:** Group policy preferences are available in Windows 2008 Group Policy Editor.<br>**NOTE:** This event is not available in earlier versions of Windows server. | Medium |
| User Group Policy Script setting changed | Created when a computer startup/shutdown script in a group policy is added, changed, or removed. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| User Internet Explorer Maintenance Automatic Browser Configuration Auto-config Option Changed | Created when the Automatic Configuration property of the Automatic Browser Configuration policy is changed in the Windows Settings Internet Explorer® Maintenance Connections policies. | Medium |
| User Internet Explorer Maintenance Automatic Browser Configuration Auto-config Time Changed | Created when the Automatically Configure Every xx Minutes property of the Automatic Browser Configuration policy is changed in the Windows Settings Internet Explorer Maintenance Connection policies. | Medium |
| User Internet Explorer Maintenance Automatic Browser Configuration Auto-config URL Changed | Created when the Auto-config URL property of the Automatic Browser Configuration policy is changed in the Windows Settings Internet Explorer Maintenance Connections policies. | Medium |
| User Internet Explorer Maintenance Automatic Browser Configuration Auto-detect Option Changed | Created when the Automatic Detect property of the Automatic Browser Configuration policy is changed in the Windows Settings Internet Explorer Maintenance Connections policies. | Medium |
| User Internet Explorer Maintenance Automatic Browser Auto-proxy URL Changed | Created when the Auto-proxy URL property of the Automatic Browser Configuration policy is changed in the Windows Settings Internet Explorer Maintenance Connections policies. | Medium |
| User Internet Explorer Maintenance Browser Title Changed | Created when the User Internet Explorer Maintenance Browser Title setting is changed. | Medium |
| User Internet Explorer Maintenance Connection Delete Existing Option Changed | Created when the Remove Old Dial-up Connections property of the Connection Settings policy is changed in the Windows Settings Internet Explorer Maintenance Connections policies. | Medium |
| User Internet Explorer Maintenance Connections Settings Import Option Changed | Created when Import Settings property of the Connection Settings policy is changed in the Windows Settings Internet Explorer Maintenance Connections policies. | Medium |
| User Internet Explorer Maintenance Content Ratings Option Changed | Created when the Content Ratings property in the Security Zones and Content Ratings policy is changed in the Windows Settings Internet Explorer Maintenance Security policies. | Medium |
| User Internet Explorer Maintenance Enable Trusted Publisher Lockdown Option Changed | Created when the Enable Trusted Publisher Lockdown property in the Authenticode Settings policy is changed in the Windows Settings Internet Explorer Maintenance Security policies. | Medium |
| User Internet Explorer Maintenance Important URLs Home Page URL Changed | Created when the Customize Home Page property in the Important URLs policy is changed in the Windows Settings Internet Explorer Maintenance URLs policies. | Medium |
| User Internet Explorer Maintenance Important URLs Online Support URL Changed | Created when the group policy setting for User Internet Maintenance Important URLs Help URL is changed. | Medium |
| User Internet Explorer Maintenance Important URLs Search Bar URL Changed | Created when the Customize Search Bar property in the Important URLs policy is changed in the Windows Settings Internet Explorer Maintenance URLs policies. | Medium |
| User Internet Explorer Maintenance Large Animated Logo Changed | Created when the Large Animated Logo Bitmap property of the Custom Logo policy is changed in the Windows Settings Internet Explorer Maintenance Browser User Interface policies. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| User Internet Explorer Maintenance Large Static Logo Changed | Created when the Large Static Logo Bitmap property of the Custom Logo policy is changed in the Windows Settings Internet Explorer Maintenance Browser User Interface policies. | Medium |
| User Internet Explorer Maintenance Program Settings Option Changed | Created when the Program Settings policy is changed in the Windows Settings Internet Explorer Maintenance Programs policies. | Medium |
| User Internet Explorer Maintenance Proxy Settings Configuration FTP Proxy Changed | Created when the FTP proxy URL property of the Proxy Settings policy is changed in the Windows Settings Internet Explorer Maintenance Connection policies. | Medium |
| User Internet Explorer Maintenance Proxy Settings Configuration Gopher Proxy Changed | Created when the Gopher proxy URL property of the Proxy Settings policy is changed in the Windows Settings Internet Explorer Maintenance Connection policies. | Medium |
| User Internet Explorer Maintenance Proxy Settings Configuration Secure Proxy Changed | Created when the Secure proxy URL property of the Proxy Settings policy is changed in the Windows Settings Internet Explorer Maintenance Connection policies. | Medium |
| User Internet Explorer Maintenance Proxy Settings HTTP Proxy Changed | Created when the HTTP proxy URL property of the Proxy Settings policy is changed in the Windows Settings Internet Explorer Maintenance Connection policies. | Medium |
| User Internet Explorer Maintenance Proxy Settings Proxy Exceptions Changed | Created when the Exceptions property of the Proxy Settings policy is changed in the Windows Settings Internet Explorer Maintenance Connection policies. | Medium |
| User Internet Explorer Maintenance Proxy Settings Socks Proxy Changed | Created when the Socks proxy URL property of the Proxy Settings policy is changed in the Windows Settings Internet Explorer Maintenance Connection policies. | Medium |
| User Internet Explorer Maintenance Security Zones and Privacy Customization Option Changed | Created when the Security Zones and Privacy property in the Security Zones and Content Ratings policy is changed in the Windows Settings Internet Explorer Maintenance Security policies. | Medium |
| User Internet Explorer Maintenance Small Animated Logo Changed | Created when the Small Animated Logo Bitmap property of the Custom Logo policy is changed in the Windows Settings Internet Explorer Maintenance Browser User Interface policies. | Medium |
| User Internet Explorer Maintenance Small Static Logo Changed | Created when the Small Static Logo Bitmap property of the Custom Logo policy is changed in the Windows Settings Internet Explorer Maintenance Browser User Interface policies. | Medium |
| User Internet Explorer Maintenance Toolbar Background Bitmap Changed | Created when the Background property of the Browser Toolbar Customizations policy is changed in the Windows Settings Internet Explorer Maintenance Browser User Interface policies. | Medium |
| User Internet Explorer Maintenance Toolbar Buttons Changed | Created when the Buttons property of the Browser Toolbar Customizations policy is changed in the Windows Settings Internet Explorer Maintenance Browser User Interface policies. | Medium |
| User Internet Explorer Maintenance URLs Browser Favorites List Changed | Created when the Favorites property in the Favorites and Links policy is changed in the Windows Settings Internet Explorer Maintenance URLs policies. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| User Internet Explorer Maintenance URLs Browser Links List Changed | Created when the Links property in the Favorites and Links policy is changed in the Windows Settings Internet Explorer Maintenance URLs policies. | Medium |
| User Internet Explorer Maintenance URLs Favorites and Links Delete Existing Channels Option Changed | Created when the Delete Existing Channels option in the Favorites and Links policy is changed in the Windows Settings Internet Explorer Maintenance URLs policies. | Medium |
| User Internet Explorer Maintenance URLs Favorites and Links Delete Existing Favorites Option Changed | Created when the Delete Existing Favorites and Links option in the Favorites and Links policy is changed in the Windows Settings Internet Explorer Maintenance URLs policies. | Medium |
| User Internet Explorer Maintenance URLs Favorites and Links Top of List Option Changed | Created when the Place Favorites and Links at the Top of the List option in the Favorites and Links policy is changed in the Windows Settings Internet Explorer Maintenance URLs policies. | Medium |
| User Internet Explorer Maintenance User Agent String Changed | Created when the User Agent String policy is changed in the Windows Settings Internet Explorer Maintenance Connection policies. | Medium |
| User Links Folder Redirection Options Changed | Created when Settings properties of the Links policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Links Folder Redirection Target Path Changed | Created when Target properties of the Links policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Music Folder Redirection Options Changed | Created when Settings properties of the Music policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Music Folder Redirection Target Path Changed | Created when Target properties of the Music policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User My Documents Folder My Pictures Preferences Changed | Created when My Pictures Settings properties of the My Documents policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User My Documents Folder Redirection Options Changed | Created when Settings (other than My Pictures) properties of the My Documents policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User My Documents Folder Redirection Target Path Changed | Created when Target properties of the My Documents policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Pictures Folder Redirection Options Changed | Created when Settings properties of the Pictures policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Pictures Folder Redirection Target Path Changed | Created when Target properties of the Pictures policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Public Key Policies Autoenrollment Settings Changed | Created when any properties of Autoenrollment Settings in the User Configuration Public Key Policies Enterprise Trust list is changed. | Medium |
| User Public Key Policies Enterprise Trust List Added | Created when a certificate is imported into the User Configuration Public Key Policies Enterprise Trust. | Medium |
| User Public Key Policies Enterprise Trust List Changed | Created when a certificate in the User Configuration Public Key Policies Enterprise Trust list is changed. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| User Public Key Policies Enterprise Trust List Removed | Created when a certificate in the User Configuration Public Key Policies Enterprise Trust list is removed. | Medium |
| User Saved Games Folder Redirection Options Changed | Created when Settings properties of the Saved Games policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Saved Games Folder Redirection Target Path Changed | Created when Target properties of the Saved Games policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Searches Folder Redirection Options Changed | Created when Settings properties of the Searches policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Searches Folder Redirection Target Path Changed | Created when Target properties of the Searches policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Software Installation Policy Added | Created when a User Software Installation Policy is added to User Configuration in Software Restriction policies. | Medium |
| User Software Installation Policy Changed | Created when a User Software Installation Policy is Changed in the User Configuration in Software Restriction policies. | Medium |
| User Software Installation Policy Removed | Created when a User Software Installation Policy is deleted from the User Configuration in Software Restriction policies. | Medium |
| User Software Restriction Basic User Hash Rule Added | Created when a Basic User Hash Rule is added to User Configuration Software Restriction policies. | Medium |
| User Software Restriction Basic User Hash Rule Changed | Created when a Basic User Hash Rule is changed in User Configuration Software Restriction policies. | Medium |
| User Software Restriction Basic User Hash Rule Removed | Created when a Basic User Hash Rule is removed from User Configuration Software Restriction policies. | Medium |
| User Software Restriction Basic User Path Rule Added | Created when a Basic User Path Rule is added to User Configuration Software Restriction policies. | Medium |
| User Software Restriction Basic User Path Rule Changed | Created when a Basic User Path Rule is changed in User Configuration Software Restriction policies. | Medium |
| User Software Restriction Basic User Path Rule Removed | Created when a Basic User Path Rule is removed in User Configuration Software Restriction. | Medium |
| User Software Restriction Basic User Zone Rule Added | Created when a Basic User Zone Rule is added to User Configuration Software Restriction policies. | Medium |
| User Software Restriction Basic User Zone Rule Changed | Created when a Basic User Zone Rule is changed in User Configuration Software Restriction policies. | Medium |
| User Software Restriction Basic User Zone Rule Removed | Created when a Basic User Zone Rule is removed in User Configuration Software Restriction. | Medium |
| User Software Restriction Designated File Types Changed | Created when the Designated File Types policy is changed in the Software Restriction Policies. | Medium |
| User Software Restriction Disallowed Certificate Rule Added | Created when a Disallowed level Certificate Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Certificate Rule Changed | Created when a Disallowed level Certificate Rule is changed in the Software Restriction Policies Additional Rules. | Medium |

**Table 19. Group Policy Item events**

| Event | Description | Severity |
|---|---|---|
| User Software Restriction Disallowed Certificate Rule Removed | Created when a Disallowed level Certificate Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Hash Rule Added | Created when a Disallowed level Hash Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Hash Rule Changed | Created when a Disallowed level Hash Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Hash Rule Removed | Created when a Disallowed level Hash Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Path Rule Added | Created when a Disallowed level Path Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Path Rule Changed | Created when a Disallowed level Path Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Path Rule Removed | Created when a Disallowed level Path Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Zone Rule Added | Created when a Disallowed level Zone Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Zone Rule Changed | Created when a Disallowed level Zone Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Disallowed Zone Rule Removed | Created when a Disallowed level Zone Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Enforcement Files Changed | Created when an Enforcement Policy Applicable Files option is changed in the Software Restriction policies. | Medium |
| User Software Restriction Enforcement Users Changed | Created when an Enforcement Policy Applicable Users option is changed in the Software Restriction policies. | Medium |
| User Software Restriction Policies Default Security Level Changed | Created when the default security level in the User Configuration Software Restriction Policies Security Levels folder is changed. | Medium |
| User Software Restriction Trusted Publishers Changed | Created when the Trusted Publishers policy is changed in the Software Restriction policies. | Medium |
| User Software Restriction Unrestricted Certificate Rule Added | Created when an Unrestricted level Certificate Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Certificate Rule Changed | Created when an Unrestricted level Certificate Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Certificate Rule Removed | Created when an Unrestricted level Certificate Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Hash Rule Added | Created when an Unrestricted level Hash Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Hash Rule Changed | Created when an Unrestricted level Hash Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Hash Rule Removed | Created when an Unrestricted level Hash Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Path Rule Added | Created when an Unrestricted level Path Rule is added to the Software Restriction Policies Additional Rules. | Medium |

Table 19. Group Policy Item events

| Event | Description | Severity |
|---|---|---|
| User Software Restriction Unrestricted Path Rule Changed | Created when an Unrestricted level Path Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Path Rule Removed | Created when an Unrestricted level Path Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Zone Rule Added | Created when an Unrestricted level Zone Rule is added to the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Zone Rule Changed | Created when an Unrestricted level Zone Rule is changed in the Software Restriction Policies Additional Rules. | Medium |
| User Software Restriction Unrestricted Zone Rule Removed | Created when an Unrestricted level Zone Rule is removed from the Software Restriction Policies Additional Rules. | Medium |
| User Start Menu Folder Redirection Options Changed | Created when Settings properties of the Start Menu policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Start Menu Folder Redirection Target Path Changed | Created when Target properties of the Start Menu policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Videos Folder Redirection Options Changed | Created when Settings properties of the Videos policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| User Videos Folder Redirection Target Path Changed | Created when Target properties of the Videos policy are changed in the Windows Settings Folder Redirection policies. | Medium |
| Wireless Network Policy Added | Created when a Wireless Network policy is added to the Computer Configuration Group Policy. | Medium |
| Wireless Network Policy Changed | Created when a Wireless Network policy in the Computer Configuration Group Policy is changed. | Medium |
| Wireless Network Policy Removed | Created when a Wireless Network policy is removed from the Computer Configuration Group Policy. | Medium |

# Group Policy Object

Table 20. Group Policy Object events

| Event | Description | Severity |
|---|---|---|
| DACL Changed on Group Policy Object | Created when a DACL is changed on a group policy object.<br>**NOTE:** Change Auditor access control list (ACL) events (discretionary access control list (DACL) and system access control list (SACL) changes), will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes. | High |
| Failed Group Policy Container Access (Change Auditor Protection) | Created when access to a group policy container is denied because it is locked down using the GPO protection feature of Change Auditor. | Medium |

**Table 20. Group Policy Object events**

| Event | Description | Severity |
|---|---|---|
| Failed Starter Group Policy Container Access (Change Auditor Protection) | Created when access to a Starter GPO is denied because it is locked down using the GPO protection feature of Change Auditor. | Medium |
| Group Policy Block Inheritance Setting Changed on Domain | Created when the block inheritance setting of a group policy linked to a domain is changed. | High |
| Group Policy Block Inheritance Setting Changed on OU | Created when the block inheritance setting of a group policy linked to an OU is changed. | High |
| Group Policy Block Inheritance Setting Changed on Site | Created when the blocked inheritance setting on a group policy linked to a site is changed. | High |
| Group Policy Disable Computer Configuration Flag Changed | Created when the disable computer configuration flag is changed. | Medium |
| Group Policy Disable User Configuration Flag Changed | Created when the disable user configuration flag is changed. | Medium |
| Group Policy Disabled Setting on Domain Changed | Created when the disabled setting of a group policy linked to a domain is changed. | High |
| Group Policy Disabled Setting on OU Changed | Created when the disabled setting of a group policy linked to an OU is changed. | Medium |
| Group Policy Disabled Setting on Site Changed | Created when the disabled setting of a group policy linked to a site is changed. | High |
| Group Policy Link Added to OU | Created when a group policy is associated with an OU. | High |
| Group Policy Link Added to Site | Created when a group policy link is associated with a site. | High |
| Group Policy Link Removed from OU | Created when a group policy link is disassociated from an OU. | High |
| Group Policy Link Removed from Site | Created when a group policy link is disassociated from a site. | High |
| Group Policy Link Settings Modified | Created when a group policy linked to an organizational unit has its flags attribute modified. | Medium |
| Group Policy Linked | Created when a group policy is linked to a domain. | High |
| Group Policy No Override Setting Changed on Domain | Created when the no override setting of a group policy linked to a domain is changed. | High |
| Group Policy No Override Setting Changed on OU | Created when the no override setting of a group policy linked to an OU is changed. | High |
| Group Policy No Override Setting Changed on Site | Created when the no override setting of a group policy linked to a site is changed. | High |
| Group Policy Object Added | Created when a group policy container is added to the policies container. | High |
| Group Policy Object Removed | Created when a group policy container is removed from the policies container. | High |
| Group Policy Object Renamed | Created when a group policy object is renamed. | High |
| Group Policy Unlinked | Created when a group policy link is detached from a domain. | High |
| Group Policy WMI Filter Changed | Created when the gPCWQLFilter attribute (WMI filter) of the objectClass=groupPolicyContainer is changed. | Medium |
| Inheritance Setting Changed on Group Policy Object | Created when the inheritance setting of a group policy object is changed. | High |
| Linked Group Policy on Domain Changed | Created when a group policy setting that is attached to a domain is changed. | High |

Table 20. Group Policy Object events

| Event | Description | Severity |
|---|---|---|
| Linked Group Policy on OU Changed | Created when a group policy setting that is attached to an OU is changed. | Medium |
| Linked Group Policy on Site Changed | Created when a group policy setting that is attached to the site is changed. | High |
| Owner Changed on Group Policy Object | Created when the owner is changed for a group policy object. | High |
| Starter GPO Created | Created when a Starter GPO is created. | Medium |
| Starter GPO Removed | Created when a Starter GPO is removed. | Medium |

# IP Security

Table 21. IP Security events

| Event | Description | Severity |
|---|---|---|
| IP Security Filter Action Created | Created when a new IP Security Filter Action is created. | Medium |
| IP Security Filter Action Deleted | Created when an IP Security Filter Action is removed. | Medium |
| IP Security Filter Action Option Changed | Created when an IP Security Filter Action Security option is changed. | Medium |
| IP Security Filter Action Security Method Changed | Created when an IP Security Filter Action Security Method is changed. | Medium |
| IP Security Filter List Created | Created when a new IP Security Filter List is created. | Medium |
| IP Security Filter List Deleted | Created when an IP Security Filter List is removed. | Medium |
| IP Security Filter List Option Changed | Created when an IP Security Filter List option is changed. | Medium |
| IP Security Policy Created | Created when a new IP Security setting is created in a domain. | Medium |
| IP Security Policy Deleted | Created when an IP Security setting is deleted from a domain. | Medium |
| IP Security Policy Key Exchange Settings Changed | Created when one or more key exchange settings are changed in an IP Security Policy. | Medium |
| IP Security Policy Option Changed | Created when one or more options are changed in an IP Security Policy. | Medium |
| IP Security Rule Created | Created when an IP Security Rule is created. | Medium |
| IP Security Rule Deleted | Created when an IP Security Rule is deleted. | Medium |
| IP Security Rule Filter Action Changed | Created when the Filter Action of an IP Security Rule is changed. | Medium |
| IP Security Rule Filter List Changed | Created when the Filter List of an IP Security Rule is changed. | Medium |
| IP Security Rule Option Changed | Created when one or more options are changed in an IP Security Rule. | Medium |
| Rule Added to IP Security Policy Rule List | Created when a rule is added (checked) to the IP Security Rule list of an IP Security Policy. | Medium |
| Rule Removed from IP Security Policy Rule List | Created when a rule is removed (cleared) from the IP Security Rule list of an IP Security Policy. | Medium |

# NETLOGON Service

**Table 22. NETLOGON Service events**

| Event | Description | Severity |
|---|---|---|
| NETLOGON AutoSiteCoverage Flag Changed | Created when the AutoSiteCoverage flag is changed. | Medium |
| NETLOGON CloseSiteTimeout Parameter Changed | Created when the CloseSiteTimeout value is changed. | Medium |
| NETLOGON Diagnostic Logging Parameter Changed | Created when the diagnostic log level for the NETLOGON service is changed. | Medium |
| NETLOGON DnsAvoidRegisterRecords Parameter Changed | Created when the contents of the DnsAvoidRegisterRecords registry entry is changed. | Medium |
| NETLOGON GcSiteCoverage Parameter Changed | Created when the GcSiteCoverage registry entry is changed. | Medium |
| NETLOGON LdapSrvPriority Parameter Changed | Created when the LdapSrvPriority registry entry is added, removed, or changed. | Medium |
| NETLOGON LdapSrvWeight Parameter Changed | Created when the LdapSrvWeight value is changed. | Medium |
| NETLOGON SiteCoverage Parameter Changed | Created when the contents of the SiteCoverage registry entry is changed. | Medium |
| NETLOGON SiteName Parameter Changed | Created when the SiteName registry entry is added, removed, or changed. | Medium |

# NTDS Service

**Table 23. NTDS Service events**

| Event | Description | Severity |
|---|---|---|
| NTDS Default TTL Changed | Created whenever the default TTL is changed. | Low |
| NTDS Garbage Collection Period Changed | Created whenever the garbage collection period is changed. | Low |
| NTDS Minimum TTL Changed | Created whenever the minimum TTL is changed. | Low |
| NTDS TCP/IP Port Assignment Changed | Created when the NTDS RPC TCP/IP port assignment is changed. | Low |
| NTDS Tombstone Lifetime Setting Changed | Created whenever the tombstone lifetime is altered. | Low |

# Organizational Unit (OU)

**Table 24. Organizational Unit (OU) events**

| Event | Description | Severity |
|---|---|---|
| Alternate UPN Suffix Added to OU | Created when an entry is added to the list of alternate user principal name (UPN) suffixes available for user names. | Medium |
| Alternate UPN Suffix Removed from OU | Created when an entry is removed from the list of alternate user principal name (UPN) suffixes available for user names. | Medium |
| DACL Changed on OU Object | Created when the DACL is changed on an OU object.<br>**NOTE:** Change Auditor access control list (ACL) events (discretionary access control list (DACL) and system access control list (SACL) changes), will not report inherited access control entry (ACE) changes. This event does NOT report inherited ACL changes. | High |
| Domain Controller Added to OU | Created when a domain controller is added to an OU. | High |
| Domain Controller Removed from OU | Created when a domain controller is removed from an OU. | High |
| OU Group Policy Order Changed | Created when the list of group policies linked to an organizational unit is re-ordered. | Medium |
| Inheritance Setting Changed on OU Object | Created when the inheritance setting of a OU object is changed. | High |
| Subordinate OU Added | Created when an OU is added to another OU. | Medium |
| Subordinate OU Removed | Created when an OU is removed from another OU. | Medium |
| Subordinate OU Renamed | Created when a subordinate OU is renamed. | Medium |

# Replication Transport

**Table 25. Replication Transport events**

| Event | Description | Severity |
|---|---|---|
| Bridge All Site Links Option Changed | Created when the Bridge all site links check box on the replication transport property page is changed. | Medium |

Table 25. Replication Transport events

| Event | Description | Severity |
|---|---|---|
| Ignore Link Schedules Option Changed | Created when the Ignore schedules check box on the replication transport property page is changed. | Medium |
| Irregular domain replication activity detected | This event identifies replication behavior that may indicate that DCSync is being used to retrieve password data through domain replication.<br>Irregular requests can include:<br>• Replication activity from the same source and target computer.<br>• Replication activity that is initiated by a user account instead of a computer account.<br>DCSync is a command within Mimikatz that can simulate the behaviour of a Domain Controller and make replication requests. This activity can result in someone gaining unauthorized access to user credentials. The stolen credentials can then be used to create a golden ticket or silver ticket and can be used for pass-the-hash and overpass-the-hash scenarios.<br>This event identifies replication behavior that may indicate that DCSync is being used to compromise the security of your network. | High |

# Schema Configuration

Table 26. Schema Configuration events

| Event | Description | Severity |
|---|---|---|
| Attribute Added to Optional Attributes | Created when a new attribute is added to the optional attributes for a class object in the schema. | High |
| Attribute Removed from Optional Attributes | Created when an attribute is removed from the Optional Attributes for a class object in the schema. | High |
| Class Removed from Auxiliary Classes in Schema | Created when a class is removed from auxiliaryClass. | High |
| Class Removed from Possible Superiors in Schema | Created when a class is removed from possSuperiors. | High |
| New Class Added to Auxiliary Classes in Schema | Created when a new class is added to auxiliaryClass. | High |
| New Class Added to Possible Superiors in Schema | Created when a new class is added to possSuperiors. | High |
| Schema Attribute Added | Created when a new attribute is added to the schema. | High |
| Schema Attribute Confidential flag changed | Created when an Attribute Confidential flag is changed. | High |
| Schema Attribute defaultHidingValue Changed | Created when the defaultHidingValue is changed. | High |
| Schema Attribute GC Flag Changed | Created when the GC flag for an attribute is changed. | High |
| Schema Attribute Indexing Flag Changed | Created when the indexing flag for an attribute is changed. | High |
| Schema Attribute RODC Filtered flag changed | Created when an Attribute RODC Replication flag is changed. | High |

Table 26. Schema Configuration events

| Event | Description | Severity |
|---|---|---|
| Schema Class Added | Created when a new class is added to the schema. | High |
| Schema Class Default Security Descriptor Changed | Created when the default security descriptor for a class is changed. | High |
| Schema Object Disabled | Created when a schema object is marked disabled. | High |
| Schema Object Enabled | Created when a schema object is marked enabled. | High |
| Schema Version Changed | Created when the schema version number changes. | High |

# Site Configuration

Table 27. Site Configuration events

| Event | Description | Severity |
|---|---|---|
| Automatic Intersite Topology Generation Role Changed | Created when the intersite topology generation role is assigned to another DC. | Medium |
| Automatic Intersite Topology Generator for the Site has been Disabled | Created when intersite topology generation is disabled for a site. | High |
| Automatic Intersite Topology Generator for the Site has been Enabled | Created when intersite topology generation is enabled for a site. | Medium |
| Automatic Intrasite Topology Generation for the Site has been Enabled | Created when intrasite topology generation is enabled for a site. | Medium |
| Automatic Intrasite Topology Generator for the Site has been Disabled | Created when intrasite topology generation is disabled for a site. | High |
| Default Site Query Policy Object Changed | Created when the default query policy object reference for a site is changed. | Medium |
| Domain Controller Moved to Site | Created when a Domain controller is moved to a site. | Medium |
| Linked Query Policy Object for Site Changed | Created when the query policy object referred to by a site is changed. | Medium |
| Site Group Policy Order Changed | Created when the list of group policies linked to a site is re-ordered. | Medium |
| Site License Server Changed | Created when the licensing server for the site is changed. | Medium |

# Site Link Bridge Configuration

Table 28. Site Link Bridge Configuration events

| Event | Description | Severity |
|---|---|---|
| Site Link Added to Site Link Bridge | Created when a site link has been added to a site link bridge. | Medium |
| Site Link Removed from Site Link Bridge | Created when a site link has been removed from a site link bridge. | High |

# Site Link Configuration

**Table 29. Site Link Configuration events**

| Event | Description | Severity |
|---|---|---|
| Inter-site Compression Setting Changed | Created when the inter-site compression setting for a site link is changed. | Medium |
| Interval Changed | Created when a change is detected in the Interval attribute of a site link. | High |
| Link Cost Changed | Created when a change is detected in the cost attribute of a site link. | High |
| Schedule Changed | Created when a change is detected in the schedule attribute of a site link. | High |
| Site Added to Site List | Created when a site is added to a site list. | Medium |
| Site Removed from Site List | Created when a site is removed from a site list. | High |

# Subnets

**Table 30. Subnets event**

| Event | Description | Severity |
|---|---|---|
| Subnet Site Assignment Changed | Created when the site association of a subnet is changed | Medium |

# SYSVOL

**Table 31. SYSVOL events**

| Event | Description | Severity |
|---|---|---|
| SYSVOL Folder Access Rights Changed | Created when access to the SYSVOL folder has been changed via Access Control Settings for SYSVOL or Share Permissions.<br>Disabled by default. | Medium |
| SYSVOL Folder Auditing Changed | Created when the SACL on the SYSVOL folder has been changed.<br>Disabled by default. | Medium |
| SYSVOL Folder Ownership Changed | Created when ownership of the SYSVOL folder has been changed.<br>Disabled by default. | Medium |

# 3

# Log Events

When event logging for Active Directory is enabled in Change Auditor, events will also be written to the InTrust® for AD event log. In addition, when event logging for ADAM (AD LDS) is enabled in Change Auditor, ADAM events will be written to the InTrust for ADAM event log. These log events can then be gathered by InTrust for further processing and reporting.

**NOTE:** To enable event logging, select Event Logging on the Agent Configuration page (Administration Tasks tab), and select the type of event logging to enable.

The tables in this section list the log events capture when Active Directory and/or ADAM event logging is enabled. They are listed in numeric order by event ID based on the event log to which they are recorded:

- InTrust for AD event log
- InTrust for ADAM event Log

# InTrust for AD event log

The following table lists the Active Directory events that are recorded to the InTrust for AD event log when Active Directory event logging is enabled in Change Auditor.

**Table 32. InTrust for AD event log events**

| Event ID | Description |
|---|---|
| 1 | Attempt to modify AD object was denied by the system |
| 2 | Attempt to delete AD object was denied by the system |
| 3 | AD object was successfully modified |
| 4 | AD object was successfully deleted |
| 5 | Attempt to modify AD object was denied by Change Auditor for Active Directory |
| 6 | Attempt to delete AD object was denied by Change Auditor for Active Directory |
| 8 | Attempt to delete Group Policy was denied by the system |
| 9 | Group Policy was successfully modified |
| 10 | Group Policy was successfully deleted |
| 11 | Attempt to modify Group Policy was denied by Change Auditor for Active Directory |
| 13 | Attempt to move AD object was denied by the system |
| 14 | AD object was successfully moved |
| 15 | Attempt to move AD object was denied by Change Auditor for Active Directory |
| 16 | Attempt to create AD object was denied by the system |
| 17 | AD object was successfully created |
| 18 | Attempt to create AD object was denied by Change Auditor for Active Directory |
| 19 | Attempt to create Group Policy was denied by the system |
| 20 | Group Policy was successfully created |
| 21 | Attempt to create Group Policy was denied by Change Auditor for Active Directory |

**Table 32. InTrust for AD event log events**

| Event ID | Description |
|---|---|
| 22 | Attempt to modify a property of AD object was denied by the system |
| 23 | Property of AD object was successfully modified |
| 24 | Attempt to modify a property of AD object was denied by Change Auditor for Active Directory |
| 25 | Heartbeat – Change Auditor for Active Directory is currently active on this computer |
| 26 | Protected objects cache update failure |
| 27 | Protected objects cache reload |
| 31 | AD object was successfully protected |
| 32 | AD object protection was successfully removed |
| 33 | AD object protection was successfully modified |
| 37 | Group Policy was successfully protected |
| 38 | Group Policy protection was successfully removed |
| 39 | Group Policy protection was successfully modified |
| 40 | Attempt to modify AD object security descriptor was denied by the system |
| 41 | Attempt to modify AD object ownership was denied by the system |
| 42 | Attempt to modify user mailbox access rights was denied by the system |
| 43 | AD object security descriptor was successfully modified |
| 44 | AD object ownership was successfully changed |
| 45 | Attempt to modify user mailbox ownership was denied by the system |
| 46 | Attempt to modify AD object security descriptor was denied by Change Auditor for Active Directory |
| 47 | Attempt to modify AD object ownership was denied by Change Auditor for Active Directory |
| 48 | User mailbox access rights were successfully changed |
| 49 | User mailbox ownership was successfully changed |
| 50 | Attempt to modify user mailbox access was denied by Change Auditor for Active Directory |
| 51 | Attempt to modify user mailbox ownership was denied by Change Auditor for Active Directory |
| 52 | Attempt to modify linked Group Policy objects was denied by the system |
| 53 | Linked Group Policy objects were successfully modified |
| 54 | Attempt to modify linked Group Policy objects was denied |
| 63 | Group Policy Template was successfully modified |
| 64 | Attempt to modify Group Policy Template was denied |
| 65 | DNS record added |
| 66 | DNS record deleted |
| 67 | DNS record changed |
| 69 | List of excluded accounts was successfully changed |
| 70 | Service start failure |
| 71 | Group policy backup is not available |
| 72 | Group policy backup is now available |
| 74 | List of protected attributes was successfully changed |
| 76 | Protection group settings was successfully changed |
| 78 | Protection group was successfully created |
| 80 | Protection group was successfully deleted |
| 82 | Protection group was successfully renamed |
| 84 | Audit filter list was successfully changed |

**Table 32. InTrust for AD event log events**

| Event ID | Description |
|---|---|
| 85 | Event log was cleared |
| 86 | Service critical error |
| 87 | Account locked out |
| 88 | Account unlocked |
| 89 | Attempt to unlock user account was denied by the system |
| 90 | Attempt to unlock user account was denied by Change Auditor for Active Directory |
| 101 | Group member-of added |
| 102 | Group member-of removed |
| 151 | User member-of added |
| 152 | User member-of removed |
| 201 | Starter GPO Computer setting changed |
| 202 | Starter GPO User setting changed |
| 251 | Starter GPO created |
| 252 | Starter GPO removed |
| 301 | IP Security Filter Action created |
| 302 | IP Security Filter Action deleted |
| 303 | IP Security Filter Action Option changed |
| 304 | IP Security Filter Action Security Method changed |
| 305 | IP Security Filter List created |
| 306 | IP Security Filter List deleted |
| 307 | IP Security Filter List Option changed |
| 308 | IP Security Policy created |
| 309 | IP Security Policy deleted |
| 310 | IP Security Policy Key Exchange Settings changed |
| 311 | IP Security Policy Option changed |
| 312 | IP Security Rule created |
| 313 | IP Security Rule deleted |
| 314 | IP Security Rule Filter Action changed |
| 315 | IP Security Rule Filter List changed |
| 316 | IP Security Rule Option changed |
| 317 | Rule added to IP Security Policy Rule List |
| 318 | Rule removed from IP Security Policy Rule List |
| 361 | Expires after period changed in DNS zone |
| 362 | Name server added to DNS zone |
| 363 | Name server removed from DNS zone |
| 364 | Primary server changed in DNS zone |
| 365 | Refresh interval changed in DNS zone |
| 366 | Retry interval changed in DNS zone |
| 367 | WINS forwarding flag disabled in DNS zone |
| 368 | WINS forwarding flag enabled in DNS zone |
| 369 | WINS forwarding host list changed in DNS zone |
| 370 | Zone default TTL changed in DNS zone |

**Table 32. InTrust for AD event log events**

| Event ID | Description |
|---|---|
| 371 | Zone delegation added to DNS zone |
| 372 | Zone delegation removed from DNS zone |
| 373 | DNS Zone added |
| 374 | DNS Zone deleted |
| 401 | Attribute added to the optional attributes for a class object in the schema |
| 402 | Attribute removed from the optional attributes for a class object in the schema |
| 403 | Class removed from auxiliary classes in schema |
| 404 | Class removed from possible superiors in schema |
| 405 | New class added to auxiliary classes in schema |
| 406 | New class added to possible superiors in schema |
| 407 | Schema attribute added |
| 408 | Schema attribute flag changed |
| 409 | Schema class added |
| 410 | Schema class default security descriptor changed |
| 411 | Schema object changed |
| 412 | Schema version changed |
| 413 | Schema class deactivated |
| 414 | Schema class reactivated |
| 415 | Schema attribute deactivated |
| 416 | Schema attribute reactivated |
| 501 | Computer Software Restriction Basic User Hash Rule added, changed or removed |
| 502 | Computer Software Restriction Basic User Path Rule added, changed or removed |
| 503 | Computer Software Restriction Basic Zone Rule added, changed or removed |
| 504 | Computer Software Restriction Designated File Types changed |
| 505 | Computer Software Restriction Disallowed Certificate Rule added, changed or removed |
| 506 | Computer Software Restriction Disallowed Hash Rule added, changed or removed |
| 507 | Computer Software Restriction Disallowed Path Rule added, changed or removed |
| 508 | Computer Software Restriction Disallowed Zone Rule added, changed or removed |
| 509 | Computer Software Restriction Enforcement Files option changed |
| 510 | Computer Software Restriction Enforcement Users option changed |
| 511 | Computer Software Restriction Policies Default Security level changed |
| 512 | Computer Software Restriction Trusted Publishers policy changed |
| 513 | Computer Software Restriction Unrestricted Certificate Rule added, changed or removed |
| 514 | Computer Software Restriction Unrestricted Hash Rule added, changed or removed |
| 515 | Computer Software Restriction Unrestricted Path Rule added, changed or removed |
| 516 | Computer Software Restriction Unrestricted Zone Rule added, changed or removed |
| 521 | Computer Software Installation Policy added, changed or removed |
| 531 | Computer Public Key Policies Autoenrollment settings changed |
| 532 | Computer Public Key Policies Automatic Certificate Request added, changed or removed |
| 533 | Computer Public Key Policies Encrypting File System DRA added, changed or removed |
| 534 | Computer Public Key Policies Enterprise Trust List added, changed or removed |
| 535 | Computer Public Key Policies Trusted Root Certification Authority changed |

Table 32. InTrust for AD event log events

| Event ID | Description |
|---|---|
| 541 | User Software Restriction Basic User Hash Rule changed |
| 542 | User Software Restriction Basic User Path Rule added, changed or removed |
| 543 | User Software Restriction Basic User Zone Rule added, changed or removed |
| 544 | User Software Restriction Designated File Types changed |
| 545 | User Software Restriction Disallowed Certificate Rule added, changed or removed |
| 546 | User Software Restriction Disallowed Hash Rule added, changed or removed |
| 547 | User Software Restriction Disallowed Path Rule added, changed or removed |
| 548 | User Software Restriction Disallowed Zone Rule added, changed or removed |
| 549 | User Software Restriction Enforcement Files option changed |
| 550 | User Software Restriction Enforcement Users option changed |
| 551 | User Software Restriction Policies Default Security Level changed |
| 552 | User Software Restriction Trusted Publishers policy changed |
| 553 | User Software Restriction Unrestricted Certificate Rule added, changed or removed |
| 554 | User Software Restriction Unrestricted Hash Rule added, changed or removed |
| 555 | User Software Restriction Unrestricted Path Rule added, changed or removed |
| 556 | User Software Restriction Unrestricted Zone Rule added, changed or removed |
| 581 | User Software Installation Policy added, changed or removed |
| 601 | User Public Key Policies Autoenrollment Settings changed |
| 602 | User Public Key Policies Enterprise Trust List added, changed or removed |

# InTrust for ADAM event Log

The following table lists the ADAM (AD LDS) events that are recorded to the InTrust for ADAM event log when ADAM (AD LDS) event logging is enabled.

Table 33. InTrust for ADAM event log events

| Event ID | Description |
|---|---|
| 1 | Attempt to modify ADAM object was denied by the system |
| 2 | Attempt to delete ADAM object was denied by the system |
| 3 | ADAM object was successfully modified |
| 4 | ADAM object was successfully deleted |
| 5 | Attempt to modify ADAM object was denied by Change Auditor |
| 6 | Attempt to modify ADAM object was denied by Change Auditor |
| 13 | Attempt to move ADAM object was denied by system |
| 14 | ADAM object was successfully moved |
| 15 | Attempt to move ADAM object was denied by Change Auditor |
| 16 | Attempt to create ADAM object was denied by system |
| 17 | ADAM object was successfully created |
| 18 | Attempt to create ADAM object was denied by Change Auditor |
| 22 | Attempt to modify property of ADAM object was denied by the system |
| 23 | Property of ADAM object was successfully modified |
| 24 | Attempt to modify a property of ADAM object was denied by Change Auditor |

**Table 33. InTrust for ADAM event log events**

| Event ID | Description |
|---|---|
| 25 | Heartbeat – Change Auditor for ADAM service is currently active on this computer |
| 27 | Protected objects cache reload |
| 31 | ADAM object was successfully protected |
| 32 | ADAM object protection was successfully removed |
| 33 | ADAM object protection was successfully modified |
| 40 | Attempt to modify ADAM object security descriptor was denied by the system |
| 41 | Attempt to modify ADAM object ownership was denied by the system |
| 43 | ADAM object security descriptor was successfully modified |
| 44 | ADAM object ownership was successfully changed |
| 46 | Attempt to modify ADAM object security descriptor was denied |
| 47 | Attempt to modify ADAM object ownership was denied |
| 69 | List of excluded accounts was successfully changed |
| 70 | Service start failure |
| 71 | Invalid ADAM instance |
| 74 | List of protected attributes was successfully changed |
| 76 | Protected attributes list mode was successfully changed |
| 78 | Protection group was successfully created |
| 80 | Protection group was successfully deleted |
| 82 | Protection group was successfully renamed |
| 84 | Audit filter list was successfully changed |
| 85 | Event log was cleared |
| 86 | Service critical error |

# About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

## Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

## Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

## Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.