Quest® Change Auditor 7.5

# Built-in Reports Reference Guide

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:
Quest Software Inc.
Attn: LEGAL Dept.
20 Enterprise, Suite 100
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.**

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

Change Auditor Built-in Reports Reference Guide
Updated - January 2025
Software Version - 7.5

# Contents

# 1

# Introduction

Change Auditor provides predefined reports which allow you to quickly retrieve valuable configuration change information from various perspectives.

> **NOTE:** The terms ‘searches’ and ‘reports’ are used in conjunction to acquire the wanted output. You run a ‘search’ and the results returned are referred to as a ‘report’.

### *To run a built-in search:*

1. Click the **Searches** tab or select **View | Searches** to open the Searches page.
2. Expand and select the appropriate folder in the explorer view to display the list of search definitions stored in the selected folder.
3. In the right pane, locate the search to run and use one of the following methods to run the selected search:
    - Double-click a search definition
    - Right-click a search definition and select **Run**
    - Select the search definition and click **Run**
4. A new Search Results page displays populated with the audited events that met the search criteria defined in the selected search definition.

This guide contains a list of the all the built-in reports provided with Change Auditor. They are listed according to the folder structure under the Shared folder on the Searches page.

> **NOTE:** Many of the built-in reports are only available when the appropriate Change Auditor license is applied For example, to capture Exchange events, Quest$^{®}$ Change Auditor for Exchange must be licensed. Some built-in reports also require auditing templates to define the auditing scope. For example, to capture File System events, you must first define a template to specify the files and folders and events to audit.
>
> Change Auditor does not prevent you from running any of the built-in reports; however, associate events are not captured unless the proper license and auditing template is applied. See the individual Change Auditor user guides for more information about auditing key environments.

2

# Built-in reports

The following criteria defines the contents of the default ‘My Favorite’ report that is displayed on the Overview page:

### Change Auditor Real-Time

Who = All Users

What = All Event Classes

Where = All sources

When = Last 20 minutes

Origin = All workstations/servers

The other built-in reports provided with Change Auditor are available under the following folders:

- Active Directory Federation Services
- AD Query
- All Events
- Authentication Services
- Microsoft Entra
- Defender
- Microsoft 365
- Logon Activity
- Recommended Best Practices
- Regulatory Compliance
- Security
- SharePoint
- SQL Data Level
- SQL Extended Events
- Threat Detection

# Active Directory Federation Services

### All Active Directory Federation Services sign-ins in the last 24 hours

Who = All Users

What = Active Directory Federation Services - Sign-in facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Claims Provider Trust events in the last 30 days

Who = All Users

What = Active Directory Federation Services - Claims Provider Trusts facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### All Endpoint events in the last 30 days

Who = All Users

What = Active Directory Federation Services - Endpoints facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### All Successful Active Directory Federation Services sign-ins in the last 24 hours

Who = All Users

What = Successful Active Directory Federation Services sign-in

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Failed Active Directory Federation Services sign-ins in the last 7 days

Who = All Users

What = Failed Active Directory Federation Services sign-in

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Authentication Method events in the last 30 days

Who = All Users

What = Active Directory Federation Services - Authentication Methods facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### All Relying Party Trust events in the last 30 days

Who = All Users

What = Active Directory Federation Services - Relying Party Trusts facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# AD Query

ℹ **NOTE:** By default, the AD Query reports include the following information on the Search Results page: Origin, LDAP Attributes, LDAP Scope, LDAP Filter, LDAP Type, LDAP Occurrences, LDAP Elapsed, LDAP Since, and LDAP Results. These additional columns are defined using the Layout tab.

### All AD Queries grouped by AD search filter

Who = All Users

What = AD Query Performed

Where = All sources

When = N/A

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped); LDAP Filter (Grouped)

### All AD Queries grouped by AD starting point

Who = All Users

What = AD Query Performed

Where = All sources

When = N/A

Origin = All workstations/servers

Layout Tab - Order By: Time Detected (Not Grouped); Object Canonical (Grouped)

### All AD Queries grouped by number of results

Who = All Users

What = AD Query Performed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout Tab - Order By: Time Detected (Not Grouped); LDAP Results (Grouped)

### All AD Queries grouped by originating hostname\IP address

Who = All Users

What = AD Query Performed

Where = All sources

When = N/A

Origin = All workstations/servers

Layout Tab - Order By: Time Detected (Not Grouped); Origin (Grouped)

### All AD Queries grouped by time elapsed (query run time)

Who = All Users

What = AD Query Performed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout Tab - Order By: Time Detected (Not Grouped); LDAP Elapsed (Grouped)

### All AD Queries in the last 1 week

Who = All Users

What = AD Query Performed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All AD Queries in last 30 days

Who = All Users

What = AD Query Performed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# All Events

### All Account Lockout events

Who = All Users

What = Local User Account Locked; Local User Account Unlocked; User Account Locked; User Account Unlocked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Active Directory Database Events

Who = All Users

What = Active Directory Database facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Active Directory events

Who = All Users

What = Active Directory subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Active Directory events including ActiveRoles/GPOADmin initiator

(Returns all Active Directory events, displaying the Initiator UserName and EventSource in the Search Results)

Who = All Users

What = Active Directory subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout Tab - Selected Columns: Initiator UserName and EventSource are added to default list

### All AD Query events

Who = All Users

What = AD Query facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All ADAM (AD LDS) events

Who = All Users

What = ADAM (AD LDS) subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Change Auditor Internal Auditing events

Who = All Users

What = Change Auditor Internal Auditing facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Computer events

Who = All Users

What = Custom Computer Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Connection Object events

Who = All Users

What = Connection Object facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All DNS events

Who = All Users

What = DNS Service facility; DNS Zone facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Domain Controller events

Who = All Users

What = Configuration Monitoring facility

Where = Domain Controller

When = Last 7 days

Origin = All domain controllers

### All Domain events

Who = All Users

What = Domain Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Dynamic Access Control events

Who = All Users

What = Dynamic Access Control facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All EMC events

Who = All Users

What = EMC facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All events

Who = All Users

What = All Event Classes

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All events in the past 24 hours

Who = All Users

What = All Event Classes

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Exchange events

Who = All Users

What = Exchange subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Fault Tolerance events

Who = All Users

What = Fault Tolerance facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All File System events

Who = All Users

What = Custom File System Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Forest Configuration events

Who = All Users

What = Forest Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All FRS events

Who = All Users

What = FRS Service facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Group events

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group; Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group

Custom Group Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Group Policy events

Who = All Users

What = Group Policy Link Added to OU; Group Policy Link Removed from OU; Group Policy Link Setting Modified; Group Policy Link Added to Site; Group Policy Link Removed from Site

Group Policy Item facility; Group Policy Object facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Group Policy events including GPOADmin initiator

Returns all Group Policy events, displaying the Initiator UserName and EventSource in the Search Results

Who = All Users

What = Group Policy subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout Tab - Selected Columns: Initiator UserName and EventSource are added to default list

### All IP Security events

Who = All Users

What = IP Security facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Irregular Domain Replication Activity events

Who = All Users

What = Irregular domain replication activity detected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Irregular Domain Controller Registration events

Who = All Users

What = Irregular domain controller registration activity detected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All NetApp events

Who = All Users

What = NetApp facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All NETLOGON events

Who = All Users

What = NETLOGON Service facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All NTDS events

Who = All Users

What = NTDS Service facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Object Restore events

Who = All Users

What = Computer Added; Domain Added; Exchange Group Added (Exchange 2003); Group Object Added; Group Policy Object Added; Subordinate OU Added; User Object Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All OU events

Who = All Users

What = OU facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Registry events

Who = All Users

What = Registry subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Replication events

Who = All Users

What = Replication Transport facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Schema Configuration events

Who = All Users

What = Schema Configuration facility

Schema FSMO Role Owner Moved; Schema Modifications Allowed Flag Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Services events

Who = All Users

What = Service Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Site events

Who = All Users

What = Site Added; Site Removed; Site Renamed; Site Link Added; Site Link Removed; Site Link Bridge Added; Site Link Bridge Removed

Site Configuration facility; Site Link Bridge Configuration facility; Site Link Configuration facility; Subnets facility; Connection Object facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All System events

Who = All Users

What = System Events facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All SYSVOL events

Who = All Users

What = SYSVOL facility

SYSVOL Location Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All User events

Who = All Users

What = Custom User Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Authentication Services

### All Authentication Services events in last 30 days

Who = All Users

What = Authentication Monitoring facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Authentication Services computer object auditing in last 30 days

Who = All Users

What = Authentication Services Computer Object Added; Authentication Services Computer Object Attribute Changed; Authentication Services Computer Object Deleted; Authentication Services Computer Object Moved; Authentication Services Computer Object Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Authentication Services computers added in last 30 days

Who = All Users

What = Authentication Services Computer Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Authentication Services computers deleted in last 30 days

Who = All Users

What = Authentication Services Computer Object Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Authentication Services GPO settings changes in last 30 days

Who = All Users

What = Authentication Services GPO Setting Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Groups set to UNIX-disabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for Group - Restriction = To: Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Groups set to UNIX-enabled and created in last 30 days

Who = All Users

What = UNIX-Enabled Changed for Group; UNIX-Enabled Group Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Groups set to UNIX-enabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for Group - Restriction = To: Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### NIS object auditing in last 30 days

Who = All Users

What = NIS Object Added; NIS Object Attribute Changed; NIS Object Deleted; NIS Object Moved; NIS Object Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Personality object auditing in last 30 days

Who = All Users

What = Personality Object Added; Personality Object Attribute Changed; Personality Object Deleted; Personality Object Moved; Personality Object Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX home directory changed in last 30 days

Who = All Users

What = UNIX Home Directory Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX login shell changed in last 30 days

Who = All Users

What = UNIX Login Shell Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX-enabled groups created in last 30 days

Who = All Users

What = UNIX-Enabled Group Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX-enabled groups deleted in last 30 days

Who = All Users

What = UNIX-Enabled Group Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX-enabled users created in last 30 days

Who = All Users

What = UNIX-Enabled User Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX-enabled users deleted in last 30 days

Who = All Users

What = UNIX-Enabled User Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users set to UNIX-disabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User - Restriction = To: Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users set to UNIX-enabled and created in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User; UNIX-Enabled User Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users set to UNIX-enabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User - Restriction = To: Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Microsoft Entra

### All Microsoft Entra application events in the past 7 days

What = Microsoft Entra - Application facility

When = Last 7 days

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra directory events in the past 7 days

What = Microsoft Entra - Directory facility

When = Last 7 days

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra events in the past 7 days

Who = All Users

What = Microsoft Entra subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra events in the past 7 days by activity

Who = All Users

What = Microsoft Entra subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected, Grouped by Activity Name/Operation

### All Microsoft Entra events in the past 7 days by activity type

Who = All Users

What = Microsoft Entra subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout: Order by: Time Detected, Grouped by Activity type

### All Microsoft Entra events in the past 7 days by category

Who = All Users

What = Microsoft Entra subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout: Order by: Time Detected, Grouped by Category

### All Microsoft Entra policy events in the past 7 days

What = Microsoft Entra - Policy facility

When = Last 7 days

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra resource events in the past 7 days

What = Microsoft Entra - Resource facility

When = Last 7 days

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra self-service activity events in the past 7 days

What = Microsoft Entra subsystem, Activity Name Like = *self-serv*

When = Last 7 days

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra sign-ins in the last 24 hours

Who = All Users

What = Microsoft Entra – Sign-in facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra synchronized events in the past 7 days

What = Microsoft Entra subsystem, Activity Origin EQUALS AD

When = Last 7 days

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra user events in the past 7 days

What = Microsoft Entra - User facility

When = Last 7 days

Layout tab - Order By: Time Detected (Not Grouped)

## Group

### All Microsoft Entra group events in the past 7 days

What = Microsoft Entra - Group facility

When = Last 7 days

Layout tab - Order By: Time Detected (Not Grouped)

### Group membership changes in the last 30 days grouped by group

What: Group member added, Group member removed

When: Last 30 days

Layout tab - Order By: Time Detected (Group by: Target Display Name)

### Group membership changes in the last 30 days grouped by member

What: Member added to group, Member removed from group

When: Last 30 days

Layout tab - Order By: Time Detected (Group by: Target Display Name)

### Group owner changes in the last 30 days grouped by group

What: Group Owner added, Group owner removed

When: Last 30 days

Layout tab - Order By: Time Detected (Group by: Target Display Name)

### Group owner changes in the last 30 days grouped by owner

What: Owner added to group, Owner removed from group

When: Last 30 days

Layout tab - Order By: Time Detected (Group by: Target Display Name)

## Risky Sign-Ins

### All Microsoft Entra sign-in from anonymous IP address events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE Sign-in from anonymous IP address

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra Sign-in from confirmed compromised user events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE Sign-in from confirmed compromised user

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra sign-in from IP address with malicious activity events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE Sign-in from IP address with malicious activity

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra sign-in from IP address with suspicious activity events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE Sign-in from IP address with suspicious activity

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra sign-in from malware-infected device events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE sign-in from malware-infected device

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra sign-in risk event changes in the past 7 days

Who = All Users

What = Microsoft Entra – Risk Event facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra sign-in with impossible travel events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE sign-in with impossible travel

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra sign-in with valid credentials from blocked IP address events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE sign-in with valid credentials from blocked IP address

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra sign-in with unfamiliar location or properties events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE sign-in with unfamiliar location or other properties

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra suspicious manipulation or rules in user's inbox events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE suspicious manipulation or rules in user’s inbox

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra user activity with known sign-in attack pattern events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE user activity with known sign-in attack pattern

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra user activity with known attack pattern events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE user activity with known attack pattern

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra unlikely travel between sign-in source locations events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE unlikely travel between sign-in source locations

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft Entra user sign-in with leaked credentials events in the past 7 days

Who = All Users

What = Microsoft Entra – Target LIKE User with leaked credential

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

## Role

### All Microsoft Entra role events in the past 7 days

What = Microsoft Entra - role facility

When = Last 7 days

Layout tab - Order By: Time Detected (Not Grouped)

### Global Administrator role membership changes in the last 30 days

What = Microsoft Entra - role facility - Role member added, Role member removed, Eligible member added to role, Eligible member removed from role.

When = Last 30 days

Layout tab - Order By: Time Detected (Not Grouped)

### Role membership changes in the last 30 days grouped by member

What = Microsoft Entra - role facility - Role assigned to eligible member, Role assigned to member, Roll removed from eligible member, Role removed from member

When = Last 30 days

Layout tab - Order By: Time Detected (Group by: Target Display Name)

### Role membership changes in the last 30 days grouped by role

What = Microsoft Entra - role facility - Role member added, Role member removed, Eligible member added to role, Eligible member removed from role.

When = Last 30 days

Layout tab - Order By: Time Detected (Group by: Target Display Name)

## Defender

### All Defender events in last 30 days

Who = All Users

What = Defender facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member added to access node in last 30 days

Who = All Users

What = Member Added to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member removed from access node in last 30 days

Who = All Users

What = Member Removed from Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node added in last 30 days

Who = All Users

What = Defender Access Node Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node removed in last 30 days

Who = All Users

What = Defender Access Node Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender password events in last 30 days

Who = All Users

What = Defender Password Changed; Defender Password Cleared; Defender Password Expiry Cleared; Defender Password Expiry Set; Defender Password Set

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy added in last 30 days

Who = All Users

What = Defender Policy Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy change events in last 30 days

Who = All Users

What = Defender Policy Changed for Access Node; Defender Policy Changed for Group; Defender Policy Changed for Security Server; Defender Policy Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy removed in last 30 days

Who = All Users

What = Defender Policy Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload added in last 30 days

Who = All Users

What = Defender RADIUS Payload Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload change events in last 30 days

Who = All Users

What = Defender RADIUS Payload Changed for Access Node; Defender RADIUS Payload Changed for Group; Defender RADIUS Payload Changed for Security Server; Defender RADIUS Payload Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload removed in last 30 days

Who = All Users

What = Defender RADIUS Payload Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server added in last 30 days

Who = All Users

What = Defender Security Server Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server assigned to access node in last 30 days

Who = All Users

What = Defender Security Server Assigned to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server removed in last 30 days

Who = All Users

What = Defender Security Server Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server unassigned from access node in last 30 days

Who = All Users

What = Defender Security Server Unassigned to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender temporary response events in last 30 days

Who = All Users

What = Defender Token Temporary Response Cleared; Defender Token Temporary Response Set; Defender Token Temporary Response Usage Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token added in last 30 days

Who = All Users

What = Defender Token Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token assigned in last 30 days

Who = All Users

What = Defender Token Assigned

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token PIN events in last 30 days

Who = All Users

What = Defender Token PIN Changed; Defender Token PIN Cleared; Defender Token PIN Expiry Cleared; Defender Token PIN Expiry Set; Defender Token PIN Set

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token removed in last 30 days

Who = All Users

What = Defender Token Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token unassigned in last 30 days

Who = All Users

What = Defender Token Unassigned

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Microsoft 365

### All Microsoft 365 events in the past 7 days

Who = All Users

What = Microsoft 365 events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

# Exchange Online

### All Microsoft 365 Exchange Online events in the past 7 days

Who = All Users

What = Microsoft 365 Exchange Online events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### Microsoft 365 Exchange Online administrative cmdlets executed this week

Who = All Users

What = Microsoft 365 Exchange Online administration events, external and local

Where = All sources

When = This week

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped); User (Grouped)

### Microsoft 365 Exchange Online events this week

Who = All Users

What = Microsoft 365 Exchange Online administration, mailbox owner and non-owner events

Where = All sources

When = This week

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### Microsoft 365 Exchange Online mailbox activity this week

Who = All Users

What = Microsoft 365 Exchange Online Mailbox facility

Where = All sources

When = This week

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped); User (Grouped)

### Microsoft 365 Exchange Online mailbox auditing configuration changed by an external application in the last 24 hours

Who = N/A

What = Microsoft 365 Exchange Online mailboxes that have had their auditing settings reconfigured in the last 24 hours

Where = All sources

When = Last 24 hours

Origin = N/A

Layout tab - Order By: Time Detected (Not Grouped)

### Microsoft 365 Exchange Online mailbox auditing configuration failures in the last 8 hours

Who = N/A

What = Microsoft 365 Exchange mailbox auditing configuration failure

Where = All sources

When = Last 8 hours

Origin = N/A

Layout tab - Order By: Time Detected (Not Grouped)

### Microsoft 365 Exchange Online mailbox login activity today

Who = All Users

What = Online mailbox login by owner event

Where = All sources

When = Today

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped); User (Grouped)

### Microsoft 365 Exchange Online mailbox non-owner activity this week

Who = All Users

What = All non-owner Microsoft 365 Exchange Online Mailbox facility events

Where = All sources

When = This week

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped); User (Grouped)

# OneDrive for Business

### All Microsoft 365 OneDrive for Business events in the past 7 days

Who = All Users

What = Microsoft 365 OneDrive for Business events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft 365 OneDrive for Business events in the past 7 days grouped by operation

Who = All Users

What = Microsoft 365 OneDrive for Business events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected; Grouped By: Microsoft Entra - Activity Name/Operation

### Microsoft 365 OneDrive for Business file activity events in the past 7 days

Who = All Users

What = Microsoft 365 OneDrive for Business file activity events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### Microsoft 365 OneDrive for Business folder activity events in the past 7 days

Who = All Users

What = Microsoft 365 OneDrive for Business folder activity events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

# SharePoint Online

### All Microsoft 365 SharePoint Online events in the past 7 days

Who = All Users

What = Microsoft 365 SharePoint Online events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### All Microsoft 365 SharePoint Online events in the past 7 days grouped by operation

Who = All Users

What = Microsoft 365 SharePoint Online events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected; Grouped By: Microsoft Entra - Activity Name/Operation

### Microsoft 365 SharePoint Online file activity events in the past 7 days

Who = All Users

What = Microsoft 365 SharePoint Online file activity events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

### Microsoft 365 SharePoint Online folder activity events in the past 7 days

Who = All Users

What = Microsoft 365 SharePoint Online folder activity events

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped)

# Logon Activity

**NOTE:** By default, Logon Activity reports include the Logon Type, Logon Start, Logon End, Logon Session Start, Logon Session End and Logon Duration columns on the Search Results page. These additional columns are defined using the Layout tab.

### All Kerberos service ticket events for unsafe encryption type in the last 7 days

Who = All Users

What = A Kerberos service ticket was created with an unsafe encryption type

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Failed Logons in the last 7 days

Who = All Users

What = User failed to authenticate through Kerberos, User failed to authenticate through NTLM, User failed to log on interactively, User failed to log on interactively from a remote computer, User failed to perform a network logon from a remote computer

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## All Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively; User logged on interactively

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## All Kerberos Authentication Activity in the past 24 hours

Who = All Users

What = User authenticated through Kerberos, User failed to authenticate through Kerberos

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## All Kerberos user ticket events that exceed the maximum ticket lifetime in the past 30 days

Who = All Users

What = Kerberos user ticket that exceeds the maximum ticket lifetime detected

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## All Logons by administrators in the past 24 hours

Who = Administrators

What = Authentication Activity; Domain Controller Authentication; Logon Session

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## All Logons in the past 24 hours

Who = All Users

What = Authentication Activity; Domain Controller Authentication; Logon Session

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## All NTLM Authentication Activity in the past 24 hours

Who = All Users

What = User authenticated through NTLM, User failed to authenticate through NTLM

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All NTLM version 1 logons in the last 7 days

Who = All Users

What = User performed a successful NTLM V1 logon

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Remote Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively from a remote computer; User failed to perform a network logon from a remote computer; User logged on interactively from a remote computer; User performed a successful network logon from a remote computer

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All User Sessions in the past 24 hours

Who = All Users

What = Logon Session facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

# Recommended Best Practices

The Recommended Best Practices reports are available under the following folders:

- Auditing Service Administrator Activity
- Domain Controller Changes
- Domain-Level Changes
- Exchange
- Forest-Level Changes
- Severity Based Changes
- SQL

# Auditing Service Administrator Activity

The Auditing Service Administration Activity reports are available under the following folders:

- Domain Wide Configuration Activity | Domain Admins
- Forest Changes by Activity
- Forest Wide Configuration Activity | Enterprise Admins
- Forest Wide Configuration Activity | Schema Admins
- Service Admins Group Membership

## Domain Wide Configuration Activity | Domain Admins

### All Domain changes performed in last 14 days

Search generated for each domain in forest:

Who = All Users

What = Domain Configuration facility; Configuration Monitoring facility

Where = Domain Controller

When = Last 14 days

Origin = All domain controllers

## Forest Changes by Activity

### All Replication Changes performed in last 30 days

Who = All Users

What = Replication Transport facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### All Schema Changes performed in last 30 days

Who = All Users

What = Schema Configuration facility

Schema FSMO Role Owner Moved; Schema Modifications Allowed Flag Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### All Site Changes performed in last 30 days

Who = All Users

What = Site Added; Site Removed; Site Renamed; Site Link Added; Site Link Removed; Site Link Bridge Added; Site Link Bridge Removed

Site Configuration facility; Site Link Bridge Configuration facility; Connection Object facility; Site Link Configuration facility; Subnets facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Forest Wide Configuration Activity | Enterprise Admins

### All Domain changes performed in last 14 days

Who = All Users

What = Domain Configuration facility; Configuration Monitoring facility

Where = Domain Controller

When = Last 14 days

Origin = All domain controllers

### All Forest changes performed in last 14 days

Who = All Users

What = Forest Configuration facility

Where = All sources

When = Last 14 days

Origin = All workstations/servers

### All Replication changes performed in last 14 days

Who = All Users

What = Replication Transport facility

Where = All sources

When = Last 14 days

Origin = All workstations/servers

### All Site changes performed in last 14 days

Who = All Users

What = Site Added; Site Removed; Site Renamed; Site Link Added; Site Link Removed; Site Link Bridge Added; Site Link Bridge Removed

Site Configuration facility; Site Link Bridge Configuration facility; Site Link Configuration facility; Connection Object facility; Subnets facility

Where = All sources

When = Last 14 days

Origin = All workstations/servers

## Forest Wide Configuration Activity | Schema Admins

### All Schema changes performed in last 14 days

Who = All Users

What = Schema Configuration facility

Schema FMSO Role Owner Moved; Schema Modifications Allowed Flag Changed

Where = All sources

When = Last 14 days

Origin = All workstations/servers

## Service Admins Group Membership

### Membership changed in critical groups in last 7 days

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Domain Controller Changes

### Changes in Domain Controller Services

Who = All Users

What = Service Monitoring facility

Where = Domain Controller

When = Last 7 days

Origin = All domain controllers

### Changes in Domain Controller System State, Registry and Configuration Files

Who = All Users

What = Custom File System Monitoring facility; Custom Registry Monitoring facility; System Events facility; Service Monitoring facility

Where = Domain Controller

When = Last 7 days

Origin = All domain controllers

# Domain-Level Changes

### Changes in domain-wide operations master roles

Who = All Users

What = RID FSMO Role Owner Moved; PDC FSMO Role Owner Moved; Infrastructure FSMO Role Owner Moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Changes in the GPO assignments

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU; Group Policy Disabled Setting on Domain Changed; Group Policy Disabled Setting on OU Changed; Group Policy Inheritance Blocked Setting Changed; on Domain; Group Policy Link Added to OU; Group Policy Link Removed from OU; Group Policy Link Settings Modified; Group Policy Linked; Group Policy No Override Setting Changed on Domain; Group Policy Unlinked; Group Policy No Override Setting Changed on OU

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Changes in the linked GPOs

Who = All Users

What = Linked Group Policy on Domain Changed; Linked Group Policy on OU Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Changes in the membership of built-in groups

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Changes in trust

Who = All Users

What = Cross-forest Trust Added; Cross-forest Trust Removed; Trust Added; Trust Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Changes to the audit policy settings

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Exchange

### Address List Added to the Organization Configuration

Who = All Users

What = Address List Added to Organization Configuration; Address List - Created; Address List - Moved; Address List - Recipient Container; Address List - Updated; Global Address List - Created; Global Address List - Recipient Container; Global Address List - Updated

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All ActiveSync Mailbox Policy Events

Who = All Users

What = ActiveSync Mailbox Policy Added to Organization Client Access Configuration; ActiveSync Mailbox Policy Allow Attachments to be Downloaded Option Changed; ActiveSync Mailbox Policy Allow Non-Provisionable Devices Options Changed; ActiveSync Mailbox Policy Allow Simple Password Option Changed; ActiveSync Mailbox Policy Enable Password Recovery Option Changed; ActiveSync Mailbox Policy Maximum Attachment Size Changed; ActiveSync Mailbox Policy Minimum Password Length Changed; ActiveSync Mailbox Policy Password Expiration Changed; ActiveSync Mailbox Policy Password History Changed; ActiveSync Mailbox Policy Password Required Option Changed; ActiveSync Mailbox Policy Removed from Organization Client Access Configuration; ActiveSync Mailbox Policy Renamed; ActiveSync Mailbox Policy Require Alphanumeric Password Option Changed; ActiveSync Mailbox Policy Require Encryption On Device Option Changed; ActiveSync Mailbox Policy User Idle Timeout Changed; ActiveSync Mailbox Policy Windows File Shares Access Option Changed; ActiveSync Mailbox Policy Windows SharePoint Services Access Option Changed; ActiveSync Mailbox Policy Number of Failed Attempts Allowed Changed; ActiveSync Mailbox Policy Refresh Interval Changed; ActiveSync Mailbox Policy Require Encryption On Device Option Changed; Mobile Device - ActiveSync Device Policy

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Email Address Policy Events

Who = All Users

What = Email Address Policy Added to Organization Configuration; Email Address Policy Email Address Filter List Changed; Email Address Policy Priority Changed; Email Address Policy Query Filter Changed;

Email Address Policy Removed from Organization Configuration; Email Address Policy Renamed; Email Address Policy Storage Filter Changed; Distribution List - Email Address Policy Enabled Changed; Mailbox - Email Address Policy Enabled Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Administrative Group Events

Who = All Users

What = Exchange Administrative Group facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Distribution List (Group) Events

Who = All Users

What = Exchange Distribution List facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Events in the last 24 hours

Who = All Users

What = Exchange subsystem

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Exchange Organization Events

Who = All Users

What = Exchange Organization facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Permission Tracking Events

Who = All Users

What = Exchange Permission Tracking facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Journaling Rule Change Events

Who = All Users

What = Journaling Rule Added to Organization Configuration; Journaling Rule Changed; Journaling Rule Removed from Organization Configuration; Journaling Rule Renamed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Send Connector Change Events

Who = All Users

What = Mutual Auth TLS Option Changed on Send Connector; Send Connector Added to Organization Configuration; Send Connector Protocol Logging Changed; Send Connector Removed from Organization Configuration; Send Connector Renamed; Send Connector Response FQDN Changed; Send Connector Status Changed; Address Space Added to Send Connector; Address Space Removed from Send Connection; External DNS Lookup Option Changed on Send Connector; Send Connector Maximum Message Size Changed; Smart Host Added to Send Connector; Smart Host Authentication Settings Changed on Send Connector; Smart Host Removed from Send Connector; Source Server Added to Send Connector; Source Server Removed from Send Connector

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Transport Rule Change Events

Who = All Users

What = Transport Rule Added to Organization Configuration; Transport Rule Changed; Transport Rule Priority Changed; Transport Rule Removed from Organization Configuration; Transport Rule Renamed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Unified Messaging (UM) Dial Plan Change Events

Who = All Users

What = Allow Announcement Interruption Option Changed in UM Dial Plan; Allow Callers To Send Voice Message Option Changed in UM Dial Plan; Allow Callers to Transfer Option Changed in UM Dial Plan; Allow Faxes Option Changed in UM Dial Plan; Announcement Changed in UM Dial Plan; Audio Codec Changed in UM Dial Plan; Callers Can Contact Address List Changed in UM Dial Plan; Callers Can Contact Auto Attendant Changed in UM Dial Plan; Callers Can Contact Extension Changed in UM Dial Plan; Callers Can Contact Option Changed in UM Dial Plan; Country Code Changed in UM Dial Plan; Default Language Changed in UM Dial Plan; Greeting Changed in UM Dial Plan; In-Country Number Format Changed in UM Dial Plan; In-Country Rule Group Added to UM Dial Plan; In-Country Rule Group Removed From UM Dial Plan; Input Failures Before Disconnect Changed in UM Dial Plan; Input Idle Timeout Changed in UM Dial Plan; Input Retries Changed in UM Dial Plan; International Access Code Changed in UM Dial Plan; International Number Format Changed in UM Dial Plan; International Rule Group Added to UM Dial Plan; International Rule Group Removed from UM Dial Plan; Logon Failure Count Changed in UM Dial Plan; Maximum Call Duration Changed in UM Dial Plan; Maximum Recording Duration Changed in UM Dial Plan; Name Match Option Changed in UM Dial Plan; National Number Prefix Changed in UM Dial Plan; Non-Delivery Report Option Changed in UM Dial Plan; Operator Extension Changed in UM Dial Plan; Outside Line Access Code Changed in UM Dial Plan; Primary Dialing Methods Changed in UM Dial Plan; Prompt Publishing Point Changed for UM Dial Plan; Recording Idle Timeout Changed in UM Dial Plan; Secondary Dialing Method Changed in UM Dial Plan; Subscriber Access Number Added to UM Dial Plan; Subscriber Access Number Removed from UM Dial Plan; UM Dial Plan

Added to Organization Configuration; UM Dial Plan Removed from Organization Configuration; UM Dial Plan Renamed; UM Dial Plan - Access Telephone Numbers; UM Dial Plan - Allow Calling Line ID Resolution via Active Directory; UM Dial Plan - Allow Calls to Extensions; UM Dial Plan - Allow Calls to Users Within Same Dial Plan; UM Dial Plan - Allowed In-Country/Region Rule Groups; UM Dial Plan - Allowed International Rule Groups; UM Dial Plan - Audio Codec; UM Dial Plan - Automatic Speech Recognition Enabled/Disabled; UM Dial Plan - Call Answering Rules Enabled/Disabled; UM Dial Plan - Callers Can Contact; UM Dial Plan - Callers Can Contact Address List; UM Dial Plan - Callers Can Contact Auto Attendant; UM Dial Plan - Callers Can Contact Extension; UM Dial Plan - Callers Can Contact Recipient List; UM Dial Plan - Country/Region Code; UM Dial Plan - Created; UM Dial Plan - Default Language; UM Dial Plan - Default Outbound Calling Line ID; UM Dial Plan - Dial By Name Primary Method; UM Dial Plan - Dial By Name Secondary Method; UM Dial Plan - Equivalent Dial Plans; UM Dial Plan - Fax Enabled/Disabled; UM Dial Plan - In-Country/Region Number Format; UM Dial Plan - In-Country/Region Rule Groups; UM Dial Plan - Informational Announcement; UM Dial Plan - Informational Announcement File; UM Dial Plan - Input Failures Before Disconnect; UM Dial Plan - International Access Code; UM Dial Plan - International Number Format; UM Dial Plan - International Rule Groups; UM Dial Plan - Legacy Prompt Publishing Point; UM Dial Plan - Logon Failures Before Disconnect; UM Dial Plan - Matched Name Selection Method; UM Dial Plan - Maximum Call Duration; UM Dial Plan - Maximum Recording Duration; UM Dial Plan - National Number Prefix; UM Dial Plan - Numbering Plan Formats; UM Dial Plan - Operator Extension; UM Dial Plan - Outside Line Access Code; UM Dial Plan - Pilot Numbers; UM Dial Plan - Recording Idle Time-out; UM Dial Plan - Removed; UM Dial Plan - Send Voice Messages Enabled/Disabled; UM Dial Plan - Telephone User Interface Prompt Editing; UM Dial Plan - Transfer to Users Enabled/Disabled; UM Dial Plan - VOIP Security; UM Dial Plan - Welcome Greeting; UM Dial Plan - Welcome Greeting Filename

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Unified Messaging (UM) Policy Change Events

Who = All Users

What = Allow Calls to Extensions Option Changed in UM Mailbox Policy; Allow Calls to Same-Plan Users Option Changed in UM Mailbox Policy; Allow Common PIN Pattern Option Changed in UM Mailbox Policy; Fax Identity Changed in UM Mailbox Policy; Fax Message Text Changed in UM Mailbox Policy; Incorrect PIN Mailbox Lockout Setting Changed in UM Mailbox Policy; Incorrect PIN Reset Setting Changed in UM Mailbox Policy; In-Country Rule Group Added to UM Mailbox Policy; In-Country Rule Group Removed From UM Mailbox Policy; International Rule Group Added to UM Mailbox Policy; International Rule Group Removed from UM Mailbox Policy; Mailbox Enabled Text Changed in UM Mailbox Policy; Maximum Greeting Duration Changed in UM Mailbox Policy; Maximum Greeting Duration Enabled Option Changed in UM Mailbox Policy; Minimum PIN Length Changed in UM Mailbox Policy; PIN History Length Changed in UM Mailbox Policy; PIN Lifetime Changed in UM Mailbox Policy; PIN Reset Text Changed in UM Mailbox Policy; UM Mailbox Policy Added to Organization Configuration; UM Mailbox Policy Removed from Organization Configuration; UM Mailbox Policy Renamed; Voice Message Text Changed in UM Mailbox Policy

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Deleted Items Retention Period Changed for a user

Who = All Users

What = Deleted Item Retention Period Changed; Deleted Item Retention Use Defaults Storage Option Changed; Mailbox - End Date Retention Hold; Mailbox - Retention Hold Enabled; Mailbox - Retention Policy; Mailbox - Start Date for Retention Hold; Mailbox - Use Database Retention Defaults

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Exchange Database Location Changed for Mailbox Store

Who = All Users

What = Exchange Database Location Changed for Mailbox Store

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Exchange Database Location Changed for Public Store

Who = All Users

What = Exchange Database Location Changed for Public Store

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Mail Enabled for Group

Who = All Users

What = Mail Enabled for Group (Exchange 2003); Distribution List - Created; Distribution List - Enabled

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Mailbox Store Dismounted

Who = All Users

What = Mailbox Store Dismounted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Mailbox Store Mounted

Who = All Users

What = Mailbox Store Mounted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Message Tracking Options Changed on an Exchange 2007 Server

Who = All Users

What = Message Tracking Option Changed on Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Outlook Anywhere Enabled or Disabled for a Server

Who = All Users

What = Outlook Anywhere Disabled for Server; Outlook Anywhere Enabled for Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### OWA Website Added to Server

Who = All Users

What = OWA Web Site Added to Server; OWA Web Site - Created

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### OWA Website Removed from the Server

Who = All Users

What = OWA Web Site Removed from Server; OWA Web Site - Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### OWA Website Renamed

Who = All Users

What = OWA Web Site Renamed on Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Public Folder Created

Who = All Users

What = Public Folder Store Created in Server Storage Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Public Folder Removed

Who = All Users

What = Public Folder Store Removed from Server Storage Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Public Folder Renamed

Who = All Users

What = Public Folder Store Renamed in Server Storage Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Public Store Dismounted

Who = All Users

What = Public Store Dismounted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Public Store Mounted

Who = All Users

What = Public Store Mounted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Storage Group Added to Exchange Server

Who = All Users

What = Storage Group Added to Exchange Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Storage Group Removed from Exchange Server

Who = All Users

What = Storage Group Removed from Exchange Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Storage Group Renamed in Exchange Server

Who = All Users

What = Storage Group Renamed in Exchange Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Forest-Level Changes

### Changes in forest-wide operations master roles

Who = All Users

What = Domain FSMO Role Owner Moved; Schema FSMO Role Owner Moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Changes in LDAP policies

Who = All Users

What = Default Site Query Policy Object Changed; Linked Query Policy Object for Domain Controller Changed; Linked Query Policy for Site Changed; Query Policy Added; Query Policy Link for Domain Controller Changed; Query Policy Removed; Query Policy Setting Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Changes in replication topology

Who = All Users

What = Replication Transport facility; Site Configuration facility; Site Link Bridge Configuration facility; Site Link Configuration facility; Subnets facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Changes in the GPO assignments for all Sites

Who = All Users

What = Group Policy Link Added to Site; Group Policy Link Removed from Site; Group Policy Block Inheritance Setting Changed on Site; Group Policy No Override Setting Changed on Site; Group Policy Disabled Setting on Site Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Changes in the GPOs linked to all Sites

Who = All Users

What = Linked Group Policy on Site Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Promotion or demotion of domain controllers

Who = All Users

What = Domain Controller Added to Domain; Domain Controller Removed from Domain; Domain Controller Renamed; GC Added; GC Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Schema Changes

Who = All Users

What = Schema Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Severity Based Changes

### High Severity changes in last 30 days

Who = All Users

What = Severity | High

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Low Severity changes in last 30 days

Who = All Users

What = Severity | Low

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Medium Severity changes in last 30 days

Who = All Users

What = Severity | Medium

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# SQL

### All SQL Add Roles, User, and Login Events in the last 24 hours

Who = All Users

What = Audit Add DB User; Audit Add Login; Audit Add Login to Server Role; Audit Add Member to DB Role; Audit Add Role

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Broker Events in the last 24 hours

Who = All Users

What = SQL Broker Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL CLR Events in the last 24 hours

Who = All Users

What = SQL CLR Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Cursors Events in the last 24 hours

Who = All Users

What = SQL Cursors Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Database Events in the last 24 hours

Who = All Users

What = SQL Database Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Deprecation Events in the last 24 hours

Who = All Users

What = SQL Deprecation Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Errors and Warning Events in the last 24 hours

Who = All Users

What = SQL Errors and Warnings Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Events

Who = All Users

What = SQL subsystem

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Events in the last 24 hours

Who = All Users

What = SQL subsystem

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Full Text Events in the last 24 hours

Who = All Users

What = SQL Full Text Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Internal Auditing Events in the last 24 hours

Who = All Users

What = Auditing Disabled for SQL Instance; Auditing Enabled for SQL Instance; SQL Auditing Template Added; SQL Auditing Template Added to Agent Configuration; SQL Auditing Template Changed; SQL Auditing Template Disabled; SQL Auditing Template Enabled; SQL Auditing Template Removed; SQL Auditing Template Removed from Agent Configuration; SQL Instance Added; SQL Instance Changed; SQL Instance Removed; SQL Reporting Services Template Added; SQL Reporting Services Template Changed; SQL Reporting Services Template Disabled; SQL Reporting Services Template Enabled; SQL Reporting Services Template Removed

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Lock Events in the last 24 hours

Who = All Users

What = SQL Locks Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Objects Events in the last 24 hours

Who = All Users

What = SQL Objects Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL OLEDB Events in the last 24 hours

Who = All Users

What = SQL OLEDB Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Performance Events in the last 24 hours

Who = All Users

What = SQL Performance Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Progress Report Events in the last 24 hours

Who = All Users

What = SQL Progress Report Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Query Notification Events in the last 24 hours

Who = All Users

What = SQL Query Notifications Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Scan Events in the last 24 hours

Who = All Users

What = SQL Scans Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Security Audit Events in the last 24 hours

Who = All Users

What = SQL Security Audit Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Server Events in the last 24 hours

Who = All Users

What = SQL Server Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Session Events in the last 24 hours

Who = All Users

What = SQL Session Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Stored Procedures Events in the last 24 hours

Who = All Users

What = SQL Stored Procedures Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Transaction Events in the last 24 hours

Who = All Users

What = SQL Transactions Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL TSQL Events in the last 24 hours

Who = All Users

What = SQL TSQL Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL User-Configuration Events in the last 24 hours

Who = All Users

What = SQL User-Configurable Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### Audit Access DB Object Changed

Who = All Users

What = Audit Access Database Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add DB User

Who = All Users

What = Audit Add DB User

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Login

Who = All Users

What = Audit Add Login

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Login to Server Role

Who = All Users

What = Audit Add Login to Server Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Member to DB Role

Who = All Users

What = Audit Add Member to DB Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Role

Who = All Users

What = Audit Add Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Database

Who = All Users

What = Audit Alter Database

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Database Object

Who = All Users

What = Audit Alter Database Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Database Principal

Who = All Users

What = Audit Alter Database Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Object Derived Permission

Who = All Users

What = Audit Alter Object Derived Permission

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Schema Object

Who = All Users

What = Audit Alter Schema Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Object

Who = All Users

What = Audit Alter Server Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Principal

Who = All Users

What = Audit Alter Server Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Drop Database

Who = All Users

What = Audit Drop Database

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Drop DB User

Who = All Users

What = Audit Drop DB User

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Data File Auto Grow Changed

Who = All Users

What = Data File Auto Grow

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Database Mirroring State Changed

Who = All Users

What = Database Mirroring State Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Full Text Crawl Aborted

Who = All Users

What = FT: Crawl Aborted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Full Text Crawl Started

Who = All Users

What = FT: Crawl Started

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Full Text Crawl Stopped

Who = All Users

What = FT: Crawl Stopped

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### SQL Data File Auto Shrink Changed

Who = All Users

What = Data File Auto Shrink

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### SQL Error Logged

Who = All Users

What = Error Logged

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### SQL Event Logged

Who = All Users

What = Event Logged

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### SQL Lock Canceled

Who = All Users

What = Lock: Cancel

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### SQL Lock Released

Who = All Users

What = Lock: Released

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### SQL Locked Acquire

Who = All Users

What = Lock: Acquired

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### SQL Transaction Begin

Who = All Users

What = SQL Transaction Begin

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### SQL Transaction Commit

Who = All Users

What = SQL Transaction Commit

Where = All sources

When = Last 7 days

Origin = All workstations/servers

**SQL Transaction Rollback**

Who = All Users

What = SQL Transaction Rollback

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Regulatory Compliance

The Regulatory Compliance reports are available under the following folders:

- FISMA (Federal Information Security Management Act)
- GLBA (Gramm-Leach-Bliley Act)
- GDPR
- HIPAA (Health Insurance Portability and Accountability Act)
- Payment Card Industry
- SAS 70 (Statement on Auditing Standards, Service Organizations)
- SOX (Sarbanes-Oxley General IT Controls Evidence based on the COBIT Framework)

# FISMA (Federal Information Security Management Act)

The FISMA reports are available under the following folders:

- NIST SP 800-53 | Technical Controls | Accountability (Including Audit Trails) | A01 – User Association
- NIST SP 800-53 | Technical Controls | Accountability (Including Audit Trails) | A02 – Content of Audit Records
- NIST SP 800-53 | Technical Controls | Accountability (Including Audit Trails) | A03 – Auditable Events
- NIST SP 800-53 | Technical Controls | Accountability (Including Audit Trails) | A04 – Audit Processing
- NIST SP 800-53 | Technical Controls | Identification and Authentication | IA02 – Remote, Privileged Access Authentication
- NIST SP 800-53 | Technical Controls | Identification and Authentication | IA03 – Password Protection Mechanisms
- NIST SP 800-53 | Technical Controls | Identification and Authentication | IA04 – Password Life
- NIST SP 800-53 | Technical Controls | Identification and Authentication | IA05 – Password Content
- NIST SP 800-53 | Technical Controls | Identification and Authentication | IA12 – Remote Access Identification Authentication
- NIST SP 800-53 | Technical Controls | Identification and Authentication | IA16 – Password Management
- NIST SP 800-53 | Technical Controls | Logical Access Control | AC01 - Remote Access Restrictions
- NIST SP 800-53 | Technical Controls | Logical Access Control | AC02 - Logon Notification Message
- NIST SP 800-53 | Technical Controls | Logical Access Control | AC05 - Session Inactivity
- NIST SP 800-53 | Technical Controls | Logical Access Control | AC06 - Limited Connection Time

- NIST SP 800-53 | Technical Controls | Logical Access Control | AC09 - Enforcement Mechanisms
- NIST SP 800-53 | Technical Controls | Logical Access Control | AC10 - Automated Account Controls
- NIST SP 800-53 | Technical Controls | Logical Access Control | AC12 - Supervision and Review
- NIST SP 800-53 | Technical Controls | Logical Access Control | AC14 - Authorization Procedures
- NIST SP 800-53 | Technical Controls | System and Communications Protection | SP02 - Information System Partitioning
- NIST SP 800-53 | Technical Controls | System and Communications Protection | SP04 - Denial of Service Protection
- NIST SP 800-53 | Technical Controls | System and Communications Protection | SP05 - Resource Priority
- NIST SP 800-53 | Technical Controls | System and Communications Protection | SP06 - Boundary Protection
- NIST SP 800-53 | Technical Controls | System and Communications Protection | SP07 - Network Segregation
- NIST SP 800-53 | Technical Controls | System and Communications Protection | SP09 - Network Disconnect
- NIST SP 800-53 | Technical Controls | System and Communications Protection | SP11 - Trust Path
- NIST SP 800-53 | Technical Controls | System and Communications Protection | SP16 - Use of Encryption

## NIST SP 800-53 | Technical Controls | Accountability (Including Audit Trails) | A01 – User Association

### (Executive Summary) A01-User Associations

A summary report containing events from all of the following reports.

### A01 – Detailed list of audit policy modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit: Audit the Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### A01 – Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled; Change Auditor Agent Connected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### A01- Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit The Access of Global System Objects Policy Changed; Audit: Audit The Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## NIST SP 800-53 | Technical Controls | Accountability (Including Audit Trails) | A02 – Content of Audit Records

### (Executive Summary) A02-Content of Audit Records

A summary report containing events from all of the following reports.

### A02 – Detailed list of audit policy modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit: Audit the Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### A02 – Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit The Access of Global System Objects Policy Changed; Audit: Audit The Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Accountability (Including Audit Trails) | A03 – Auditable Events

### (Executive Summary) A03 - Auditable Events

A summary report containing events from all of the following reports.

### A03 – Detailed list of audit policy modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit: Audit the Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### A03 – Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled; Change Auditor Agent Connected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Accountability (Including Audit Trails) | A04 – Audit Processing

### (Executive Summary) A04 - Audit Processing

A summary report containing events from all of the following reports.

### A04 – Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled; Change Auditor Agent Connected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Identification and Authentication | IA02 – Remote, Privileged Access Authentication

### IA02 – Detailed list of dial-in modifications

Who = All Users

What = User Dial-in Static Route Added; User Dial-in Static Route Removed; User Dial-in Callback Options Changed; User Dial-in Static IP Address Changed; User Dial-in Remote Access Permission Changed; User Dial-in Verify Caller ID Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Identification and Authentication | IA03 – Password Protection Mechanisms

### (Executive Summary) IA03 - Password Protection Mechanisms

A summary report containing events from all of the following reports.

### IA03 – Detailed list of account lockout policy modifications

Who = All Users

What = Account Lockout Threshold Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA03 – Detailed list of lockout duration policy modifications

Who = All Users

What = Account Lockout Duration Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA03 – Detailed list of password age policy modifications

Who = All Users

What = Maximum Password Age Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA03 – Detailed list of password complexity policy modifications

Who = All Users

What = Password Must Meet Complexity Requirements Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA03 – Detailed list of password history policy modifications

Who = All Users

What = Enforce Password History Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA03 – Detailed list of storing password policy modifications

## NIST SP 800-53 | Technical Controls | Identification and Authentication | IA04 – Password Life

### IA04 – Detailed list of password age policy modifications

Who = All Users

What = Minimum Password Age Policy Changed; Maximum Password Age Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## NIST SP 800-53 | Technical Controls | Identification and Authentication | IA05 – Password Content

### (Executive Summary) IA05 - Password Content

A summary report containing events from all of the following reports.

### IA05 – Detailed list of password complexity policy modifications

Who = All Users

What = Password Must Meet Complexity Requirements Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA05 – Detailed list of password history policy modifications

Who = All Users

What = Enforce Password History Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Identification and Authentication | IA12 – Remote Access Identification Authentication

### IA12 – Detailed list of dial-in modifications

Who = All Users

What = User Dial-in Static Route Added; User Dial-in Static Route Removed; User Dial-in Callback Options Changed; User Dial-in Static IP Address Changed; User Dial-in Remote Access Permission Changed; User Dial-in Verify Caller ID Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Identification and Authentication | IA16 – Password Management

### (Executive Summary) IA016 - Password Management

A summary report containing events from all of the following reports.

### IA16 – Detailed list of account lockout policy modifications

Who = All Users

What = Account Lockout Threshold Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA16 – Detailed list of lockout duration policy modifications

Who = All Users

What = Account Lockout Duration Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA16 – Detailed list of password age policy modifications

Who = All Users

What = Minimum Password Age Policy Changed; Maximum Password Age Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA16 – Detailed list of password complexity policy modifications

Who = All Users

What = Password Must Meet Complexity Requirements Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA16 – Detailed list of password history policy modifications

Who = All Users

What = Enforce Password History Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### IA16 – Detailed list of storing passwords policy modifications

Who = All Users

What = Store Passwords Using Reversible Encryption Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## NIST SP 800-53 | Technical Controls | Logical Access Control | AC01 - Remote Access Restrictions

### AC01 – Detailed list of dial-in modifications

Who = All Users

What = User Dial-in Static Route Added; User Dial-in Static Route Removed; User Dial-in Callback Options Changed; User Dial-in Static IP Address Changed; User Dial-in Remote Access Permission Changed; User Dial-in Verify Caller ID Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## NIST SP 800-53 | Technical Controls | Logical Access Control | AC02 - Logon Notification Message

### AC02 – Detailed list of interactive login policy modifications

Who = All Users

What = Interactive Logon: Message Title for Users Attempting to Log On Changed; Interactive Logon: Do Not Require CTRL+ALT+DEL Policy Changed; Interactive Logon: Message Text for Users Attempting to Log On Policy Changed; Interactive Logon: Do Not Display Last User Name Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Logical Access Control | AC05 - Session Inactivity

### (Executive Summary) AC05 - Session Inactivity

A summary report containing events from all of the following reports.

### AC05 – Detailed list of idle time policy modifications

Who = All Users

What = Microsoft Network Server: Amount of Idle Time Required Before Suspending Session Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### AC05 – Detailed list of time expires policy modifications

Who = All Users

What = Network Security: Force Logoff When Logon Hours Expire Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Logical Access Control | AC06 - Limited Connection Time

### AC06 – Detailed list of logon time policy modifications

Who = All Users

What = User logonHours Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Logical Access Control | AC09 - Enforcement Mechanisms

### AC09 – Detailed list of user logon restrictions policy modifications

Who = All Users

What = Enforce User Logon Restrictions Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Logical Access Control | AC10 - Automated Account Controls

### (Executive Summary) AC10 - Automated Account Controls

A summary report containing events from all of the following reports.

### AC10 – Detailed list of account expires modifications

Who = All Users

What = User accountExpires Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### AC10 – Detailed list of workstation restrictions

Who = All Users

What = User userWorkstations Added; User userWorkstations Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Logical Access Control | AC12 - Supervision and Review

### AC12 – Detailed list of rename administrator and guest policy modifications

Who = All Users

What = Accounts: Rename Guest Account Policy Changed; Accounts: Rename Administrator Account Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | Logical Access Control | AC14 - Authorization Procedures

### AC14 – Detailed list of enforce logon policy modifications

Who = All Users

What = Enforce User Logon Restrictions Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | System and Communications Protection | SP02 - Information System Partitioning

### SP02 – Detailed list of trust policy modifications

Who = All Users

What = Cross-forest Trust Removed; Cross-forest Trust Added; Trust Removed; Trust Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | System and Communications Protection | SP04 - Denial of Service Protection

### (Executive Summary) SP04 - Denial of Service Protection

A summary report containing events from all of the following reports.

### SP04 – Detailed list of global catalog modifications

Who = All Users

What = GC Removed; GC Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### SP04 – Detailed list of NETLOGON service modifications

Who = All Users

What = NETLOGON Service facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | System and Communications Protection | SP05 - Resource Priority

### SP05 – Detailed list of high severity changes

Who = All Users

What = High severity

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | System and Communications Protection | SP06 - Boundary Protection

### SP06 – Detailed list of trust modifications

Who = All Users

What = Cross-forest Trust Removed; Cross-forest Trust Added; Trust Removed; Trust Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | System and Communications Protection | SP07 - Network Segregation

### SP07 – Detailed list of IP Security and Configuration modifications

Who = All Users

What = IP Security facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | System and Communications Protection | SP09 - Network Disconnect

### SP09 – Detailed list of forced logout policy modifications

Who = All Users

What = Microsoft Network Server: Amount of Idle Time Required Before Suspending Sessions Policy Changed; Network Security: Force Logoff When Logon Hours Expire Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# NIST SP 800-53 | Technical Controls | System and Communications Protection | SP11 - Trust Path

### SP11 – Detailed list of trust modifications

Who = All Users

What = Cross-forest Trust Removed; Cross-forest Trust Added; Trust Removed; Trust Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## NIST SP 800-53 | Technical Controls | System and Communications Protection | SP16 - Use of Encryption

### SP16 – Detailed list of public key modifications

Who = All Users

What = Computer Public Key Policies Autoenrollment Settings Changed; Computer Public Key Policies Automatic Certificate Request Added; Computer Public Key Policies Automatic Certificate Request Removed; Computer Public Key Policies Encrypting File System DRA Added; Computer Public Key Policies Encrypting File System DRA Changed; Computer Public Key Policies Encrypting File System DRA Removed; Computer Public Key Policies Enterprise Trust List Added; Computer Public Key Policies Enterprise Trust List Changed; Computer Public Key Policies Enterprise Trust List Removed; Computer Public Key Policies Trusted Root Certification Authority Added; Computer Public Key Policies Trusted Root Certification Authority Changed; Computer Public Key Policies Trusted Root Certification Authority Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# GLBA (Gramm-Leach-Bliley Act)

The GLBA reports are available under the following folders:

- 6801 – Protection of Non Public Personal Information | 6801(a) – Privacy Obligation Policy
- 6805 – Enforcement | 6805(b) – Enforcement of Section 6801

## 6801 – Protection of Non Public Personal Information | 6801(a) – Privacy Obligation Policy

### (Executive Summary) - 6801(a) Formal Mechanisms for Processing Records

A summary report containing events from all of the following reports.

### 6801(a) – Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled; Change Auditor Agent Connected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6801(a) – Detailed list of critical group membership modifications

Who = All Users

What = Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group; Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6801(a) – Detailed list of file system permission modifications

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed; Local Share Permissions Changed; SYSVOL Folder Access Rights Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6801(a) – Detailed list of GPO modifications

Who = All Users

What = Group Policy Item facility; Group Policy Object facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6801(a) – Detailed list of interactive login policy modifications

Who = All Users

What = Interactive Logon: Message Title for Users Attempting to Log On Changed; Interactive Logon: Do Not Require CTRL+ALT+DEL Policy Changed; Interactive Logon: Message Text for Users Attempting to Log On Policy Changed; Interactive Logon: Do Not Display Last User Name Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6801(a) – Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit: Audit the Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audit Policy Changed; Security Audit Log Rolled Over; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down The Computer When The Security Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6801(a) – Detailed list of share modifications

Who = All Users

What = Active Directory Shared Added; Active Directory Shared Removed; Local Share Added; Local Share Folder Path Changed; Local Share Permissions Changed; Local Share Removed; SYSVOL Folder Access Rights Changed; SYSVOL Folder Auditing Changed; SYSVOL Folder Ownership Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# 6805 – Enforcement | 6805(b) – Enforcement of Section 6801

### (Executive Summary) - 6805(b) Enforcement of Section 6801

A summary report containing events from all of the following reports.

### 6805(b) – Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled; Change Auditor Agent Connected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6805(b) – Detailed list of Change Auditor Internal Controls modifications

Who = All Users

What = Change Auditor Internal Auditing facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6805(b) – Detailed list of critical group membership modifications

Who = All Users

What = Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group; Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6805(b) – Detailed list of file system permission modifications

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed; Local Share Permissions Changed; SYSVOL Folder Access Rights Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6805(b) – Detailed list of GPO modifications

Who = All Users

What = Group Policy Item facility; Group Policy Object facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6805(b) – Detailed list of interactive login policy modifications

Who = All Users

What = Interactive Logon: Message Title for Users Attempting to Log On Changed; Interactive Logon: Do Not Require CTRL+ALT+DEL Policy Changed; Interactive Logon: Message Text for Users Attempting to Log On Policy Changed; Interactive Logon: Do Not Display Last User Name Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 6805(b) – Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit: Audit Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audit Policy Changed; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down The Computer When The Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# GDPR

- Audit and Accountability
- Integrity and Confidentiality
- Responsibility of the Controller
- Security of Processing

## Audit and Accountability

- Active Directory
- Active Directory\Computers
- Active Directory\Configuration
- Active Directory\GPO Configuration
- Active Directory\Group Policy
- Active Directory\Organizational Unit
- Active Directory\Users and Groups
- Authentication Services
- Messaging\Exchange

- Messaging\Exchange Online
- Microsoft SQL\Audit
- Windows

## Active Directory

### - All Account Lockout Events

Who = All Users

What = Local User Account Locked; Local User Account Unlocked; User Account Locked; User Account Unlocked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - All Object Restore Events

Who = All Users

What = Computer Added; Domain Added; Exchange Group Added (Exchange 2003); Group Object Added; Group Policy Object Added; Subordinate OU Added; User Object Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - All OU Events

Who = All Users

What = OU facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - Changes to User Profiles in the last 30 days

Who = All Users

What = Home Folder Changed on User Object; Home Folder Mapped Drive Changed on User Object; Level of Control Changed for User Object; Primary Group ID Changed for User Object; Profile Path Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - GDPR - Active Directory Database Events in last 30 days

Who = All Users

What = Active Directory Database facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Active Directory\Computers

### - Computers added in last 30 days

Who = All Users

What = Computer Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Computers disabled in last 30 days

Who = All Users

What = Computer Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Computers enabled in last 30 days

Who = All Users

What = Computer Account Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Computers moved in last 30 days

Who = All Users

What = Computer Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Computers removed in last 30 days

Who = All Users

What = Computer Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Computers renamed in last 30 days

Who = All Users

What = Computer Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Computers with a Service Pack applied in last 30 days

Who = All Users

What = Computer Service Pack Applied

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Computers with a Service Pack rolled back in last 30 days

Who = All Users

What = Computer Service Pack Rolled Back

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Active Directory\Configuration

### - All Basic Domain Controller changes in last 30 days

Who = All Users

What = Append Parent Suffixes Option Changed; Connection DNS Registration Option Changed; Connection-Specific DNS Suffixes Changed; Contents of DNS Server List Changed; Contents of DNS Suffix List Changed; Default Gateway Changed; DHCP Enabled; DHCP Disabled; Disk Size Changed; IP Deny List Entry Added; IP Deny List Entry Removed; IPSEC Settings Changed; Memory Amount Changed; NIC Added; NIC Removed; Processor Speed Changed; Raw IP Allowed Protocols List Changed; Static IP Address Changed; Subnet Mask Changed; Use Connection Suffix in DNS Registration Option Changed; Use of Dynamic DNS Changed; Use Primary and Connection Specific Suffixes Flag Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - All Forest changes performed in last 14 days

Who = All Users

What = Forest Configuration facility

Where = All sources

When = Last 14 days

Origin = All workstations/servers

### - All Domain changes performed in last 14 days

Search generated for each domain in forest:

Who = All Users

What = Domain Configuration facility; Configuration Monitoring facility

Where = Domain Controller

When = Last 14 days

Origin = All domain controllers

### - All Replication Changes performed in last 30 days

Who = All Users

What = Replication Transport facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - All Schema Changes performed in last 30 days

Who = All Users

What = Schema Configuration facility

Schema FSMO Role Owner Moved; Schema Modifications Allowed Flag Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - All Site Changes performed in last 30 days

Who = All Users

What = Site Added; Site Removed; Site Renamed; Site Link Added; Site Link Removed; Site Link Bridge Added; Site Link Bridge Removed

Site Configuration facility; Site Link Bridge Configuration facility; Connection Object facility; Site Link Configuration facility; Subnets facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Allow raw IP allowed protocols list changed in last 30 days

Who = All Users

What = Raw IP Allowed Protocols List Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - Changes in Domain Controller Services

Who = All Users

What = Service Monitoring facility

Where = Domain Controller

When = Last 7 days

Origin = All domain controllers

### - Changes in Domain Controller System State, Registry and Configuration Files

Who = All Users

What = Custom File System Monitoring facility; Custom Registry Monitoring facility; System Events facility; Service Monitoring facility

Where = Domain Controller

When = Last 7 days

Origin = All domain controllers

### - Changes in domain-wide operations master roles

Who = All Users

What = RID FSMO Role Owner Moved; PDC FSMO Role Owner Moved; Infrastructure FSMO Role Owner Moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - Changes in forest-wide operations master roles

Who = All Users

What = Domain FSMO Role Owner Moved; Schema FSMO Role Owner Moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - Changes in LDAP policies

Who = All Users

What = Default Site Query Policy Object Changed; Linked Query Policy Object for Domain Controller Changed; Linked Query Policy for Site Changed; Query Policy Added; Query Policy Link for Domain Controller Changed; Query Policy Removed; Query Policy Setting Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - Changes to audit policy settings

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - Changes to DNS settings in last 30 days

Who = All Users

What = DHCP Enabled; DHCP Disabled; Static IP Address Changed; Subnet Mask Changed; Default Gateway Changed; Contents of DNS Server List Changed; Use Primary and Connection Specific Suffixes Flag Changed; Append Parent Suffixes Option Changed; Connection Specific DNS Suffix Changed; Contents of DNS Suffix List Changed; Use Connection Suffix in DNS Registration Option Changed; Connection DNS Registration Option Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - Default gateway changes in last 30 days

Who = All Users

What = Default Gateway Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - DHCP disabled in last 30 days

Who = All Users

What = DHCP Disabled

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - DHCP enabled in last 30 days

Who = All Users

What = DHCP Enabled

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - Domain Controller moved in the last 30 days

Who = All Users

What = Domain Controller Moved to Another OU

Where = All sources

When = Last 30 days

Origin = All domain controllers

### - Global Catalog added to Domain Controller in last 30 days

Who = All Users

What = GC Added

Where = All sources

When = Last 30 days

Origin = All domain controllers

### - Global Catalog removed from Domain Controller in last 30 days

Who = All Users

What = GC Removed

Where = All sources

When = Last 30 days

Origin = All domain controllers

### - Hot fixes applied in last 30 days

Who = All Users

What = Hotfix Applied

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - Hot fixes rolled back in last 30 days

Who = All Users

What = Hotfix Rolled Back

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - Medium Severity changes in the last 30 days

Who = All Users

What = Severity | Medium

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Promotion or demotion of Domain Controllers

Who = All Users

What = Domain Controller Added to Domain; Domain Controller Removed from Domain; Domain Controller Renamed; GC Added; GC Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - All Basic Domain Controller changes in last 30 days

Who = All Users

What = Append Parent Suffixes Option Changed; Connection DNS Registration Option Changed; Connection-Specific DNS Suffixes Changed; Contents of DNS Server List Changed; Contents of DNS Suffix List Changed; Default Gateway Changed; DHCP Enabled; DHCP Disabled; Disk Size Changed; IP Deny List Entry Added; IP Deny List Entry Removed; IPSEC Settings Changed; Memory Amount Changed; NIC Added; NIC Removed; Processor Speed Changed; Raw IP Allowed Protocols List Changed; Static IP Address Changed; Subnet Mask Changed; Use Connection Suffix in DNS Registration Option Changed; Use of Dynamic DNS Changed; Use Primary and Connection Specific Suffixes Flag Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - Schema Changes

Who = All Users

What = Schema Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - Service Packs rolled back in last 30 days

Who = All Users

What = Domain Controller Service Pack Rolled Back

Where = All sources

When = Last 30 days

Origin = All domain controllers

### - Static IP address changes in last 30 days

Who = All Users

What = Static IP Address Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### - TCP/IP allowed list changes in last 30 days

Who = All Users

What = IP Deny List Entry Added; IP Deny List Entry Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Active Directory\GPO Configuration

### - Changes in GPO assignments

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU; Group Policy Disabled Setting on Domain Changed; Group Policy Disabled Setting on OU Changed; Group Policy Inheritance Blocked Setting Changed; on Domain; Group Policy Link Added to OU; Group Policy Link Removed from OU; Group Policy Link Settings Modified; Group Policy Linked; Group Policy No Override Setting Changed on Domain; Group Policy Unlinked; Group Policy No Override Setting Changed on OU

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - Changes in linked GPOs

Who = All Users

What = Linked Group Policy on Domain Changed; Linked Group Policy on OU Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - Changes in the GPO assignments for all Sites

Who = All Users

What = Group Policy Link Added to Site; Group Policy Link Removed from Site; Group Policy Block Inheritance Setting Changed on Site; Group Policy No Override Setting Changed on Site; Group Policy Disabled Setting on Site Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - Group Policy block inheritance changes

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU; Group Policy Block Inheritance Setting Changed on Site; Group Policy Block Inheritance Setting Changed on Domain

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Group Policy disabled setting changes

Who = All Users

What = Group Policy Disabled Setting on OU Changed; Group Policy Disabled Setting on Site Changed; Group Policy Disabled Setting on Domain Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Active Directory\Group Policy

### - All Group Policy Events

Who = All Users

What = Group Policy Link Added to OU; Group Policy Link Removed from OU; Group Policy Link Setting Modified; Group Policy Link Added to Site; Group Policy Link Removed from Site

Group Policy Item facility; Group Policy Object facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - All Group Policy Events Including GPOAdmin Initiator

Returns all Group Policy events, displaying the Initiator UserName and EventSource in the Search Results

Who = All Users

What = Group Policy subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Layout Tab - Selected Columns: Initiator UserName and EventSource are added to default list

## Active Directory\Organizational Unit

### - Organizational Unit policy changes last 30 days

Report generated for each domain

Who = All Users

What = Linked Group Policy on OU Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Organizational Units added in last 30 days

Who = All Users

What = Subordinate OU Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Organizational Units deleted in last 30 days

Who = All Users

What = Subordinate OU Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Organizational Units renamed in last 30 days

Who = All Users

What = Subordinate OU Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Active Directory\Users and Groups

### - Group renamed (SAM account name) changes in last 30 days

Who = All Users

What = Group samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Group renamed in last 30 days

Who = All Users

What = Group Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Group type changes in last 30 days

Who = All Users

What = Group Type Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### - Nested group changes in last 30 days

Who = All Users

What = Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group; Nested Member Added to Group; Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Authentication Services

### - All Failed Logons in the last 7 days

Who = All Users

What = User failed to authenticate through Kerberos, User failed to authenticate through NTLM, User failed to log on interactively, User failed to log on interactively from a remote computer, User failed to perform a network logon from a remote computer

Where = All sources

When = Last 7 days

Origin = All workstations/servers

Info Tab = Fetch Every 10 Seconds

## Messaging\Exchange

### - All Exchange Administrative Group Events

Who = All Users

What = Exchange Administrative Group facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - All Email Address Policy Events

Who = All Users

What = Email Address Policy Added to Organization Configuration; Email Address Policy Email Address Filter List Changed; Email Address Policy Priority Changed; Email Address Policy Query Filter Changed; Email Address Policy Removed from Organization Configuration; Email Address Policy Renamed; Email

Address Policy Storage Filter Changed; Distribution List - Email Address Policy Enabled Changed; Mailbox - Email Address Policy Enabled Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - All Exchange Organization events in last 30 days

Who = All Users

What = Exchange Organization facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

- All Exchange Permission Tracking events in last 30 days

## Messaging\Exchange Online

### Microsoft 365 Exchange Online administrative cmdlets executed this week

Who = All Users

What = Microsoft 365 Exchange Online administration events, external and local

Where = All sources

When = This week

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped); User (Grouped)

## Microsoft SQL\Audit

### - All SQL Session Events in the last 24 hours

Who = All Users

What = SQL Session Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### - All SQL Stored Procedures Events in the last 24 hours

Who = All Users

What = SQL Stored Procedures Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### - All SQL TSQL Events in the last 24 hours

Who = All Users

What = SQL TSQL Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### Microsoft SQL\Configuration

#### - Audit Access DB Object Changed

Who = All Users

What = Audit Access Database Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Windows

#### - All Registry Events

Who = All Users

What = Registry subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Responsibility of the Controller

#### 24.2 - User Association

A summary report containing events from all of the following reports.

### Detailed list of audit policy modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit: Audit the Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled; Change Auditor Agent Connected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit The Access of Global System Objects Policy Changed; Audit: Audit The Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## 24.2 - Password Protection Mechanisms

A summary report containing events from all of the following reports.

### Detailed list of account lockout policy modifications

Who = All Users

What = Account Lockout Threshold Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of lockout duration policy modifications

Who = All Users

What = Account Lockout Duration Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of password age policy modifications

Who = All Users

What = Maximum Password Age Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of password complexity policy modifications

Who = All Users

What = Password Must Meet Complexity Requirements Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of password history policy modifications

Who = All Users

What = Enforce Password History Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of storing password policy modifications

Who = All Users

What = Store Passwords Using Reversible Encryption Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Integrity and Confidentiality

- Active Directory
- Active Directory\Users and Groups
- Active Directory\Organizational Units
- Messaging\Exchange
- Microsoft SQL\Configuration
- Microsoft SQL\Security
- Storage\Windows File System
- SharePoint
- Security of Processing

## Active Directory

### 24.2 - All AD Queries grouped by AD Search Filter

Who = All Users

What = AD Query Performed

Where = All sources

When = N/A

Origin = All workstations/servers

Layout tab - Order By: Time Detected (Not Grouped); LDAP Filter (Grouped)

### 24.2 - All AD Queries grouped by AD starting point

Who = All Users

What = AD Query Performed

Where = All sources

When = N/A

Origin = All workstations/servers

Layout Tab - Order By: Time Detected (Not Grouped); Object Canonical (Grouped)

## Active Directory\Users and Groups

### 5.6 - Changes in the membership of critical built-in Enterprise groups

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Active Directory\Organizational Units

### 5.6 - Organizational Units set to block GPO inheritance in last 30 days

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Messaging\Exchange

### 5.6 - Deleted Items Retention Period Changed for a user

Who = All Users

What = Deleted Item Retention Period Changed; Deleted Item Retention Use Defaults Storage Option Changed; Mailbox - End Date Retention Hold; Mailbox - Retention Hold Enabled; Mailbox - Retention Policy; Mailbox - Start Date for Retention Hold; Mailbox - Use Database Retention Defaults

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Mail Enabled for Group

Who = All Users

What = Mail Enabled for Group (Exchange 2003); Distribution List - Created; Distribution List - Enabled

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Mailbox Store Mounted

Who = All Users

What = Mailbox Store Mounted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Outlook Anywhere Enabled or Disabled for a Server

Who = All Users

What = Outlook Anywhere Disabled for Server; Outlook Anywhere Enabled for Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Public Folder Created

Who = All Users

What = Public Folder Store Created in Server Storage Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Public Store Mounted

Who = All Users

What = Public Store Mounted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Storage Group Removed from Exchange Server

Who = All Users

What = Storage Group Removed from Exchange Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Microsoft SQL\Configuration

### 5.6 - Audit Add Role

Who = All Users

What = Audit Add Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Alter Database

Who = All Users

What = Audit Alter Database

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Alter Database Object

Who = All Users

What = Audit Alter Database Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Alter Database Principal

Who = All Users

What = Audit Alter Database Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Alter Schema Object

Who = All Users

What = Audit Alter Schema Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Alter Server Object

Who = All Users

What = Audit Alter Server Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Alter Server Principal

Who = All Users

What = Audit Alter Server Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Drop DB User

Who = All Users

What = Audit Drop DB User

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Microsoft SQL\Data

### 5.6 - SQL Data Level Events in the last 24 hours

Who = All Users

What = Check Constraint Added to a Table; Check Constraint Removed from a Table; Default Constraint Added to a Table; Default Constraint Removed from a Table; Default Object Added; Default Object Removed; Foreign Key Added to a Table; Foreign Key Removed from a Table; Function Added; Function Altered; Function Removed; Index Added to a Table; Index Removed from a Table; Object Renamed; Primary Key Added to a Table; Primary Key Removed from a Table; Procedure Added; Procedure Altered; Procedure Removed; Row Added to a Table; Row Removed from a Table; Row Updated in a Table; Rule Added; Rule Removed; Statistics Added to a Table; Statistics Removed from a Table; Table Added; Table Altered; Table Removed; Table Truncated; Trigger Added; Trigger Altered; Trigger Removed; Type Added; Type Removed; User Added; User Removed; View Added; View Altered; View Removed

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### 5.6 - SQL Data Level Row Change Events in the last 24 hours

Who = All Users

What = Row Added to a Table; Row Removed from a Table; Row Updated in a Table

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### 5.6 - SQL Data Level Structure Change Events in the last 7 days

Who = All Users

What = Check Constraint Added to a Table; Check Constraint Removed from a Table; Default Constraint Added to a Table; Default Constraint Removed from a Table; Default Object Added; Default Object Removed; Foreign Key Added to a Table; Foreign Key Removed from a Table; Function Added; Function Altered; Function Removed; Index Added to a Table; Index Removed from a Table; Object Renamed; Primary Key Added to a Table; Primary Key Removed from a Table; Procedure Added; Procedure Altered; Procedure Removed; Rule Added; Rule Removed; Statistics Added to a Table; Statistics Removed from a Table; Table Added; Table Altered; Table Removed; Table Truncated; Trigger Added; Trigger Altered; Trigger Removed; Type Added; Type Removed; User Added; User Removed; View Added; View Altered; View Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Microsoft SQL\Security

### 5.6 - Audit Alter Object Derived Permission

Who = All Users

What = Audit Alter Object Derived Permission

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Storage\Windows File System

### 5.6 - Directory share added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - Directory share removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - File/Folder added in last 30 days

Who = All Users

What = File Created; Folder Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - File/Folder moved in last 30 days

Who = All Users

What = File Moved; Folder Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - File/Folder ownership changed in last 30 days

Who = All Users

What = File Ownership Changed; Folder Ownership Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - File/Folder permission changed in last 30 days

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - File/Folder removed in last 30 days

Who = All Users

What = File Deleted; Folder Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - Local share added in last 30 days

Who = All Users

What = Local Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - Local share permission changed in last 30 days

Who = All Users

What = Local Share Permissions Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - Local share removed in last 30 days

Who = All Users

What = Local Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - Shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 5.6 - Shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## SharePoint

### 5.6 - Site Collection Groups created and deleted in the last 7 days

Who = All Users

What = Security group created; Security group deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Site Collection Groups Membership changes in the last 7 days

Who = All Users

What = Member added to security group; Member removed from security group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Site Collection Ownership changes in the last 7 days

Who = All Users

What = Site collection ownership granted; Site collection ownership revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Site Collections created and deleted in the last 7

Who = All Users

What = Site collection created; Site collection deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Sites created and deleted in the last 7 days

Who = All Users

What = Site created; Site deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Sites moved in the last 7 days

Who = All Users

What = Site moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Security of Processing

- 32 - Detailed List of security log modifications
- Active Directory
- Authentication Services
- Active Directory\Configuration
- Authentication Services
- Microsoft SQL\Security
- SharePoint
- Storage\Windows File System

### 32 - Detailed List of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit The Access of Global System Objects Policy Changed; Audit: Audit The Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Active Directory

### 32 - Active Directory Database Events in last 30 days

Who = All Users

What = Active Directory Database facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Changes to SYSVOL on all Domain Controllers in last 30 days

Who = All Users

What = SYSVOL facility; SYSVOL Location Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Default domain audit policy changes last 30 days

Report generated for each domain

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy

Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Event Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Authentication Services

### 32 - Authentication Services computers added in last 30 days

Who = All Users

What = Authentication Services Computer object added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Authentication Services computers deleted in last 30 days

Who = All Users

What = Authentication Services Computer object deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Default domain Kerberos policy changes last 30 days

Report generated for each domain

Who = All Users

What = Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Default domain password policy changes last 30 days

Report generated for each domain

Who = All Users

What = Enforce Password History Policy Changed; Maximum Password Age Policy Changed; Minimum Password Age Policy Changed; Minimum Password Length Policy Changed; Password Must Meet Complexity Requirements Policy Changed; Store Passwords Using Reversible Encryption Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Active Directory\Configuration

## 32 - All Schema Configuration Events

Who = All Users

What = Schema Configuration facility

Schema FSMO Role Owner Moved; Schema Modifications Allowed Flag Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## 32 - Authentication Services GPO settings changes in last 30 days

Who = All Users

What = Authentication Services GPO Settings Computer Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## 32 - Changes in trust

Who = All Users

What = Cross-forest Trust Added; Cross-forest Trust Removed; Trust Added; Trust Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## 32 - Changes to Domain account policies (GPO filter) in last 30 days

Who = All Users

What = Account Lockout Duration Policy Changed; Account Lockout Threshold Policy Changed; Enforce Password History Policy Changed; Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Password Age Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed; Minimum Password Age Policy Changed; Minimum Password Length Policy Changed; Password Must Meet Complexity Requirements Policy Changed; Store Passwords Using Reversible Encryption Policy Changed; Reset Account Lockout Counter After Change Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## 32 - Changes to Domain Audit Policies (GPO filter) in the last 30 days

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Event Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## 32 - Changes to Domain Kerberos policies (GPO filter) in the last 30 days

Who = All Users

What = Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## 32 - Changes to IP deny filter changes in last 30 days

Who = All Users

What = IP Deny List Entry Added; IP Deny List Entry Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## 32 - Cross Forest level trusts added in last 30 days

Who = All Users

What = Cross-forest Trust Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## 32 - Cross Forest level trusts deleted in last 30 days

Who = All Users

What = Cross-forest Trust Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## 32 - DNS server list changes in last 30 days

Who = All Users

What = Contents of DNS Server List Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

## 32 - Domain policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Linked Group Policy or Domain Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - High Severity changes in the last 30 days

Who = All Users

What = Severity | High

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Permission changes on domains in the last 30 days

Who = All Users

What = DACL Changed on Domain Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Trusts added in last 30 days

Who = All Users

What = Trust Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Trusts deleted in last 30 days

Who = All Users

What = Trust Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Use of dynamic DNS changed in last 30 days

Who = All Users

What = Use of Dynamic DNS Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

## Active Directory\GPO Configuration

### 32 - GPO Link changes on Domain objects in the last 30 days

Who = All Users

What = DACL Changed on Group Policy Object; Group Policy Linked; Group Policy Unlinked; Group Policy Block Inheritance Setting Changed on Domain; Group Policy No Override Setting Changed on Domain; Group Policy Disabled Setting on Domain Changed; Owner Changed on Group Policy Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Active Directory\Users and Groups

### 32 - Critical Group Membership changes in last 30 days

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group; Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Group added in last 30 days

Who = All Users

What = Group Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Group deleted in last 30 days

Who = All Users

What = Group Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Group member added changes in last 30 days

Who = All Users

What = Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Group member removed changes in last 30 days

Who = All Users

What = Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Group Membership changes in last 30 days

Who = All Users

What = Member Added to Group, Member Removed from Group; Nested Member Added to Group; Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Group moved in last 30 days

Who = All Users

What = Group Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Group nested member added changes in last 30 days

Who = All Users

What = Nested Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Group nested member removed changes in last 30 days

Who = All Users

What = Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Membership changed in critical groups in last 7 days

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 32 - Permissions on group changes last 30 days

Who = All Users

What = DACL Changed on Group Object; Active Directory subsystem

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Permissions on user accounts changed in last 30 days

Who = All Users

What = DACL Changed on User Object; Required User’s Permissions Changed for User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Permissions to AdminSDHolder in last 30 days

Who = All Users

What = DACL Changed on AdminSDHolder Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - User account restrictions changed in the last 30 days

Who = All Users

What = User Account Enabled; User Account Disabled; DACL Change on User Object; User Member-of Added; User Member-of Removed; User accountExpires Changed; User Password Changed; User logonHours Changed; User Account Locked; User Account Unlocked; Active Session Limit Changed for User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - User logon hours changed in last 30 days

Who = All Users

What = User logonHours Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users added in last 30 days

Who = All Users

What = User Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users added to group in last 30 days

Who = All Users

What = User Member-of Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users deleted in last 30 days

Who = All Users

What = User Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users disabled in last 30 days

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users enabled in last 30 days

Who = All Users

What = User Account Enabled; User Account Re-enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users expiration date changed in last 30 days

Who = All Users

What = User Account Expires changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users locked in last 30 days

Who = All Users

What = User Account Locked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users locked out in last 30 days

Who = All Users

What = User Account Locked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users logon hours changed in last 30 days

Who = All Users

What = User logonHours Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users moved in last 30 days

Who = All Users

What = User Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users removed from group in last 30 days

Who = All Users

What = User Member-of Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users renamed in last 30 days

Who = All Users

What = Domain User Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users SAM account name changed in last 30 days

Who = All Users

What = User samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users unlocked in last 30 days

Who = All Users

What = User Account Unlocked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - Users workstation access restrictions changed in last 30 days

Who = All Users

What = User userWorkstations Added; User userWorkstations Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Authentication Services

### 32 - Detailed list of password age policy modifications

Who = All Users

What = Maximum Password Age Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 32 - Detailed list of password complexity policy modifications

Who = All Users

What = Password Must Meet Complexity Requirements Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 32 - Detailed list of password history policy modifications

Who = All Users

What = Enforce Password History Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 32 - Detailed list of storing password policy modifications

Who = All Users

What = Store Passwords Using Reversible Encryption Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### - IPSec changes in last 30 days

Who = All Users

What = IPSEC Settings Changed

Where = All sources

When = Last 30 days

Origin = All domain controllers

## Messaging\Exchange

### 32 - All Exchange Administrative Group events in last 30 days

Who = All Users

What = Exchange Administrative Group facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### 32 - All Send Connector Change Events

Who = All Users

What = Mutual Auth TLS Option Changed on Send Connector; Send Connector Added to Organization Configuration; Send Connector Protocol Logging Changed; Send Connector Removed from Organization Configuration; Send Connector Renamed; Send Connector Response FQDN Changed; Send Connector Status Changed; Address Space Added to Send Connector; Address Space Removed from Send Connection; External DNS Lookup Option Changed on Send Connector; Send Connector Maximum Message Size Changed; Smart Host Added to Send Connector; Smart Host Authentication Settings Changed on Send Connector; Smart Host Removed from Send Connector; Source Server Added to Send Connector; Source Server Removed from Send Connector

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 32 - All Unified Messaging (UM) Policy Change Events

Who = All Users

What = Allow Calls to Extensions Option Changed in UM Mailbox Policy; Allow Calls to Same-Plan Users Option Changed in UM Mailbox Policy; Allow Common PIN Pattern Option Changed in UM Mailbox Policy; Fax Identity Changed in UM Mailbox Policy; Fax Message Text Changed in UM Mailbox Policy; Incorrect PIN Mailbox Lockout Setting Changed in UM Mailbox Policy; Incorrect PIN Reset Setting Changed in UM Mailbox Policy; In-Country Rule Group Added to UM Mailbox Policy; In-Country Rule Group Removed From UM Mailbox Policy; International Rule Group Added to UM Mailbox Policy; International Rule Group Removed from UM Mailbox Policy; Mailbox Enabled Text Changed in UM Mailbox Policy; Maximum Greeting Duration Changed in UM Mailbox Policy; Maximum Greeting Duration Enabled Option Changed in UM Mailbox Policy; Minimum PIN Length Changed in UM Mailbox Policy; PIN History Length Changed in UM Mailbox Policy; PIN Lifetime Changed in UM Mailbox Policy; PIN Reset Text Changed in UM Mailbox Policy; UM Mailbox Policy Added to Organization Configuration; UM Mailbox Policy Removed from Organization Configuration; UM Mailbox Policy Renamed; Voice Message Text Changed in UM Mailbox Policy

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Microsoft SQL\Security

### 32 - All SQL Add Roles, User, and Login Events in the last 24 hours

Who = All Users

What = Audit Add DB User; Audit Add Login; Audit Add Login to Server Role; Audit Add Member to DB Role; Audit Add Role

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### 32 - All SQL Security Audit Events in the last 24 hours

Who = All Users

What = SQL Security Audit Event facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### 5.6 - Audit Add DB User

Who = All Users

What = Audit Add DB User

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Add Login

Who = All Users

What = Audit Add Login

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Add Login to Server Role

Who = All Users

What = Audit Add Login to Server Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 5.6 - Audit Add Member to DB Role

Who = All Users

What = Audit Add Member to DB Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## SharePoint

### 32 - Permission changes in the last 7 days

Who = All Users

What = All permission levels revoked; Permission level created; Permission level deleted; Permission level granted; Permission level permissions modified; Permission level revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### 32 - Permission Inheritance changes in the last 7 days

Who = All Users

What = Permission inheritance broken; Permission inheritance restored; Permission level inheritance broken; Permission level permissions modified

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Storage\Windows File System

### 32 - File/Folder auditing changed in last 30 days

Who = All Users

What = File Auditing Changed; Folder Auditing Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# HIPAA (Health Insurance Portability and Accountability Act)

The HIPAA reports are available in the following folders:

- 164.308 – Administrative Safeguards | Information Access Management
- 164.308 – Administrative Safeguards | Security Awareness and Training
- 164.308 – Administrative Safeguards | Security Management
- 164.308 – Administrative Safeguards | Workforce Security
- 164.310 – Physical Safeguards | Standard Workstation Security
- 164.310 – Physical Safeguards | Standard Workstation Use
- 164.312 – Technical Safeguards | Standard Person or entity authentication
- 164.312 – Technical Safeguards | Standard Access Control
- 164.312 – Technical Safeguards | Standard Audit Control

# 164.308 – Administrative Safeguards | Security Management

## Information System Activity Review

### (Executive Summary) - Formal Mechanism for Processing Records

A summary report containing events from all of the following reports.

### Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Connected; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Object Policy Changed; Audit: Audit the use of Backup and Restore Privilege Policy Changed; Crash on Audit Fail Policy Changed; Security Audit Log Rolled Over; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Access Control - File Access

### Directory shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Directory shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder added in last 30 days

Who = All Users

What = File Created; Folder Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder attribute changed in last 30 days

Who = All Users

What = File Attribute Changed; Folder Attribute Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder auditing changed in last 30 days

Who = All Users

What = File Auditing Changed; Folder Auditing Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder modified date changed in last 30 days

Who = All Users

What = File Last Write Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder moved in last 30 days

Who = All Users

What = File Moved; Folder Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder ownership changed in last 30 days

Who = All Users

What = File Ownership Changed; Folder Ownership Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder permission changed in last 30 days

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder removed in last 30 days

Who = All Users

What = File Deleted; Folder Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder renamed in last 30 days

Who = All Users

What = File Renamed; Folder Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share added in last 30 days

Who = All Users

What = Local Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share auditing changed in last 30 days

Who = All Users

What = Local Share Auditing changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share permission changed in last 30 days

Who = All Users

What = Local Share Permissions Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share removed in last 30 days

Who = All Users

What = Local Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## EMC

### EMC file access rights changed

Who = All Users

What = EMC file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents written

Who = All Users

What = EMC file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents created

Who = All Users

What = EMC file contents created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents deleted

Who = All Users

What = EMC file contents deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents moved

Who = All Users

What = EMC file contents moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents opened

Who = All Users

What = EMC file contents opened

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file ownership changed

Who = All Users

What = EMC file ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file renamed

Who = All Users

What = EMC file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder access rights changed

Who = All Users

What = EMC folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder created

Who = All Users

What = EMC folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder deleted

Who = All Users

What = EMC folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder moved

Who = All Users

What = EMC folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder ownership changed

Who = All Users

What = EMC folder ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder renamed

Who = All Users

What = EMC folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## Exchange

### All Exchange Permission Tracking Events

Who = All Users

What = Exchange Permission Tracking facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Journaling Rule Change Events

Who = All Users

What = Journaling Rule Added to Organization Configuration; Journaling Rule Changed; Journaling Rule Removed from Organization Configuration; Journaling Rule Renamed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Deleted Items Retention Period Changed for a user

Who = All Users

What = Deleted Item Retention Period Changed; Deleted Item Retention Use Defaults Storage Option Changed; Mailbox - End Date Retention Hold; Mailbox - Retention Hold Enabled; Mailbox - Retention Policy; Mailbox - Start Date for Retention Hold; Mailbox - Use Database Retention Defaults

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Logon Activity

### All Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively; User logged on interactively

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

Info Tab = Fetch Every 10 Seconds

### All Logons in the past 24 hours

Who = All Users

What = Authentication Activity; Domain Controller Authentication; Logon Session

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

Info Tab = Fetch Every 10 Seconds

### All Remote Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively from a remote computer; User failed to perform a network logon from a remote computer; User logged on interactively from a remote computer; User performed a successful network logon from a remote computer

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

Info Tab = Fetch Every 10 Seconds

### All User Sessions in the past 24 hours

Who = All Users

What = Logon Session facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

Info Tab = Fetch Every 10 Seconds

## NetApp

### NetApp file access rights changed (no from-value)

Who = All Users

What = NetApp file access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file access rights changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file contents written

Who = All Users

What = NetApp file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file created

Who = All Users

What = NetApp file created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file deleted

Who = All Users

What = NetApp file deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file moved

Who = All Users

What = NetApp file moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file opened

Who = All Users

What = NetApp file opened

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed (no from-value)

Who = All Users

What = NetApp file access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file renamed

Who = All Users

What = NetApp file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder created

Who = All Users

What = NetApp folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder deleted

Who = All Users

What = NetApp folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder moved

Who = All Users

What = NetApp folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder renamed

Who = All Users

What = NetApp folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## SharePoint

### Permission changes in the last 7 days

Who = All Users

What = All permission levels revoked; Permission level created; Permission level deleted; Permission level granted; Permission level permissions modified; Permission level revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Permission inheritance changes in the last 7 days

Who = All Users

What = Permission inheritance broken; Permission inheritance restored; Permission level inheritance broken; Permission level permissions modified

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups created and deleted in the last 7 days

Who = All Users

What = Security group created; Security group deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups membership changes in the last 7 days

Who = All Users

What = Member added to security group; Member removed from security group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection ownership changes in the last 7 days

Who = All Users

What = Site collection ownership granted; Site collection ownership revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

#### Site Collections created and deleted in the last 7 days

Who = All Users

What = Site collection created; Site collection deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

#### Sites created and deleted in the last 7 days

Who = All Users

What = Site created; Site deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

#### Sites moved in the last 7 days

Who = All Users

What = Site moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# 164.308 – Administrative Safeguards | Workforce Security

# Authorization and Supervision

## Authentication Services

#### Authentication Services computers added in last 30 days

Who = All Users

What = Authentication Services Computer object added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

#### Authentication Services computers deleted in last 30 days

Who = All Users

What = Authentication Services Computer object deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Groups set to UNIX-disabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for Group - Restriction = To: Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Groups set to UNIX-enabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for Group - Restriction = To: Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX home directory changed in last 30 days

Who = All Users

What = UNIX Home Directory Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX login shell changed in last 30 days

Who = All Users

What = UNIX Login Shell Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX-enabled groups deleted in last 30 days

Who = All Users

What = UNIX-Enabled Group Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX-enabled users deleted in last 30 days

Who = All Users

What = UNIX-Enabled User Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users set to UNIX-disabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User - Restriction = To: Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users set to UNIX-enabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User - Restriction = To: Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Computer Activity

### Computers added in the last 30 days

Who = All Users

What = Computer Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers disabled in the last 30 days

Who = All Users

What = Computer Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers enabled in the last 30 days

Who = All Users

What = Computer Account Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers moved in the last 30 days

Who = All Users

What = Computer Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers removed in the last 30 days

Who = All Users

What = Computer Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers renamed in the last 30 days

Who = All Users

What = Computer Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Exchange

### All Exchange Administrative Group Events

Who = All Users

What = Exchange Administrative Group facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Distribution List (Group) Events

Who = All Users

What = Exchange Security Group facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Permission Tracking Events

Who = All Users

What = Exchange Permission Tracking facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Group Management

### Group added in last 30 days

Who = All Users

What = Group Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group deleted in last 30 days

Who = All Users

What = Group Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member added changes in last 30 days

Who = All Users

What = Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member removed changes in last 30 days

Who = All Users

What = Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group moved in last 30 days

Who = All Users

What = Group Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member added changes in last 30 days

Who = All Users

What = Nested Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member removed changes in last 30 days

Who = All Users

What = Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group permissions changed in last 30 days

Who = All Users

What = DACL Changed on Group Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed (SAM account name) changes in last 30 days

Who = All Users

What = Group samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed in last 30 days

Who = All Users

What = Group Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group type changes in last 30 days

Who = All Users

What = Group Type Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## SQL

### All SQL Add Roles, User, and Login Events in the last 24 hours

Who = All Users

What = Audit Add DB User; Audit Add Login; Audit Add Login to Server Role; Audit Add Member to DB Role; Audit Add Role

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### Audit Add Login

Who = All Users

What = Audit Add Login

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Audit Add Login to Server Role

Who = All Users

What = Audit Add Login to Server Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Audit Add Member to DB Role

Who = All Users

What = Audit Add Member to DB Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Audit Add Role

Who = All Users

What = Audit Add Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Audit Alter Database

Who = All Users

What = Audit Alter Database

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Audit Alter Database Object

Who = All Users

What = Audit Alter Database Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Audit Alter Database Principal

Who = All Users

What = Audit Alter Database Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Object Derived Permission

Who = All Users

What = Audit Alter Object Derived Permission

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Schema Object

Who = All Users

What = Audit Alter Schema Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Object

Who = All Users

What = Audit Alter Server Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Principal

Who = All Users

What = Audit Alter Server Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Trust Activity

### Cross Forest level trust added in last 30 days

Who = All Users

What = Cross-forest Trust Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Cross Forest level trust deleted in last 30 days

Who = All Users

What = Cross-forest Trust Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Trusts added in last 30 days

Who = All Users

What = Trust Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Trusts deleted in last 30 days

Who = All Users

What = Trust Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## User Management

### Changes to user profiles in last 30 days

Who = All Users

What = Home Folder Changed on User Object; Home Folder Mapped Drive Changed on User Object; Level of Control Changed for User Object; Primary Group ID Changed for User Object; Profile Path Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions on user accounts changed in last 30 days

Who = All Users

What = DACL Changed on User Object; Required User’s Permissions Changed for User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users added in last 30 days

Who = All Users

What = User Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users added to group in last 30 days

Who = All Users

What = User Member-of Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users deleted in last 30 days

Who = All Users

What = User Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users disabled in last 30 days

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users display name changed in last 30 days

Who = All Users

What = Display Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users enabled in last 30 days

Who = All Users

What = User Account Enabled; User Account Re-enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users first name changed in last 30 days

Who = All Users

What = First Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users last name changed in last 30 days

Who = All Users

What = Last Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Users locked out in last 30 days

Who = All Users

What = User Account Locked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Users logon hours changed in last 30 days

Who = All Users

What = User logonHours Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Users moved in last 30 days

Who = All Users

What = User Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Users name(s) changed in last 30 days

Who = All Users

What = Display Name Changed on User Object; First Name Changed on User Object; User samAccountName Changed; Last Name Changed on User Object; User userPrincipal Name Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Users principal name changed in last 30 days

Who = All Users

What = User userPrincipalName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Users removed from group in last 30 days

Who = All Users

What = User Member-of Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users renamed in last 30 days

Who = All Users

What = Domain User Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users SAM account name changed in last 30 days

Who = All Users

What = User samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users status changed in last 30 days (Enabled, Disabled, Created, Deleted, Locked, Unlocked)

Who = All Users

What = User Account Enabled; User Account Disabled; User Object Added; User Object Removed; User Account Locked; User Account Unlocked; User Account Re-enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users unlocked in last 30 days

Who = All Users

What = User Account Unlocked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users workstation access restrictions changed in last 30 days

Who = All Users

What = User userWorkstations Added; User userWorkstations Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Workforce Clearance Procedures

## Access Control - File System

### Directory shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Directory shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## File/Folder added in last 30 days

Who = All Users

What = File Created; Folder Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## File/Folder attribute changed in last 30 days

Who = All Users

What = File Attribute Changed; Folder Attribute Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## File/Folder auditing changed in last 30 days

Who = All Users

What = File Auditing Changed; Folder Auditing Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## File/Folder modified date changed in last 30 days

Who = All Users

What = File Last Write Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## File/Folder moved in last 30 days

Who = All Users

What = File Moved; Folder Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder ownership changed in last 30 days

Who = All Users

What = File Ownership Changed; Folder Ownership Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder permission changed in last 30 days

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder removed in last 30 days

Who = All Users

What = File Deleted; Folder Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder renamed in last 30 days

Who = All Users

What = File Renamed; Folder Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share added in last 30 days

Who = All Users

What = Local Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share auditing changed in last 30 days

Who = All Users

What = Local Share Auditing changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share permission changed in last 30 days

Who = All Users

What = Local Share Permissions Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share removed in last 30 days

Who = All Users

What = Local Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## EMC

### EMC file access rights changed

Who = All Users

What = EMC file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents written

Who = All Users

What = EMC file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents created

Who = All Users

What = EMC file contents created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents deleted

Who = All Users

What = EMC file contents deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents moved

Who = All Users

What = EMC file contents moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents opened

Who = All Users

What = EMC file contents opened

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file ownership changed

Who = All Users

What = EMC file ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file renamed

Who = All Users

What = EMC file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## EMC folder access rights changed

Who = All Users

What = EMC folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

## EMC folder created

Who = All Users

What = EMC folder created

Where = All sources

When = This Week

Origin = All workstations/servers

## EMC folder deleted

Who = All Users

What = EMC folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

## EMC folder moved

Who = All Users

What = EMC folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

## EMC folder ownership changed

Who = All Users

What = EMC folder ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

## EMC folder renamed

Who = All Users

What = EMC folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## NetApp

### NetApp file access rights changed (no from-value)

Who = All Users

What = NetApp file access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file access rights changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file contents written

Who = All Users

What = NetApp file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file created

Who = All Users

What = NetApp file created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file deleted

Who = All Users

What = NetApp file deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file moved

Who = All Users

What = NetApp file moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file opened

Who = All Users

What = NetApp file opened

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed (no from-value)

Who = All Users

What = NetApp file access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file renamed

Who = All Users

What = NetApp file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder created

Who = All Users

What = NetApp folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder deleted

Who = All Users

What = NetApp folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder moved

Who = All Users

What = NetApp folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder renamed

Who = All Users

What = NetApp folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## SharePoint

### Permission changes in the last 7 days

Who = All Users

What = All permission levels revoked; Permission level created; Permission level deleted; Permission level granted; Permission level permissions modified; Permission level revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Permission inheritance changes in the last 7 days

Who = All Users

What = Permission inheritance broken; Permission inheritance restored; Permission level inheritance broken; Permission level permissions modified

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups created and deleted in the last 7 days

Who = All Users

What = Security group created; Security group deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups membership changes in the last 7 days

Who = All Users

What = Member added to security group; Member removed from security group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection ownership changes in the last 7 days

Who = All Users

What = Site collection ownership granted; Site collection ownership revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collections created and deleted in the last 7 days

Who = All Users

What = Site collection created; Site collection deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Sites created and deleted in the last 7 days

Who = All Users

What = Site created; Site deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Sites moved in the last 7 days

Who = All Users

What = Site moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Termination Procedures

### (Executive Summary) – Termination Procedures

A summary report containing events from all of the following reports.

### Detailed list of deleted user modifications

Who = All Users

What = User Object Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of disabled user modifications

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Group Management

### Group added in last 30 days

Who = All Users

What = Group Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group deleted in last 30 days

Who = All Users

What = Group Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member added changes in last 30 days

Who = All Users

What = Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member removed changes in last 30 days

Who = All Users

What = Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group moved in last 30 days

Who = All Users

What = Group Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member added changes in last 30 days

Who = All Users

What = Nested Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member removed changes in last 30 days

Who = All Users

What = Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group permissions changed in last 30 days

Who = All Users

What = DACL Changed on Group Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed (SAM account name) changes in last 30 days

Who = All Users

What = Group samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed in last 30 days

Who = All Users

What = Group Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# 164.308 – Administrative Safeguards | Information Access Management

# Access Establishment and Modification

## Access Control - File System

### Directory shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Directory shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder added in last 30 days

Who = All Users

What = File Created; Folder Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder attribute changed in last 30 days

Who = All Users

What = File Attribute Changed; Folder Attribute Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder auditing changed in last 30 days

Who = All Users

What = File Auditing Changed; Folder Auditing Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder modified date changed in last 30 days

Who = All Users

What = File Last Write Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder moved in last 30 days

Who = All Users

What = File Moved; Folder Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder ownership changed in last 30 days

Who = All Users

What = File Ownership Changed; Folder Ownership Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder permission changed in last 30 days

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder removed in last 30 days

Who = All Users

What = File Deleted; Folder Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder renamed in last 30 days

Who = All Users

What = File Renamed; Folder Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share added in last 30 days

Who = All Users

What = Local Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share auditing changed in last 30 days

Who = All Users

What = Local Share Auditing changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share permission changed in last 30 days

Who = All Users

What = Local Share Permissions Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share removed in last 30 days

Who = All Users

What = Local Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Critical GPO Changes

### Default domain audit policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Event Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Default domain Kerberos policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Default domain password policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Enforce Password History Policy Changed; Maximum Password Age Policy Changed; Minimum Password Age Policy Changed; Minimum Password Length Policy Changed; Password Must Meet Complexity Requirements Policy Changed; Store Passwords Using Reversible Encryption Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Detailed list of GPO modifications

Who = All Users

What = Accounts: Administrator Account Status Policy Changed; Accounts: Guest Account Status Policy Changed; Accounts: Limit Local Account Use of Blank Passwords to Console Only Policy Changed; Accounts: Rename Administrator Account Policy Changed; Accounts: Rename Guest Account Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit: Audit the User of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed; Devices: Allow Undock Without Having to Logon Policy Changed; Devices: Allowed to Format and Eject Removable Media Policy Changed; Devices: Prevent Users from Installing Printer Drivers Policy Changed; Devices: Restrict CD-ROM Access to Locally Logged-on User Only Policy Changed; Devices: Restrict Floppy Access to Locally Logged-on User Only Policy Changed; Devices: Unsigned Driver Installation Behavior Policy Changed; Domain Controller: Allow Server Operators to Schedule Tasks Policy Changed; Domain Controller: LDAP Server Signing Requirements Policy Changed; Domain Controller: Refuse Machine Account Password Changes Policy Changed; Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always) Policy Changed; Enforce Password History Policy Changed; Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; System Objects: Strengthen Default Permissions of Global System Objects Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Domain policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Linked Group Policy or Domain Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational unit policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Linked Group Policy on OU Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Domain Security

### Changes to Domain account policies (GPO filter) in last 30 days

Who = All Users

What = Account Lockout Duration Policy Changed; Account Lockout Threshold Policy Changed; Enforce Password History Policy Changed; Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Password Age Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed; Minimum Password Age Policy Changed; Minimum Password Length Policy Changed; Password Must Meet Complexity Requirements Policy Changed; Store Passwords Using Reversible Encryption Policy Changed; Reset Account Lockout Counter After Change Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to Domain Audit policies (GPO filter) in last 30 days

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Event Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to Domain Kerberos policies (GPO filter) in last 30 days

Who = All Users

What = Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### GPO Link changes on Domain objects in last 30 days

Who = All Users

What = DACL Changed on Group Policy Object; Group Policy Linked; Group Policy Unlinked; Group Policy Block Inheritance Setting Changed on Domain; Group Policy No Override Setting Changed on Domain; Group Policy Disabled Setting on Domain Changed; Owner Changed on Group Policy Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permission changes on domains in last 30 days

Who = All Users

What = DACL Changed on Domain Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions to AdminSDHolder Changes in last 30 days

Who = All Users

What = DACL Changed on AdminSDHolder Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## EMC

### EMC file access rights changed

Who = All Users

What = EMC file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents written

Who = All Users

What = EMC file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents created

Who = All Users

What = EMC file contents created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents deleted

Who = All Users

What = EMC file contents deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents moved

Who = All Users

What = EMC file contents moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents opened

Who = All Users

What = EMC file contents opened

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file ownership changed

Who = All Users

What = EMC file ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file renamed

Who = All Users

What = EMC file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder access rights changed

Who = All Users

What = EMC folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder created

Who = All Users

What = EMC folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder deleted

Who = All Users

What = EMC folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder moved

Who = All Users

What = EMC folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder ownership changed

Who = All Users

What = EMC folder ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder renamed

Who = All Users

What = EMC folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## Exchange

### All ActiveSync Mailbox Policy Events

Who = All Users

What = ActiveSync Mailbox Policy Added to Organization Client Access Configuration; ActiveSync Mailbox Policy Allow Attachments to be Downloaded Option Changed; ActiveSync Mailbox Policy Allow Non-Provisionable Devices Options Changed; ActiveSync Mailbox Policy Allow Simple Password Option Changed; ActiveSync Mailbox Policy Enable Password Recovery Option Changed; ActiveSync Mailbox Policy Maximum Attachment Size Changed; ActiveSync Mailbox Policy Minimum Password Length Changed; ActiveSync Mailbox Policy Password Expiration Changed; ActiveSync Mailbox Policy Password History Changed; ActiveSync Mailbox Policy Password Required Option Changed; ActiveSync Mailbox Policy Removed from Organization Client Access Configuration; ActiveSync Mailbox Policy Renamed; ActiveSync Mailbox Policy Require Alphanumeric Password Option Changed; ActiveSync Mailbox Policy Require Encryption On Device Option Changed; ActiveSync Mailbox Policy User Idle Timeout Changed; ActiveSync Mailbox Policy Windows File Shares Access Option Changed; ActiveSync Mailbox Policy Windows SharePoint Services Access Option Changed; ActiveSync Mailbox Policy Number of Failed Attempts Allowed Changed; ActiveSync Mailbox Policy Refresh Interval Changed; ActiveSync Mailbox Policy Require Encryption On Device Option Changed; Mobile Device - ActiveSync Device Policy

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Email Address Policy Events

Who = All Users

What = Email Address Policy Added to Organization Configuration; Email Address Policy Email Address Filter List Changed; Email Address Policy Priority Changed; Email Address Policy Query Filter Changed; Email Address Policy Removed from Organization Configuration; Email Address Policy Renamed; Email Address Policy Storage Filter Changed; Distribution List - Email Address Policy Enabled Changed; Mailbox - Email Address Policy Enabled Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Permission Tracking Events

Who = All Users

What = Exchange Permission Tracking facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Journaling Rule Change Events

Who = All Users

What = Journaling Rule Added to Organization Configuration; Journaling Rule Changed; Journaling Rule Removed from Organization Configuration; Journaling Rule Renamed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Deleted Items Retention Period Changed for a user

Who = All Users

What = Deleted Item Retention Period Changed; Deleted Item Retention Use Defaults Storage Option Changed; Mailbox - End Date Retention Hold; Mailbox - Retention Hold Enabled; Mailbox - Retention Policy; Mailbox - Start Date for Retention Hold; Mailbox - Use Database Retention Defaults

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Message Tracking Options Changed on an Exchange 2007 Server

Who = All Users

What = Message Tracking Option Changed on Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Group Management

### Group added in last 30 days

Who = All Users

What = Group Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group deleted in last 30 days

Who = All Users

What = Group Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member added changes in last 30 days

Who = All Users

What = Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member removed changes in last 30 days

Who = All Users

What = Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group moved in last 30 days

Who = All Users

What = Group Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member added changes in last 30 days

Who = All Users

What = Nested Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member removed changes in last 30 days

Who = All Users

What = Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group permissions changed in last 30 days

Who = All Users

What = DACL Changed on Group Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed (SAM account name) changes in last 30 days

Who = All Users

What = Group samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed in last 30 days

Who = All Users

What = Group Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users removed from group in last 30 days

Who = All Users

What = User member-of removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Logon Activity

### All Failed Logons in the last 7 days

Who = All Users

What = User failed to authenticate through Kerberos, User failed to authenticate through NTLM, User failed to log on interactively, User failed to log on interactively from a remote computer, User failed to perform a network logon from a remote computer

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively; User logged on interactively

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Logons in the past 24 hours

Who = All Users

What = Authentication Activity; Domain Controller Authentication; Logon Session

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Remote Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively from a remote computer; User failed to perform a network logon from a remote computer; User logged on interactively from a remote computer; User performed a successful network logon from a remote computer

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All User Sessions in the past 24 hours

Who = All Users

What = Logon Session facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## NetApp

### NetApp file access rights changed (no from-value)

Who = All Users

What = NetApp file access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file access rights changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file contents written

Who = All Users

What = NetApp file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file created

Who = All Users

What = NetApp file created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file deleted

Who = All Users

What = NetApp file deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file moved

Who = All Users

What = NetApp file moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file opened

Who = All Users

What = NetApp file opened

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed (no from-value)

Who = All Users

What = NetApp file access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file renamed

Who = All Users

What = NetApp file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder created

Who = All Users

What = NetApp folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder deleted

Who = All Users

What = NetApp folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder moved

Who = All Users

What = NetApp folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder renamed

Who = All Users

What = NetApp folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## Organizational Unit Management

### Organizational Units added in last 30 days

Who = All Users

What = Subordinate OU Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units deleted in last 30 days

Who = All Users

What = Subordinate OU Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units renamed in last 30 days

Who = All Users

What = Subordinate OU Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units set to block GPO inheritance in last 30 days

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Group Policy Changed last 30 days

### Group Policy block inheritance changes

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU; Group Policy Block Inheritance Setting Changed on Site; Group Policy Block Inheritance Setting Changed on Domain

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group Policy disabled setting changes

Who = All Users

What = Group Policy Disabled Setting on OU Changed; Group Policy Disabled Setting on Site Changed; Group Policy Disabled Setting on Domain Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group Policy no override changes

Who = All Users

What = Group Policy No Override Setting Changed on OU; Group Policy No Override Setting Changed on Site; Group Policy No Override Setting Changed on Domain

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## SharePoint

### Permission changes in the last 7 days

Who = All Users

What = All permission levels revoked; Permission level created; Permission level deleted; Permission level granted; Permission level permissions modified; Permission level revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Permission inheritance changes in the last 7 days

Who = All Users

What = Permission inheritance broken; Permission inheritance restored; Permission level inheritance broken; Permission level permissions modified

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups created and deleted in the last 7 days

Who = All Users

What = Security group created; Security group deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups membership changes in the last 7 days

Who = All Users

What = Member added to security group; Member removed from security group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection ownership changes in the last 7 days

Who = All Users

What = Site collection ownership granted; Site collection ownership revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collections created and deleted in the last 7 days

Who = All Users

What = Site collection created; Site collection deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

#### Sites created and deleted in the last 7 days

Who = All Users

What = Site created; Site deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

#### Sites moved in the last 7 days

Who = All Users

What = Site moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# 164.308 – Administrative Safeguards | Security Awareness and Training

# Log-in Monitoring

## Exchange

#### Access by non-owners

Who = All Users

What = Contact Copied by Non-Owner, Contact Created by Non-Owner, Contact Deleted by Non-Owner, Contact Modified by Non-Owner, Contact Moved by Non-Owner, Contact Permanently Deleted by Non-Owner, Contact Read by Non-Owner, Contacts Opened by Non-Owner, Folder Copied by Non-Owner, Folder Created by Non-Owner, Folder Deleted by Non-Owner, Folder Moved by Non-Owner, Folder Permanently Deleted by Non-Owner, Folder Renamed by Non-Owner, Calendar Opened by Non-Owner, Appointment Read by Non-Owner, Appointment Moved by Non-Owner, Appointment Permanently Deleted by Non-Owner, Appointment Modified by Non-Owner, Appointment Deleted by Non-Owner, Appointment Created by Non-Owner, Appointment Copied by Non-Owner, Inbox Opened by Non-Owner, Mailbox Opened by Non-Owner, Message Copied by Non-Owner, Message Created by Non-Owner, Message Deleted by Non-Owner, Message Modified by Non-Owner, Message Moved by Non-Owner, Message Permanently Deleted by Non-Owner, Message Read by Non-Owner

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Logon Activity

#### All Failed Logons in the last 7 days

Who = All Users

What = User failed to authenticate through Kerberos, User failed to authenticate through NTLM, User failed to log on interactively, User failed to log on interactively from a remote computer, User failed to perform a network logon from a remote computer

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## All Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively; User logged on interactively

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## All Kerberos Logons in the past 24 hours

Who = All Users

What = User authenticated through Kerberos, User failed to authenticate through Kerberos

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## All Logons in the past 24 hours

Who = All Users

What = Authentication Activity; Domain Controller Authentication; Logon Session

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## All NTLM Logons in the past 24 hours

Who = All Users

What = User authenticated through NTLM, User failed to authenticate through NTLM

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## All Remote Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively from a remote computer; User failed to perform a network logon from a remote computer; User logged on interactively from a remote computer; User performed a successful network logon from a remote computer

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All User Sessions in the past 24 hours

Who = All Users

What = Logon Session facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## SQL

### All SQL Add Roles, User, and Login Events in the last 24 hours

Who = All Users

What = Audit Add DB User; Audit Add Login; Audit Add Login to Server Role; Audit Add Member to DB Role; Audit Add Role

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### Audit Add Login

Who = All Users

What = Audit Add Login

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Login to Server Role

Who = All Users

What = Audit Add Login to Server Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Member to DB Role

Who = All Users

What = Audit Add Member to DB Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Role

Who = All Users

What = Audit Add Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Object

Who = All Users

What = Audit Alter Server Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Principal

Who = All Users

What = Audit Alter Server Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Password Management

## Domain Security

### Changes to Domain account policies (GPO filter) in last 30 days

Who = All Users

What = Account Lockout Duration Policy Changed; Account Lockout Threshold Policy Changed; Enforce Password History Policy Changed; Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Password Age Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed; Minimum Password Age Policy Changed; Minimum Password Length Policy Changed; Password Must Meet Complexity Requirements Policy Changed; Store Passwords Using Reversible Encryption Policy Changed; Reset Account Lockout Counter After Change Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to Domain Audit policies (GPO filter) in last 30 days

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Event Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to Domain Kerberos policies (GPO filter) in last 30 days

Who = All Users

What = Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### GPO Link changes on Domain objects in last 30 days

Who = All Users

What = DACL Changed on Group Policy Object; Group Policy Linked; Group Policy Unlinked; Group Policy Block Inheritance Setting Changed on Domain; Group Policy No Override Setting Changed on Domain; Group Policy Disabled Setting on Domain Changed; Owner Changed on Group Policy Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permission changes on domains in last 30 days

Who = All Users

What = DACL Changed on Domain Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions to AdminSDHolder Changes in last 30 days

Who = All Users

What = DACL Changed on AdminSDHolder Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Protect from Malicious Software

### File detailed list of services changes

Who = All Users

What = Service account changed, service dependencies changed, Service paused, Service recovery actions changed, Service resumed, Service start type changed, Service started, Service stopped

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Security Reminders

## Service Pack and Hotfixes

### Detailed list of all hot fixes applied

Who = All Users

What = Hotfix Applied

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of hot fixes rolled back

Who = All Users

What = Hotfix Rolled Back

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of service packs applied

Who = All Users

What = Computer Service Pack Applied; Domain Controller Service Pack Applied

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of service packs rolled back

Who = All Users

What = Domain Controller Service Pack Rolled Back

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# 164.310 – Physical Safeguards | Standard Workstation Security

### Detailed list of GPO workstation access modifications

Who = All Users

What = Deny Access to this Computer from the Network Policy Changed; Access this Computer from the Network Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of user workstation access modifications

Who = All Users

What = User userWorkstations Added; User userWorkstations Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# 164.310 – Physical Safeguards | Standard Workstation Use

### Detailed list of GPO disk access modifications

Who = All Users

What = Devices: Restrict CD-ROM Access to Locally Logged-on User Only Policy Changed; Devices: Allowed to Format and Eject Removable Media Policy Changed; Devices: Restrict Floppy Access to Locally Logged-Out User Only Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of hard disk modifications

Who = All Users

What = Disk Size Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of GPO workstation access modifications

Who = All Users

What = Deny Access to this Computer from the Network Policy Changed; Access this Computer from the Network Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# 164.312 – Technical Safeguards | Standard Person or entity authentication

## Defender

### All Defender events in last 30 days

Who = All Users

What = Defender facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member added to access node in last 30 days

Who = All Users

What = Member Added to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member removed from access node in last 30 days

Who = All Users

What = Member Removed from Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node added in last 30 days

Who = All Users

What = Defender Access Node Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node removed in last 30 days

Who = All Users

What = Defender Access Node Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender password events in last 30 days

Who = All Users

What = Defender Password Changed; Defender Password Cleared; Defender Password Expiry Cleared; Defender Password Expiry Set; Defender Password Set

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy added in last 30 days

Who = All Users

What = Defender Policy Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy change events in last 30 days

Who = All Users

What = Defender Policy Changed for Access Node; Defender Policy Changed for Group; Defender Policy Changed for Security Server; Defender Policy Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# 164.312 – Technical Safeguards | Standard Access Control

# Automatic Logoff

### Detailed list of Authentication modifications

Who = All Users

What = Deny Log On Locally Policy Changed; Deny Log On As a Service Policy Changed; Deny Access to this Computer from the Network Policy Changed; Allow Log On Through Terminal Services Policy Changed; Allow Log On Locally Policy Changed; Deny Log On As a Batch Job Policy Changed; Deny Log On Through Terminal Services/Remote Desktop Services Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of dial-in modifications

Who = All Users

What = User Dial-in Static Route Added; User Dial-in Static Route Removed; User Dial-in Callback Options Changed; User Dial-in Static IP Address Changed; User Dial-in Remote Access Permission Changed; User Dial-in Verify Caller ID Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of forced logoff modifications

Who = All Users

What = Network Security: Force Logoff When Logon Hours Expire Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of GPO workstation access modifications

Who = All Users

What = Deny Access to this Computer from the Network Policy Changed; Access this Computer from the Network Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

#### Detailed list of logon hours modifications

Who = All Users

What = User logonHours Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

#### Detailed list of user account policy modifications

Who = All Users

What = Maximum Password Age Policy Changed; Enforce Password History Policy Changed; Account Lockout Threshold Policy Changed; Account Lockout Duration Policy Changed; Enforce User Logon Restrictions Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

#### Detailed list of user workstation modifications

Who = All Users

What = User userWorkstations Added; User userWorkstations Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Unique User Identification

### Authentication Services

#### Users set to UNIX-enabled and created in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## 164.312 – Technical Safeguards | Standard Audit Control

#### (Executive Summary) – 164.312(b) – Audit Controls

A summary report containing events from all of the following reports.

#### Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled; Change Auditor Agent Connected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of critical group membership modifications

Who = All Users

What = Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group; Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Object Policy Changed; Audit: Audit the use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audit Policy Changed; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Payment Card Industry

The reports are available under the following folders:

- Build and Maintain a Secure Network and Systems
- Implement Strong Access Control Measures
- Maintain a Vulnerability Management Program
- Regularly Monitor and Test Networks

# Build and Maintain a Secure Network and Systems

# R1 - Establish firewall and router configuration standards

## Authentication Services

### Authentication Services computers added in the last 30 days

Who = All Users

What = Authentication Services Computer Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Authentication Services computers deleted in the last 30 days

Who = All Users

What = Authentication Services Computer Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Computer Activity

### Computers added in the last 30 days

Who = All Users

What = Computer Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers disabled in the last 30 days

Who = All Users

What = Computer Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers enabled in the last 30 days

Who = All Users

What = Computer Account Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers moved in the last 30 days

Who = All Users

What = Computer Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers removed in the last 30 days

Who = All Users

What = Computer Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers renamed in the last 30 days

Who = All Users

What = Computer Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Detailed list of file system modifications

Who = All Users

What = Custom File System Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of interactive login policy modifications

Who = All Users

What = Interactive Logon: Do Not Display Last Name Policy Changed; Interactive Logon: Do Not Require CTRL+ALT+DEL Policy Changed; Interactive Logon: Message Text for Users Attempting to Log on Policy Changed; Interactive Logon: Message Title for Users Attempting to Log On Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of NETLOGON modifications

Who = All Users

What = NETLOGON Services facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of service changes

Who = All Users

What = Service Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of software installations via GPO added

Who = All Users

What = Computer Software Installation Policy Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of software installations via GPO modified

Who = All Users

What = Computer Software Installation Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of software installations via GPO removed

Who = All Users

What = Computer Software Installation Policy Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Domain Controller Security

### All Basic Domain Controller changes in last 30 days

Who = All Users

What = Append Parent Suffixes Option Changed; Connection DNS Registration Option Changed; Connection-Specific DNS Suffixes Changed; Contents of DNS Server List Changed; Contents of DNS Suffix List Changed; Default Gateway Changed; DHCP Enabled; DHCP Disabled; Disk Size Changed; IP Deny List Entry Added; IP Deny List Entry Removed; IPSEC Settings Changed; Memory Amount Changed; NIC Added; NIC Removed; Processor Speed Changed; Raw IP Allowed Protocols List Changed; Static IP Address Changed; Subnet Mask Changed; Use Connection Suffix in DNS Registration Option Changed; Use of Dynamic DNS Changed; Use Primary and Connection Specific Suffixes Flag Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Allow raw IP allowed protocols list changed in last 30 days

Who = All Users

What = Raw IP Allowed Protocols List Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Changes to DNS settings in last 30 days

Who = All Users

What = DHCP Enabled; DHCP Disabled; Static IP Address Changed; Subnet Mask Changed; Default Gateway Changed; Contents of DNS Server List Changed; Use Primary and Connection Specific Suffixes Flag Changed; Append Parent Suffixes Option Changed; Connection Specific DNS Suffix Changed; Contents of DNS Suffix List Changed; Use Connection Suffix in DNS Registration Option Changed; Connection DNS Registration Option Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Changes to IP deny filter changes in last 30 days

Who = All Users

What = IP Deny List Entry Added; IP Deny List Entry Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to IP settings in last 30 days

Who = All Users

What = Append Parent Suffixes Option Changed; Connection DNS Registration Option Changed; Connection-Specific DNS Suffix Changed; Contents of DNS Server List Changed; Contents of DNS Suffix List Changed; Default Gateway Changed; DHCP Enabled; DHCP Disabled; Static IP Address Changed; Subnet Mask Changed; Use Primary and Connection-Specific Suffixes Flag Changed; Use Connection Suffix in DNS Registration Option Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Default gateway changes in last 30 days

Who = All Users

What = Default Gateway Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### DHCP disabled in last 30 days

Who = All Users

What = DHCP Disabled

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### DHCP enabled in last 30 days

Who = All Users

What = DHCP Enabled

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Disk size changes in last 30 days

Who = All Users

What = Disk Size Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### DNS server list changes in last 30 days

Who = All Users

What = Contents of DNS Server List Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Domain Controllers moved in last 30 days

Who = All Users

What = Domain Controller Moved to Another OU

Where = All sources

When = Last 30 days

Origin = All domain controllers

### Domain Controllers renamed in last 30 days

Who = All Users

What = Domain Controller Renamed

Where = All sources

When = Last 30 days

Origin = All domain controllers

### Global Catalog added to Domain Controller in last 30 days

Who = All Users

What = GC Added

Where = All sources

When = Last 30 days

Origin = All domain controllers

### Global Catalog removed from Domain Controller in last 30 days

Who = All Users

What = GC Removed

Where = All sources

When = Last 30 days

Origin = All domain controllers

### IPSec changes in last 30 days

Who = All Users

What = IPSEC Settings Changed

Where = All sources

When = Last 30 days

Origin = All domain controllers

### NIC added/removed in last 30 days

Who = All Users

What = NIC Added; NIC Removed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Static IP address changes in last 30 days

Who = All Users

What = Static IP Address Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Subnet mask changes in last 30 days

Who = All Users

What = Subnet Mask Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### TCP/IP allowed in last 30 days

Who = All Users

What = IP Deny List Entry Added; IP Deny List Entry Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Use of dynamic DNS changed in last 30 days

Who = All Users

What = Use of Dynamic DNS Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

## Exchange

### OWA Website Added to Server

Who = All Users

What = OWA Web Site Added to Server

Where = All sources

When = Last 7days

Origin = All workstations/servers

### OWA Website Removed from the Server

Who = All Users

What = OWA Web Site Removed from Server

Where = All sources

When = Last 7days

Origin = All workstations/servers

### OWA Website Renamed

Who = All Users

What = OWA Web Site Renamed on Server

Where = All sources

When = Last 7days

Origin = All workstations/servers

## Trust Activity

### Cross Forest level trust added in last 30 days

Who = All Users

What = Cross-forest Trust Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Cross Forest level trust deleted in last 30 days

Who = All Users

What = Cross-forest Trust Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Trusts added in last 30 days

Who = All Users

What = Trust Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Trusts deleted in last 30 days

Who = All Users

What = Trust Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# R2 - Do not use vendor-supplied defaults for system passwords and other security parameters

## Authentication Services

### Authentication Services GPO Settings Changes in the last 30 days

Who = All Users

What = Authentication Services GPO Settings Computer Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Critical GPO Changes

### Default domain audit policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Event Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Default domain Kerberos policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Default domain password policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Enforce Password History Policy Changed; Maximum Password Age Policy Changed; Minimum Password Age Policy Changed; Minimum Password Length Policy Changed; Password Must Meet Complexity Requirements Policy Changed; Store Passwords Using Reversible Encryption Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Detailed list of GPO modifications

Who = All Users

What = Accounts: Administrator Account Status Policy Changed; Accounts: Guest Account Status Policy Changed; Accounts: Limit Local Account Use of Blank Passwords to Console Only Policy Changed; Accounts: Rename Administrator Account Policy Changed; Accounts: Rename Guest Account Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit: Audit the User of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed; Devices: Allow Undock Without Having to Logon Policy Changed; Devices: Allowed to Format and Eject Removable Media Policy Changed; Devices: Prevent Users from Installing Printer Drivers Policy Changed; Devices: Restrict CD-ROM Access to Locally Logged-on User Only Policy Changed; Devices: Restrict Floppy Access to Locally Logged-on User Only Policy Changed; Devices: Unsigned Driver Installation Behavior Policy Changed; Domain Controller: Allow Server Operators to Schedule Tasks Policy Changed; Domain Controller: LDAP Server Signing Requirements Policy Changed; Domain Controller: Refuse Machine Account Password Changes Policy Changed; Domain Member: Digitally Encrypt or Sign Secure Channel Data (Always) Policy Changed; Enforce Password History Policy Changed; Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; System Objects: Strengthen Default Permissions of Global System Objects Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Domain policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Linked Group Policy or Domain Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Domain Security

### Changes to Domain account policies (GPO filter) in last 30 days

Who = All Users

What = Account Lockout Duration Policy Changed; Account Lockout Threshold Policy Changed; Enforce Password History Policy Changed; Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Password Age Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed; Minimum Password Age Policy Changed; Minimum Password Length Policy Changed; Password Must Meet Complexity Requirements Policy Changed; Store Passwords Using Reversible Encryption Policy Changed; Reset Account Lockout Counter After Change Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to Domain Audit policies (GPO filter) in last 30 days

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Event Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to Domain Kerberos policies (GPO filter) in last 30 days

Who = All Users

What = Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### GPO Link changes on Domain objects in last 30 days

Who = All Users

What = DACL Changed on Group Policy Object; Group Policy Linked; Group Policy Unlinked; Group Policy Block Inheritance Setting Changed on Domain; Group Policy No Override Setting Changed on Domain; Group Policy Disabled Setting on Domain Changed; Owner Changed on Group Policy Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permission changes on domains in last 30 days

Who = All Users

What = DACL Changed on Domain Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions to AdminSDHolder Changes in last 30 days

Who = All Users

What = DACL Changed on AdminSDHolder Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Exchange

### All ActiveSync Mailbox Policy Events

Who = All Users

What = ActiveSync Mailbox Policy Added to Organization Client Access Configuration; ActiveSync Mailbox Policy Allow Attachments to be Downloaded Option Changed; ActiveSync Mailbox Policy Allow Non-Provisionable Devices Options Changed; ActiveSync Mailbox Policy Allow Simple Password Option Changed; ActiveSync Mailbox Policy Enable Password Recovery Option Changed; ActiveSync Mailbox Policy Maximum Attachment Size Changed; ActiveSync Mailbox Policy Minimum Password Length Changed; ActiveSync Mailbox Policy Password Expiration Changed; ActiveSync Mailbox Policy Password History Changed; ActiveSync Mailbox Policy Password Required Option Changed; ActiveSync Mailbox Policy Removed from Organization Client Access Configuration; ActiveSync Mailbox Policy Renamed; ActiveSync Mailbox Policy Require Alphanumeric Password Option Changed; ActiveSync Mailbox Policy Require Encryption On Device Option Changed; ActiveSync Mailbox Policy User Idle Timeout Changed; ActiveSync Mailbox Policy Windows File Shares Access Option Changed; ActiveSync Mailbox Policy Windows SharePoint Services Access Option Changed; ActiveSync Mailbox Policy Number of Failed Attempts Allowed Changed; ActiveSync Mailbox Policy Refresh Interval Changed; ActiveSync Mailbox Policy Require Encryption On Device Option Changed; Mobile Device - ActiveSync Device Policy

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Email Address Policy Events

Who = All Users

What = Email Address Policy Added to Organization Configuration; Email Address Policy Email Address Filter List Changed; Email Address Policy Priority Changed; Email Address Policy Query Filter Changed; Email Address Policy Removed from Organization Configuration; Email Address Policy Renamed; Email Address Policy Storage Filter Changed; Distribution List - Email Address Policy Enabled Changed; Mailbox - Email Address Policy Enabled Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Permission Tracking Events

Who = All Users

What = Exchange Permission Tracking facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Journaling Rule Change Events

Who = All Users

What = Journaling Rule Added to Organization Configuration; Journaling Rule Changed; Journaling Rule Removed from Organization Configuration; Journaling Rule Renamed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Deleted Items Retention Period Changed for a user

Who = All Users

What = Deleted Item Retention Period Changed; Deleted Item Retention Use Defaults Storage Option Changed; Mailbox - End Date Retention Hold; Mailbox - Retention Hold Enabled; Mailbox - Retention Policy; Mailbox - Start Date for Retention Hold; Mailbox - Use Database Retention Defaults

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Message Tracking Options Changed on an Exchange 2007 Server

Who = All Users

What = Message Tracking Option Changed on Server

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Organizational Unit Management

### Organizational Units added in last 30 days

Who = All Users

What = Subordinate OU Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units deleted in last 30 days

Who = All Users

What = Subordinate OU Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units renamed in last 30 days

Who = All Users

What = Subordinate OU Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units set to block GPO inheritance in last 30 days

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Group Policy Changed last 30 days

### Group Policy block inheritance changes

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU; Group Policy Block Inheritance Setting Changed on Site; Group Policy Block Inheritance Setting Changed on Domain

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group Policy disabled setting changes

Who = All Users

What = Group Policy Disabled Setting on OU Changed; Group Policy Disabled Setting on Site Changed; Group Policy Disabled Setting on Domain Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group Policy no override changes

Who = All Users

What = Group Policy No Override Setting Changed on OU; Group Policy No Override Setting Changed on Site; Group Policy No Override Setting Changed on Domain

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Implement Strong Access Control Measures

# Requirement 7: Restrict access to cardholder data by business need to know

## Access Control - File System

### Directory shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Directory shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder added in last 30 days

Who = All Users

What = File Created; Folder Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder attribute changed in last 30 days

Who = All Users

What = File Attribute Changed; Folder Attribute Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder auditing changed in last 30 days

Who = All Users

What = File Auditing Changed; Folder Auditing Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder modified date changed in last 30 days

Who = All Users

What = File Last Write Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder moved in last 30 days

Who = All Users

What = File Moved; Folder Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder ownership changed in last 30 days

Who = All Users

What = File Ownership Changed; Folder Ownership Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder permission changed in last 30 days

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder removed in last 30 days

Who = All Users

What = File Deleted; Folder Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder renamed in last 30 days

Who = All Users

What = File Renamed; Folder Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share added in last 30 days

Who = All Users

What = Local Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share permission changed in last 30 days

Who = All Users

What = Local Share Permissions Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share removed in last 30 days

Who = All Users

What = Local Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Authentication Services

### Authentication Services computers added in last 30 days

Who = All Users

What = Authentication Services Computer object added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Authentication Services computers deleted in last 30 days

Who = All Users

What = Authentication Services Computer object deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Groups set to UNIX-disabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for Group - Restriction = To: Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Groups set to UNIX-enabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for Group - Restriction = To: Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX home directory changed in last 30 days

Who = All Users

What = UNIX Home Directory Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX login shell changed in last 30 days

Who = All Users

What = UNIX Login Shell Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX-enabled groups deleted in last 30 days

Who = All Users

What = UNIX-Enabled Group Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### UNIX-enabled users deleted in last 30 days

Who = All Users

What = UNIX-Enabled User Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users set to UNIX-disabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User - Restriction = To: Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users set to UNIX-enabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User - Restriction = To: Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Defender

### All Defender events in last 30 days

Who = All Users

What = Defender facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member added to access node in last 30 days

Who = All Users

What = Member Added to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member removed from access node in last 30 days

Who = All Users

What = Member Removed from Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node added in last 30 days

Who = All Users

What = Defender Access Node Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node removed in last 30 days

Who = All Users

What = Defender Access Node Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender password events in last 30 days

Who = All Users

What = Defender Password Changed; Defender Password Cleared; Defender Password Expiry Cleared; Defender Password Expiry Set; Defender Password Set

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy added in last 30 days

Who = All Users

What = Defender Policy Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy change events in last 30 days

Who = All Users

What = Defender Policy Changed for Access Node; Defender Policy Changed for Group; Defender Policy Changed for Security Server; Defender Policy Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy removed in last 30 days

Who = All Users

What = Defender Policy Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload added in last 30 days

Who = All Users

What = Defender RADIUS Payload Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload change events in last 30 days

Who = All Users

What = Defender RADIUS Payload Changed for Access Node; Defender RADIUS Payload Changed for Group; Defender RADIUS Payload Changed for Security Server; Defender RADIUS Payload Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload removed in last 30 days

Who = All Users

What = Defender RADIUS Payload Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server added in last 30 days

Who = All Users

What = Defender Security Server Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server assigned to access node in last 30 days

Who = All Users

What = Defender Security Server Assigned to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server removed in last 30 days

Who = All Users

What = Defender Security Server Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server unassigned from access node in last 30 days

Who = All Users

What = Defender Security Server Unassigned from Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender temporary response events in last 30 days

Who = All Users

What = Defender Token Temporary Response Cleared; Defender Token Temporary Response Set; Defender Token Temporary Response Usage Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token added in last 30 days

Who = All Users

What = Defender Token Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token assigned in last 30 days

Who = All Users

What = Defender Token Assigned

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token PIN events in last 30 days

Who = All Users

What = Defender Token PIN Changed; Defender Token PIN Cleared; Defender Token PIN Expiry Cleared; Defender Token PIN Expiry Set; Defender Token PIN Set

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token removed in last 30 days

Who = All Users

What = Defender Token Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token unassigned in last 30 days

Who = All Users

What = Defender Token Unassigned

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Dynamic Access Control - DAC

### File central access policy changed

Who = All Users

What = File central access policy changed

Where = All sources

When = Last 7days

Origin = All workstations/servers

## EMC

### EMC file access rights changed

Who = All Users

What = EMC file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents written

Who = All Users

What = EMC file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents created

Who = All Users

What = EMC file contents created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents deleted

Who = All Users

What = EMC file contents deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents moved

Who = All Users

What = EMC file contents moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents opened

Who = All Users

What = EMC file contents opened

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file ownership changed

Who = All Users

What = EMC file ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file renamed

Who = All Users

What = EMC file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder access rights changed

Who = All Users

What = EMC folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder created

Who = All Users

What = EMC folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder deleted

Who = All Users

What = EMC folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder moved

Who = All Users

What = EMC folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder ownership changed

Who = All Users

What = EMC folder ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder renamed

Who = All Users

What = EMC folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## Exchange

### All Exchange Administrative Group Events

Who = All Users

What = Exchange Administrative Group facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Distribution List (Group) Events

Who = All Users

What = Exchange Security Group facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Permission Tracking Events

Who = All Users

What = Exchange Permission Tracking facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Group Management

### Group added in last 30 days

Who = All Users

What = Group Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group deleted in last 30 days

Who = All Users

What = Group Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member added changes in last 30 days

Who = All Users

What = Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member removed changes in last 30 days

Who = All Users

What = Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group moved in last 30 days

Who = All Users

What = Group Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member added changes in last 30 days

Who = All Users

What = Nested Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member removed changes in last 30 days

Who = All Users

What = Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group permissions changed in last 30 days

Who = All Users

What = DACL Changed on Group Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed (SAM account name) changes in last 30 days

Who = All Users

What = Group samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed in last 30 days

Who = All Users

What = Group Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group type changes in last 30 days

Who = All Users

What = Group Type Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## NetApp

### NetApp file access rights changed (no from-value)

Who = All Users

What = NetApp file access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file access rights changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file contents written

Who = All Users

What = NetApp file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file created

Who = All Users

What = NetApp file created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file deleted

Who = All Users

What = NetApp file deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file moved

Who = All Users

What = NetApp file moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file opened

Who = All Users

What = NetApp file opened

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed (no from-value)

Who = All Users

What = NetApp file access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file renamed

Who = All Users

What = NetApp file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder created

Who = All Users

What = NetApp folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder deleted

Who = All Users

What = NetApp folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder moved

Who = All Users

What = NetApp folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder renamed

Who = All Users

What = NetApp folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## SharePoint

### Permission changes in the last 7 days

Who = All Users

What = All permission levels revoked; Permission level created; Permission level deleted; Permission level granted; Permission level permissions modified; Permission level revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Permission inheritance changes in the last 7 days

Who = All Users

What = Permission inheritance broken; Permission inheritance restored; Permission level inheritance broken; Permission level permissions modified

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups created and deleted in the last 7 days

Who = All Users

What = Security group created; Security group deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups membership changes in the last 7 days

Who = All Users

What = Member added to security group; Member removed from security group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection ownership changes in the last 7 days

Who = All Users

What = Site collection ownership granted; Site collection ownership revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collections created and deleted in the last 7 days

Who = All Users

What = Site collection created; Site collection deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Sites created and deleted in the last 7 days

Who = All Users

What = Site created; Site deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Sites moved in the last 7 days

Who = All Users

What = Site moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## SQL

### All SQL Add Roles, User, and Login Events in the last 24 hours

Who = All Users

What = Audit Add DB User; Audit Add Login; Audit Add Login to Server Role; Audit Add Member to DB Role; Audit Add Role

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### Audit Add Login

Who = All Users

What = Audit Add Login

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Login to Server Role

Who = All Users

What = Audit Add Login to Server Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Member to DB Role

Who = All Users

What = Audit Add Member to DB Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Role

Who = All Users

What = Audit Add Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Database

Who = All Users

What = Audit Alter Database

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Database Object

Who = All Users

What = Audit Alter Database Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Database Principal

Who = All Users

What = Audit Alter Database Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Object Derived Permission

Who = All Users

What = Audit Alter Object Derived Permission

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Schema Object

Who = All Users

What = Audit Alter Schema Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Object

Who = All Users

What = Audit Alter Server Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Principal

Who = All Users

What = Audit Alter Server Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Drop Database

Who = All Users

What = Audit Drop Database

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Drop DB User

Who = All Users

What = Audit Drop DB User

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## User Activity

### Users disabled in last 30 days

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users expiration date changed in last 30 days

Who = All Users

What = User Account Expires changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users locked in last 30 days

Who = All Users

What = User Account Locked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users unlocked in last 30 days

Who = All Users

What = User Account Unlocked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## User Management

### Changes to user profiles in last 30 days

Who = All Users

What = Home Folder Changed on User Object; Home Folder Mapped Drive Changed on User Object; Level of Control Changed for User Object; Primary Group ID Changed for User Object; Profile Path Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions on user accounts changed in last 30 days

Who = All Users

What = DACL Changed on User Object; Required User’s Permissions Changed for User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users added in last 30 days

Who = All Users

What = User Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users added to group in last 30 days

Who = All Users

What = User Member-of Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users deleted in last 30 days

Who = All Users

What = User Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users disabled in last 30 days

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users display name changed in last 30 days

Who = All Users

What = Display Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users enabled in last 30 days

Who = All Users

What = User Account Enabled; User Account Re-enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users first name changed in last 30 days

Who = All Users

What = First Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users last name changed in last 30 days

Who = All Users

What = Last Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users locked out in last 30 days

Who = All Users

What = User Account Locked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users logon hours changed in last 30 days

Who = All Users

What = User logonHours Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users moved in last 30 days

Who = All Users

What = User Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users name(s) changed in last 30 days

Who = All Users

What = Display Name Changed on User Object; First Name Changed on User Object; User samAccountName Changed; Last Name Changed on User Object; User userPrincipal Name Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users principal name changed in last 30 days

Who = All Users

What = User userPrincipalName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users removed from group in last 30 days

Who = All Users

What = User Member-of Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users renamed in last 30 days

Who = All Users

What = Domain User Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users SAM account name changed in last 30 days

Who = All Users

What = User samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users status changed in last 30 days (Enabled, Disabled, Created, Deleted, Locked, Unlocked)

Who = All Users

What = User Account Enabled; User Account Disabled; User Object Added; User Object Removed; User Account Locked; User Account Unlocked; User Account Re-enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users unlocked in last 30 days

Who = All Users

What = User Account Unlocked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users workstation access restrictions changed in last 30 days

Who = All Users

What = User userWorkstations Added; User userWorkstations Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# R8 - Identify and authenticate access to system components

## Defender

### All Defender events in last 30 days

Who = All Users

What = Defender facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member added to access node in last 30 days

Who = All Users

What = Member Added to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member removed from access node in last 30 days

Who = All Users

What = Member Removed from Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node added in last 30 days

Who = All Users

What = Defender Access Node Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node removed in last 30 days

Who = All Users

What = Defender Access Node Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender password events in last 30 days

Who = All Users

What = Defender Password Changed; Defender Password Cleared; Defender Password Expiry Cleared; Defender Password Expiry Set; Defender Password Set

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy added in last 30 days

Who = All Users

What = Defender Policy Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy change events in last 30 days

Who = All Users

What = Defender Policy Changed for Access Node; Defender Policy Changed for Group; Defender Policy Changed for Security Server; Defender Policy Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy removed in last 30 days

Who = All Users

What = Defender Policy Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload added in last 30 days

Who = All Users

What = Defender RADIUS Payload Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload change events in last 30 days

Who = All Users

What = Defender RADIUS Payload Changed for Access Node; Defender RADIUS Payload Changed for Group; Defender RADIUS Payload Changed for Security Server; Defender RADIUS Payload Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload removed in last 30 days

Who = All Users

What = Defender RADIUS Payload Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server added in last 30 days

Who = All Users

What = Defender Security Server Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server assigned to access node in last 30 days

Who = All Users

What = Defender Security Server Assigned to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server removed in last 30 days

Who = All Users

What = Defender Security Server Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server unassigned from access node in last 30 days

Who = All Users

What = Defender Security Server Unassigned from Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender temporary response events in last 30 days

Who = All Users

What = Defender Token Temporary Response Cleared; Defender Token Temporary Response Set; Defender Token Temporary Response Usage Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token added in last 30 days

Who = All Users

What = Defender Token Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token assigned in last 30 days

Who = All Users

What = Defender Token Assigned

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token PIN events in last 30 days

Who = All Users

What = Defender Token PIN Changed; Defender Token PIN Cleared; Defender Token PIN Expiry Cleared; Defender Token PIN Expiry Set; Defender Token PIN Set

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token removed in last 30 days

Who = All Users

What = Defender Token Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token unassigned in last 30 days

Who = All Users

What = Defender Token Unassigned

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Maintain a Vulnerability Management Program

# R5 - Protect all systems against malware and regularly update ant-virus software or programs

**Detailed list of service changes**

Who = All Users

What = Service Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# R6 - Develop and maintain secure systems and applications

## Service Packs and Hot Fixes

**Detailed list of all hot fixes applied**

Who = All Users

What = Hotfix Applied

Where = All sources

When = Last 7 days

Origin = All workstations/servers

**Detailed list of hot fixes rolled back**

Who = All Users

What = Hotfix Rolled Back

Where = All sources

When = Last 7 days

Origin = All workstations/servers

**Detailed list of service packs applied**

Who = All Users

What = Computer Service Pack Applied; Domain Controller Service Pack Applied

Where = All sources

When = Last 7 days

Origin = All workstations/servers

**Detailed list of service packs rolled back**

Who = All Users

What = Domain Controller Service Pack Rolled Back

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Regularly Monitor and Test Networks

# R10 - Track and monitor all access to network resources and cardholder data

### Detailed list of audit policy modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Object Policy Changed; Audit: Audit the use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audit Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Connected; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of Change Auditor security group modifications

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group; Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of critical group membership modifications

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group; Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of DACL modifications

Who = All Users

What = DACL Changed on AdminSDHolder Object; DACL Changed on Domain Object; DACL Changed on Exchange Group Object (Exchange 2003); DACL Changed on Group Object; DACL Changed on Group Policy Object; DACL Changed on OU Object; DACL Changed on User Object; DACL Changed on Computer Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of file system permission modifications

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed; Local Share Permissions Changed; SYSVOL Folder Access Rights Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of nested group membership modifications

Who = All Users

What = Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group; Nested Member Added to Group; Nested Member Removed from Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Object Policy Changed; Audit: Audit the use of Backup and Restore Privilege Policy Changed; Crash on Audit Fail Policy Changed; Security Audit Log Rolled Over; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Access Control - File System

### Directory shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Directory shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File Access Denied NTFS

Who = All Users

What = Failed File Access (FTFS Permissions)

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### File Access Denied Change Auditor Lockdown

Who = All Users

What = Failed File Access

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### File/Folder added in last 30 days

Who = All Users

What = File Created; Folder Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder attribute changed in last 30 days

Who = All Users

What = File Attribute Changed; Folder Attribute Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder auditing changed in last 30 days

Who = All Users

What = File Auditing Changed; Folder Auditing Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder modified date changed in last 30 days

Who = All Users

What = File Last Write Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder moved in last 30 days

Who = All Users

What = File Moved; Folder Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder ownership changed in last 30 days

Who = All Users

What = File Ownership Changed; Folder Ownership Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder permission changed in last 30 days

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder removed in last 30 days

Who = All Users

What = File Deleted; Folder Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder renamed in last 30 days

Who = All Users

What = File Renamed; Folder Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Folder Access Denied NTFS

Who = All Users

What = Failed Folder Access (FTFS Permissions)

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Folder Access Denied Change Auditor Lockdown

Who = All Users

What = Failed Folder Access

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Local share added in last 30 days

Who = All Users

What = Local Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share auditing changed in last 30 days

Who = All Users

What = Local Share Auditing changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share permission changed in last 30 days

Who = All Users

What = Local Share Permissions Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share removed in last 30 days

Who = All Users

What = Local Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Share Access Denied NTFS

Who = All Users

What = Failed Share Access (FTFS Permissions)

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Share Access Denied Change Auditor Lockdown

Who = All Users

What = Failed Share Access

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Change Auditor Internal Auditing

### CEPP Configuration changed

Who = All Users

What = CEPP configuration changed

Where = All sources

When = This Week

Origin = All workstations/servers

## Dynamic Access Control - DAC

### File Classification changed

Who = All Users

What = File classification changed

Where = All sources

When = This week

Origin = All workstations/servers

## EMC

### EMC file access rights changed

Who = All Users

What = EMC file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents written

Who = All Users

What = EMC file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents created

Who = All Users

What = EMC file contents created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents deleted

Who = All Users

What = EMC file contents deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents moved

Who = All Users

What = EMC file contents moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents opened

Who = All Users

What = EMC file contents opened

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file ownership changed

Who = All Users

What = EMC file ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file renamed

Who = All Users

What = EMC file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder access rights changed

Who = All Users

What = EMC folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder created

Who = All Users

What = EMC folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder deleted

Who = All Users

What = EMC folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder moved

Who = All Users

What = EMC folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder ownership changed

Who = All Users

What = EMC folder ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder renamed

Who = All Users

What = EMC folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## Logon Activity

### All Failed Logons in the last 7 days

Who = All Users

What = User failed to authenticate through Kerberos, User failed to authenticate through NTLM, User failed to log on interactively, User failed to log on interactively from a remote computer, User failed to perform a network logon from a remote computer

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively; User logged on interactively

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Kerberos Logons in the past 24 hours

Who = All Users

What = User authenticated through Kerberos, User failed to authenticate through Kerberos

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Logons in the past 24 hours

Who = All Users

What = Authentication Activity; Domain Controller Authentication; Logon Session

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All NTLM Logons in the past 24 hours

Who = All Users

What = User authenticated through NTLM, User failed to authenticate through NTLM

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All Remote Interactive Logons in the past 24 hours

Who = All Users

What = User failed to log on interactively from a remote computer; User failed to perform a network logon from a remote computer; User logged on interactively from a remote computer; User performed a successful network logon from a remote computer

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All User Sessions in the past 24 hours

Who = All Users

What = Logon Session facility

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

## NetApp

### NetApp file access rights changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file access rights (no from value)

Who = All Users

What = NetApp file access rights (no from value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file contents written

Who = All Users

What = NetApp file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file created

Who = All Users

What = NetApp file created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file deleted

Who = All Users

What = NetApp file deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file moved

Who = All Users

What = NetApp file moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file opened

Who = All Users

What = NetApp file opened

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed (no from value)

Who = All Users

What = NetApp file access rights changed (no from value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file renamed

Who = All Users

What = NetApp file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder created

Who = All Users

What = NetApp folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder deleted

Who = All Users

What = NetApp folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder moved

Who = All Users

What = NetApp folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed (no from value)

Who = All Users

What = NetApp folder access rights changed (no from value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder renamed

Who = All Users

What = NetApp folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## SharePoint

### Document Content changes in the last 7 days

Who = All Users

What = Document added; Document check out canceled; Document checked in; Document checked out; Document deleted; Document metadata updated; Document updated

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Document Story changes in the last 7 days

Who = All Users

What = Document library restored from recycle bin; Document metadata updated; Document moved; Document renamed; Document restored from recycle bin; Document updated; Document version deleted; Document viewed; SharePoint folder deleted; SharePoint folder moved; SharePoint folder renamed; SharePoint folder restored from recycle bin; SharePoint folder updated; Site collection deleted; Site deleted; Site moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Document Version changes in the last 7 days

Who = All Users

What = All document versions deleted; Document version deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### List Item changes in the last 7 days

Who = All Users

What = All list item versions deleted; List item added; List item attachment added; List item attachment deleted; List item deleted; List item restored from recycle bin; List item updated; List item version deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## SQL

### All SQL Errors and Warning events in the last 24 hours

Who = All Users

What = SQL Errors and Warnings Event

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

# SAS 70 (Statement on Auditing Standards, Service Organizations)

The SAS 70 reports are located under the following folder:

- Service Auditor’s Reports: Type I

## Service Auditor’s Reports: Type I

### (Executive Summary) – Service Auditor’s Report Type I

A summary report containing events from all of the following reports.

### Service Auditor’s Report Type I – Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service Has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Connected; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Service Auditor’s Report Type I – Detailed list of Change Auditor Internal Controls modifications

Who = All Users

What = Change Auditor Internal Auditing facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Service Auditor’s Report Type I – Detailed list of critical group membership modifications

Who = All Users

What = Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group; Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Service Auditor’s Report Type I – Detailed list of file system permission modifications

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed; Local Share Permissions Changed; SYSVOL Folder Access Rights Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Service Auditor’s Report Type I – Detailed list of GPO modifications

Who = All Users

What = Group Policy Item facility; Group Policy Object facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Service Auditor’s Report Type I – Detailed list of interactive login policy modifications

Who = All Users

What = Interactive Logon: Message Title for Users Attempting to Log On Changed; Interactive Logon: Do Not Require CTRL+ALT+DEL Policy Changed; Interactive Logon: Message Text for Users Attempting to Log On Policy Changed; Interactive Logon: Do Not Display Last User Name Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Service Auditor’s Report Type I – Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Object Policy Changed; Audit: Audit the use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audit Policy Changed; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# SOX (Sarbanes-Oxley General IT Controls Evidence based on the COBIT Framework)

The SOX reports are available under the following folders:

- Section 404 | Acquisition and Implementation
- Section 404 | Delivery and Support
- Section 404 | Planning and Organization

## Section 404 | Acquisition and Implementation

The Acquisition and Implementation reports are available under the following folders:

- BAI2.1 - Define and maintain business functional and technical requirements
- BAI2.2 - Perform a feasibility study and formulate alternative solutions
- BAI3.10 – Maintain solutions
  - Authentication Services
  - Computer Activity
  - Exchange
- BAI3.9 – Manage changes to requirements
- BAI6.1 – Evaluate, prioritize and authorize change requests
  - Organizational Unit Management
- BAI6.2 – Manage emergency changes
  - Organizational Unit Management
- BAI6.3 – Track and report change status
  - Organizational Unit Management
- BAI7.5 - Perform acceptance tests
- BAI7.6 - Promote to production and manage releases
- BAI7.8 – Perform a post-implementation review

## BAI2.1 - Define and maintain business functional and technical requirements

## BAI2.2 - Perform a feasibility study and formulate alternative solutions

### (Executive Summary) Identify Automated Solutions

A summary report containing events from all of the following reports.

### Detailed list of all registry changes

Who = All Users

What = Registry subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of all schema changes

Who = All Users

What = Schema Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of service changes

Who = All Users

What = Service Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## BAI3.10 – Maintain solutions

### (Executive Summary) BAI3.10 - Acquire and Maintain Technology Infrastructure

A summary report containing events from all of the following reports.

### (Executive Summary) BAI3.10 - Acquire and Maintain Application Software

A summary report containing events from all of the following reports.

### BAI3.10 – Detailed list of all hot fixes applied

Who = All Users

What = Hotfix Applied

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.10 – Detailed list of all registry changes

Who = All Users

What = Registry subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.10 – Detailed list of hot fixes rolled back

Who = All Users

What = Hotfix Rolled Back

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.10 – Detailed list of schema modifications

Who = All Users

What = Schema Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.10 – Detailed list of service packs applied

Who = All Users

What = Computer Service Pack Applied

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.10 – Detailed list of service packs rolled back

Who = All Users

What = Computer Service Pack Rolled Back

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.10 – Detailed list of software installations via GPO added

Who = All Users

What = Computer Software Installation Policy Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.10 – Detailed list of software installations via GPO modified

Who = All Users

What = Computer Software Installation Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.10 – Detailed list of software installations via GPO removed

Who = All Users

What = Computer Software Installation Policy Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Authentication Services

### BAI3.10 – Authentication Services computers added in the last 30 days

Who = All Users

What = Authentication Services Computer Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### BAI3.10 – Authentication Services computers deleted in the last 30 days

Who = All Users

What = Authentication Services Computer Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Computer Activity

### BAI3.10 – Computers added in the last 30 days

Who = All Users

What = Computer Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### BAI3.10 – Computers disabled in the last 30 days

Who = All Users

What = Computer Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### BAI3.10 – Computers enabled in the last 30 days

Who = All Users

What = Computer Account Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### BAI3.10 – Computers moved in the last 30 days

Who = All Users

What = Computer Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### BAI3.10 – Computers removed in the last 30 days

Who = All Users

What = Computer Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### BAI3.10 – Computers renamed in the last 30 days

Who = All Users

What = Computer Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Exchange

### BAI3.10 – OWA Website Added to Server

Who = All Users

What = OWA Web Site Added to Server

Where = All sources

When = Last 7days

Origin = All workstations/servers

### BAI3.10 – OWA Website Removed from the Server

Who = All Users

What = OWA Web Site Removed from Server

Where = All sources

When = Last 7days

Origin = All workstations/servers

### BAI3.10 – OWA Website Renamed

Who = All Users

What = OWA Web Site Renamed on Server

Where = All sources

When = Last 7days

Origin = All workstations/servers

# BAI3.9 – Manage changes to requirements

### (Executive Summary) BAI3.9 - Acquire and Maintain Application Software

A summary report containing events from all of the following reports.

### BAI3.9 – Detailed list of software installations via GPO added

Who = All Users

What = Computer Software Installation Policy Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.9 – Detailed list of software installations via GPO modified

Who = All Users

What = Computer Software Installation Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### BAI3.9 – Detailed list of software installations via GPO removed

Who = All Users

What = Computer Software Installation Policy Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# BAI6.1 – Evaluate, prioritize and authorize change requests

# BAI6.2 – Manage emergency changes

# BAI6.3 – Track and report change status

### (Executive Summary) Develop and Maintain Procedures

A summary report containing events from all of the following reports.

### (Executive Summary) Ensure Continuous Service

A summary report containing events from all of the following reports.

### (Executive Summary) Manage Changes

A summary report containing events from all of the following reports.

### Detailed list of authorized changes made during business hours

Who = All Users

What = All categories

Where = All sources

When = From 08:00 PM to 05:00 AM

Origin = All workstations/servers

### Detailed list of unauthorized changes made during business after hours

Who = All Users

What = All categories

Where = All sources

When = From 05:00 PM to 08:00 AM

Origin = All workstations/servers

### Detailed list of GPO modifications

Who = All Users

What = Group Policy Item facility; Group Policy Object facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of computer modifications

Who = All Users

What = Custom Computer Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of DNS modifications

Who = All Users

What = DNS Service facility; DNS Zone facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of domain modifications

Who = All Users

What = Domain Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of domain controller

Who = All Users

What = Configuration Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of Exchange modifications

Who = All Users

What = Exchange Administrative Group facility; Exchange Distribution List facility; Exchange Organization facility; Exchange Permission Tracking facility; Exchange Security Group facility; Exchange User facility

Where = All sources

When = Last 7 days

Origin = All workstations/server

### Detailed list of Exchange infrastructure modifications

Who = All Users

What = Exchange Organization facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of fault tolerance modifications

Who = All Users

What = Fault Tolerance facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of file system modifications

Who = All Users

What = Custom File System Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of forest modifications

Who = All Users

What = Forest Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of group modifications

Who = All Users

What = Custom Group Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of IP modifications

Who = All Users

What = IP Security facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of NETLOGON modifications

Who = All Users

What = NETLOGON Service facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of registry modifications

Who = All Users

What = Registry subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of replication modifications

Who = All Users

What = Replication Transport facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of schema modifications

Who = All Users

What = Schema Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of service modifications

Who = All Users

What = Service Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of site modifications

Who = All Users

What = Site Configuration facility; Site Link Configuration facility; Site Link Bridge Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of user modifications

Who = All Users

What = Custom User Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of subnet modifications

Who = All Users

What = Subnets facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Organizational Unit Management

### Organizational Units Added in Last 30 days

Who = All Users

What = Subordinate OU added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units Deleted in Last 30 days

Who = All Users

What = Subordinate OU removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units Renamed in Last 30 days

Who = All Users

What = Subordinate Ou renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units set to block GPO inheritance in Last 30 days

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## BAI7.5 - Perform acceptance tests

## BAI7.6 - Promote to production and manage releases

## BAI7.8 – Perform a post-implementation review

### (Executive Summary) Install and Accredit Systems

A summary of reports containing events from all of the following reports.

### Detailed list of software installations via GPO added

Who = All Users

What = Computer Software Installation Policy Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of software installations via GPO modified

Who = All Users

What = Computer Software Installation Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Section 404 | Delivery and Support

The Delivery and Support reports are available under the following folders:

- APO9.2 – Catalogue IT-enabled services
- APO9.4 – Monitor and report service levels
- BAI10.3 – Maintain and control configuration items
- BAI10.4 – Produce status and configuration reports
- BAI10.5 – Verify and review integrity of the configuration repository
- BAI4.1 – Assess current availability, performance and capacity and create a baseline
- BAI4.3 – Plan for new or changed service requirements

- BAI4.4 – Monitor and review availability and capacity
- BAI4.5 – Investigate and address availability, performance and capacity issues
- DSS1.1 – Perform operational procedures
- DSS1.3 – Monitor IT infrastructure
- DSS3.1 – Identify and classify problems
- DSS3.2 – Investigate and diagnose problems
- DSS3.5 – Perform proactive problem management
- DSS5.1 – Protect against malware
  - Antivirus Scanning
  - Defender
  - Group Management
  - Service Pack and Hotfixes
  - User Management
- DSS5.2 – Manager network and connectivity security
  - Antivirus Scanning
  - Defender
  - Group Management
  - Service Pack and Hotfixes
  - User Management
- DSS5.3 – Manage endpoint security
  - Antivirus Scanning
  - Defender
  - Group Management
  - Service Pack and Hotfixes
  - User Management
- DSS5.4 – Manager user identity and logical access
  - Antivirus Scanning
  - Defender
  - Group Management
  - Service Pack and Hotfixes
  - User Management
- DSS5.6 – Manage sensitive documents and output devices
  - Access Control - File System
  - Authentication Services
  - Dynamic Access Control - DAC
  - EMC
  - Exchange
  - NetApp
  - SharePoint
  - SQL

- DSS5.7 – Monitor the infrastructure for security-related events
  - Antivirus Scanning
  - Defender
  - Group Management
  - Service Pack and Hotfixes
  - User Management
- DSS6.6 – Secure information assets
  - Access Control - File System
  - Authentication Services
  - Dynamic Access Control - DAC
  - EMC
  - Exchange
  - NetApp
  - SharePoint
  - SQL

# APO9.2 – Catalogue IT-enabled services

# APO9.4 – Monitor and report service levels

### (Executive Summary) Define and Manage Service Levels

A summary report containing events from all of the following reports.

### (Executive Summary) Manage Third Party Services

A summary report containing events from all of the following reports.

### Detailed list of DNS modifications

Who = All Users

What = DNS Service facility; DNS Zone facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of domain controller modifications

Who = All Users

What = Configuration Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of domain controller removed

Who = All Users

What = Configuration Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of NETLOGON modifications

Who = All Users

What = NetLOGON Service facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of NTDS modifications

Who = All Users

What = NTDS Service facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of replication modifications

Who = All Users

What = Replication Transport facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of service modifications

Who = All Users

What = Service Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of software installations via GPO removed

Who = All Users

What = Computer Software Installation Policy Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of software installations via GPO modified

Who = All Users

What = Computer Software Installation Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of software installations via GPO added

Who = All Users

What = Computer Software Installation Policy Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Users enabled in last 30 days

Who = All Users

What = User Account Enabled; User Account re-enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users disabled in last 30 days

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users deleted in last 30 days

Who = All Users

What = User Account Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users added in last 30 days

Who = All Users

What = User Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users logon hours changed in last 30 days

Who = All Users

What = User logonhours changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# BAI10.3 – Maintain and control configuration items

# BAI10.4 – Produce status and configuration reports

# BAI10.5 – Verify and review integrity of the configuration repository

### (Executive Summary) Manage the Configuration

A summary report containing events from all of the following reports.

### Detailed list of all Active Directory modifications

Who = All Users

What = Active Directory subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of all Exchange modifications

Who = All Users

What = Exchange Administrative Group facility; Exchange Distribution List facility; Exchange Organization facility; Exchange Permission Tracking facility; Exchange Security Group facility; Exchange User facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of all file system modifications

Who = All Users

What = File System subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of all registry modifications

Who = All Users

What = Registry subsystem

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# BAI4.1 – Assess current availability, performance and capacity and create a baseline

# BAI4.3 – Plan for new or changed service requirements

# BAI4.4 – Monitor and review availability and capacity

# BAI4.5 – Investigate and address availability, performance and capacity issues

### (Executive Summary) Manage Performance and Capacity

A summary report containing events from all of the following reports.

### Detailed list of disk size modifications

Who = All Users

What = Disk Size Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of memory modifications

Who = All Users

What = Memory Amount Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of NETLOGON modifications

Who = All Users

What = NETLOGON Service facility

Where = All sources

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# DSS1.1 – Perform operational procedures

# DSS1.3 – Monitor IT infrastructure

### (Executive Summary) Manage Operations

A summary report containing events from all of the following reports.

### Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled; Change Auditor Agent Connected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of computer modifications

Who = All Users

What = Custom Computer Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of domain modifications

Who = All Users

What = Domain Configuration facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of Exchange modifications

Who = All Users

What = Exchange Distribution List facility; Exchange Permission Tracking facility; Exchange Security Group facility; Exchange Administrative Group facility; Exchange User facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of file system modifications

Who = All Users

What = Custom File System Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of GPO modifications

Who = All Users

What = Group Policy Item facility; Group Policy Object facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of group modifications

Who = All Users

What = Custom Group Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of OU modifications

Who = All Users

What = OU facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of user modifications

Who = All Users

What = Custom User Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## DSS3.1 – Identify and classify problems

## DSS3.2 – Investigate and diagnose problems

## DSS3.5 – Perform proactive problem management

### (Executive Summary) Manage Problems and Incidents

A summary report containing events from all of the following reports.

### Detailed list of all high severity modifications

Who = All Users

What = Severity | High

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of all low severity modifications

Who = All Users

What = Severity | Low

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of all medium severity modifications

Who = All Users

What = Severity | Medium

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## DSS5.1 – Protect against malware

# DSS5.2 – Manager network and connectivity security

# DSS5.3 – Manage endpoint security

# DSS5.4 – Manager user identity and logical access

# DSS5.7 – Monitor the infrastructure for security-related events

### (Executive Summary) Ensure Systems Security

A summary report containing events from all of the following reports.

### (Executive Summary) Identify and Allocate Costs

A summary report containing events from all of the following reports.

### Detailed list of audit policy modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed; Audit: Audit the Use of Backup and Restore Privilege Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit Privilege Use Policy Changed; Audit System Events Policy Changed; Audit Process Tracking Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Account Management Policy Changed; Audit Policy Change Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of computers added

Who = All Users

What = Computers Added

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of DACL (permissions) modifications

Who = All Users

What = DACL Changed on Group Object; DACL Changed on OU Object; DACL Changed on User Object; DACL Changed on AdminSDHolder Object; DACL Changed on Exchange Group Object (Exchange 2003); DACL Changed on Domain Object; DACL Changed on Computer Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of domain controllers added

Who = All Users

What = Domain Controller Added to Domain

Where = All sources

When = Last 7 days

Origin = All domain controllers

### Detailed list of Exchange permission modifications

Who = All Users

What = Exchange Permission Tracking facility; Mailbox Rights Changed for User

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of file system permission modifications

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed; Local Share Permissions Changed; SYSVOL Folder Access Rights Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process

Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit: Audit the use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of share modifications

Who = All Users

What = Active Directory Share Added; Active Directory Share Removed; Local Share Added; Local Share Folder Path Changed; Local Share Permissions Changed; Local Share Removed; SYSVOL Folder Access Rights Changed; SYSVOL Folder Auditing Changed; SYSVOL Folder Ownership Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Antivirus Scanning

### Detailed list of service changes

Who = All Users

What = Service Monitoring facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Defender

### All Defender events in last 30 days

Who = All Users

What = Defender facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member added to access node in last 30 days

Who = All Users

What = Member Added to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender – Member removed from access node in last 30 days

Who = All Users

What = Member Removed from Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node added in last 30 days

Who = All Users

What = Defender Access Node Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender access node removed in last 30 days

Who = All Users

What = Defender Access Node Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender password events in last 30 days

Who = All Users

What = Defender Password Changed; Defender Password Cleared; Defender Password Expiry Cleared; Defender Password Expiry Set; Defender Password Set

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy added in last 30 days

Who = All Users

What = Defender Policy Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy change events in last 30 days

Who = All Users

What = Defender Policy Changed for Access Node; Defender Policy Changed for Group; Defender Policy Changed for Security Server; Defender Policy Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender policy removed in last 30 days

Who = All Users

What = Defender Policy Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload added in last 30 days

Who = All Users

What = Defender RADIUS Payload Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload change events in last 30 days

Who = All Users

What = Defender RADIUS Payload Changed for Access Node; Defender RADIUS Payload Changed for Group; Defender RADIUS Payload Changed for Security Server; Defender RADIUS Payload Changed for User

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender RADIUS payload removed in last 30 days

Who = All Users

What = Defender RADIUS Payload Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server added in last 30 days

Who = All Users

What = Defender Security Server Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server assigned to access node in last 30 days

Who = All Users

What = Defender Security Server Assigned to Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server removed in last 30 days

Who = All Users

What = Defender Security Server Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender security server unassigned from access node in last 30 days

Who = All Users

What = Defender Security Server Unassigned from Access Node

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender temporary response events in last 30 days

Who = All Users

What = Defender Token Temporary Response Cleared; Defender Token Temporary Response Set; Defender Token Temporary Response Usage Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token added in last 30 days

Who = All Users

What = Defender Token Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token assigned in last 30 days

Who = All Users

What = Defender Token Assigned

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token PIN events in last 30 days

Who = All Users

What = Defender Token PIN Changed; Defender Token PIN Cleared; Defender Token PIN Expiry Cleared; Defender Token PIN Expiry Set; Defender Token PIN Set

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token removed in last 30 days

Who = All Users

What = Defender Token Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Defender token unassigned in last 30 days

Who = All Users

What = Defender Token Unassigned

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Group Management

### Group added in last 30 days

Who = All Users

What = Group Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group deleted in last 30 days

Who = All Users

What = Group Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member added changes in last 30 days

Who = All Users

What = Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member removed changes in last 30 days

Who = All Users

What = Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group moved in last 30 days

Who = All Users

What = Group Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member added changes in last 30 days

Who = All Users

What = Nested Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member removed changes in last 30 days

Who = All Users

What = Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group permissions changed in last 30 days

Who = All Users

What = DACL Changed on Group Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed (SAM account name) changes in last 30 days

Who = All Users

What = Group samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed in last 30 days

Who = All Users

What = Group Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group type changes in last 30 days

Who = All Users

What = Group Type Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Service Pack and Hotfixes

### Detailed list of all hot fixes applied

Who = All Users

What = Hotfix Applied

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of hot fixes rolled back

Who = All Users

What = Hotfix Rolled Back

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of service packs applied

Who = All Users

What = Computer Service Pack Applied; Domain Controller Service Pack Applied

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of service packs rolled back

Who = All Users

What = Domain Controller Service Pack Rolled Back

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## User Management

### Changes to user profiles in last 30 days

Who = All Users

What = Home Folder Changed on User Object; Home Folder Mapped Drive Changed on User Object; Level of Control Changed for User Object; Primary Group ID Changed for User Object; Profile Path Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions on user accounts changed in last 30 days

Who = All Users

What = DACL Changed on User Object; Required User’s Permissions Changed for User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users added in last 30 days

Who = All Users

What = User Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users added to group in last 30 days

Who = All Users

What = User Member-of Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users deleted in last 30 days

Who = All Users

What = User Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users disabled in last 30 days

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users display name changed in last 30 days

Who = All Users

What = Display Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# DSS5.6 – Manage sensitive documents and output devices

# DSS6.6 – Secure information assets

### (Executive Summary) Manage Data

A summary report containing events from all of the following reports.

### Detailed list of audit policy modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audits Policy Changed; Audit: Audit the Use of Backup and Restore Privilege Policy Changed; Audit: Audit the Access of Global System Objects Policy Changed; Audit Privilege Use Policy Changed; Audit System Events Policy Changed; Audit Process Tracking Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Account Management Policy Changed; Audit Policy Change Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of Change Auditor agent modifications

Who = All Users

What = Agent Service Has More Than 100 Events Waiting; Agent Service has Reached a Critical Load; Agent Service Has Returned to Normal Operations; Change Auditor Agent Disconnected; Change Auditor Agent Uninstalled; Change Auditor Agent Connected

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of security log modifications

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Events Policy Changed; Audit: Audit the Access of Global System Object Policy Changed; Audit: Audit the Use of Backup and Restore Privilege Policy Changed; Audit: Shut Down System Immediately if Unable to Log Security Audit Policy Changed; Security Audit Log Rolled Over; Crash on Audit Fail Policy Changed; Shut Down the Computer When the Security Audit Log is Full Policy Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## Access Control - File System

### Directory shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Directory shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder added in last 30 days

Who = All Users

What = File Created; Folder Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder attribute changed in last 30 days

Who = All Users

What = File Attribute Changed; Folder Attribute Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder auditing changed in last 30 days

Who = All Users

What = File Auditing Changed; Folder Auditing Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder modified date changed in last 30 days

Who = All Users

What = File Last Write Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder moved in last 30 days

Who = All Users

What = File Moved; Folder Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder ownership changed in last 30 days

Who = All Users

What = File Ownership Changed; Folder Ownership Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder permission changed in last 30 days

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder removed in last 30 days

Who = All Users

What = File Deleted; Folder Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder renamed in last 30 days

Who = All Users

What = File Renamed; Folder Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share added in last 30 days

Who = All Users

What = Local Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share auditing changed in last 30 days

Who = All Users

What = Local Share Auditing changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share permission changed in last 30 days

Who = All Users

What = Local Share Permissions Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share removed in last 30 days

Who = All Users

What = Local Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Authentication Services

### Authentication Services computers added in last 30 days

Who = All Users

What = Authentication Services Computer object added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Authentication Services computers deleted in last 30 days

Who = All Users

What = Authentication Services Computer object deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Groups set to UNIX-disabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for Group - Restriction = To: Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Groups set to UNIX-enabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for Group - Restriction = To: Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## UNIX home directory changed in last 30 days

Who = All Users

What = UNIX Home Directory Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## UNIX login shell changed in last 30 days

Who = All Users

What = UNIX Login Shell Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## UNIX-enabled groups deleted in last 30 days

Who = All Users

What = UNIX-Enabled Group Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## UNIX-enabled users deleted in last 30 days

Who = All Users

What = UNIX-Enabled User Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users set to UNIX-disabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User - Restriction = To: Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users set to UNIX-enabled in last 30 days

Who = All Users

What = UNIX-Enabled Changed for User - Restriction = To: Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Dynamic Access Control - DAC

### All Dynamic Access Control Events

Who = All Users

What = Dynamic Access Control

Where = All sources

When = Last 7days

Origin = All workstations/servers

## EMC

### EMC file access rights changed

Who = All Users

What = EMC file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents written

Who = All Users

What = EMC file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents created

Who = All Users

What = EMC file contents created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents deleted

Who = All Users

What = EMC file contents deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents moved

Who = All Users

What = EMC file contents moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file contents opened

Who = All Users

What = EMC file contents opened

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file ownership changed

Who = All Users

What = EMC file ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC file renamed

Who = All Users

What = EMC file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder access rights changed

Who = All Users

What = EMC folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder created

Who = All Users

What = EMC folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder deleted

Who = All Users

What = EMC folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder moved

Who = All Users

What = EMC folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder ownership changed

Who = All Users

What = EMC folder ownership changed

Where = All sources

When = This Week

Origin = All workstations/servers

### EMC folder renamed

Who = All Users

What = EMC folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## Exchange

### All Exchange Administrative Group Events

Who = All Users

What = Exchange Administrative Group facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Distribution List (Goup) Events

Who = All Users

What = Exchange Security Group facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### All Exchange Permission Tracking Events

Who = All Users

What = Exchange Permission Tracking facility

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## NetApp

### NetApp file access rights changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file access rights changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file access rights (no from value)

Who = All Users

What = NetApp file access rights (no from value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file contents written

Who = All Users

What = NetApp file contents written

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file created

Who = All Users

What = NetApp file created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file deleted

Who = All Users

What = NetApp file deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file moved

Who = All Users

What = NetApp file moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file opened

Who = All Users

What = NetApp file opened

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed

Who = All Users

What = NetApp file access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file ownership changed (no from value)

Who = All Users

What = NetApp file access rights changed (no from value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp file renamed

Who = All Users

What = NetApp file renamed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed (no from-value)

Who = All Users

What = NetApp folder access rights changed (no from-value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder access rights changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder created

Who = All Users

What = NetApp folder created

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder deleted

Who = All Users

What = NetApp folder deleted

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder moved

Who = All Users

What = NetApp folder moved

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed

Who = All Users

What = NetApp folder access rights changed

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder ownership changed (no from value)

Who = All Users

What = NetApp folder access rights changed (no from value)

Where = All sources

When = This Week

Origin = All workstations/servers

### NetApp folder renamed

Who = All Users

What = NetApp folder renamed

Where = All sources

When = This Week

Origin = All workstations/servers

## SharePoint

### Permission changes in the last 7 days

Who = All Users

What = All permission levels revoked; Permission level created; Permission level deleted; Permission level granted; Permission level permissions modified; Permission level revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Permission inheritance changes in the last 7 days

Who = All Users

What = Permission inheritance broken; Permission inheritance restored; Permission level inheritance broken; Permission level permissions modified

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups created and deleted in the last 7 days

Who = All Users

What = Security group created; Security group deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups membership changes in the last 7 days

Who = All Users

What = Member added to security group; Member removed from security group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection ownership changes in the last 7 days

Who = All Users

What = Site collection ownership granted; Site collection ownership revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collections created and deleted in the last 7 days

Who = All Users

What = Site collection created; Site collection deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Sites created and deleted in the last 7 days

Who = All Users

What = Site created; Site deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Sites moved in the last 7 days

Who = All Users

What = Site moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

## SQL

### All SQL Add Roles, User, and Login Events in the last 24 hours

Who = All Users

What = Audit Add DB User; Audit Add Login; Audit Add Login to Server Role; Audit Add Member to DB Role; Audit Add Role

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### Audit Add Login

Who = All Users

What = Audit Add Login

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Login to Server Role

Who = All Users

What = Audit Add Login to Server Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Member to DB Role

Who = All Users

What = Audit Add Member to DB Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Add Role

Who = All Users

What = Audit Add Role

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Database

Who = All Users

What = Audit Alter Database

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Database Object

Who = All Users

What = Audit Alter Database Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Database Principal

Who = All Users

What = Audit Alter Database Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Object Derived Permission

Who = All Users

What = Audit Alter Object Derived Permission

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Schema Object

Who = All Users

What = Audit Alter Schema Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Object

Who = All Users

What = Audit Alter Server Object

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Alter Server Principal

Who = All Users

What = Audit Alter Server Principal

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Drop Database

Who = All Users

What = Audit Drop Database

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Audit Drop DB User

Who = All Users

What = Audit Drop DB User

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Section 404 | Planning and Organization

The Planning and Organization reports are available under the following folder:

- Manage Contract Staff

## Manage Contract Staff

### (Executive Summary) Manage Human Resources

A summary report containing events from all of the following reports.

### Detailed list of disabled user accounts

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of enabled user accounts

Who = All Users

What = User Account Enabled

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of expired user accounts

Who = All Users

What = User accountExpires Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of user dial-in modifications

Who = All Users

What = User Dial-in Static Route Added; User Dial-in Static Route Removed; User Dial-in Callback Options Changed; User Dial-in Static IP Address Changed; User Dial-in Remote Access Permission Changed; User Dial-in Verify Caller ID Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of user Exchange mailbox modifications

Who = All Users

What = Mailbox Enabled for User; Mail Disabled for User; Mailbox Rights Changed for User; Mailbox Disabled for User; Mail Enabled for User; Email Addresses Changed for User

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of user name modifications

Who = All Users

What = User userPrincipalName Changed; Display Name Changed on User Object; First Name Changed on User Object; User samAccountName Changed; Last Name Changed on User Object; Domain User Renamed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of user permitted logon hour modifications

Who = All Users

What = User logonHours Changed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Detailed list of user workstation restriction modifications

Who = All Users

What = User userWorkstations Added; User userWorkstations Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# Security

The Security reports are available in the following folders:

- Access Control - Administrator Account Activity
- Access Control - Administrator Group Activity
- Access Control - File System
- Access Management
- Computer Activity
- Critical GPO Changes
- Domain Controller Security
- Domain Security
- Exchange
- Group Activity
- Group Management
- Organizational Unit Management
- Severity Based Changes
- Trust Activity
- User Activity
- User Management

# Access Control - Administrator Account Activity

### Critical Group Membership changes in last 30 days

Report generated for each domain

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group; Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group Membership changes in last 30 days

Who = All Users

What = Member Added to Group, Member Removed from Group; Nested Member Added to Group; Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions to AdminSDHolder changes in last 30 days

Who = All Users

What = DACL Changed on AdminSDHolder Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Access Control - Administrator Group Activity

### Nested group changes in last 30 days

Who = All Users

What = Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group; Nested Member Added to Group; Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions on group changes in last 30 days

Who = All Users

What = DACL Changed on Group Object; Active Directory subsystem

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions to AdminSDHolder changes in last 30 days

Who = All Users

What = DACL Changed on AdminSDHolder Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Access Control - File System

### Changes to SYSVOL on all Domain Controllers in last 30 days

Who = All Users

What = SYSVOL facility; SYSVOL Location Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Directory shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Directory shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder added in last 30 days

Who = All Users

What = File Created; Folder Created

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder attribute changed in last 30 days

Who = All Users

What = File Attribute Changed; Folder Attribute Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder auditing changed in last 30 days

Who = All Users

What = File Auditing Changed; Folder Auditing Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder modified date changed in last 30 days

Who = All Users

What = File Last Write Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder moved in last 30 days

Who = All Users

What = File Moved; Folder Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder ownership changed in last 30 days

Who = All Users

What = File Ownership Changed; Folder Ownership Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder permission changed in last 30 days

Who = All Users

What = File Access Rights Changed; Folder Access Rights Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder removed in last 30 days

Who = All Users

What = File Deleted; Folder Deleted

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### File/Folder renamed in last 30 days

Who = All Users

What = File Renamed; Folder Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share added in last 30 days

Who = All Users

What = Local Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share permission changed in last 30 days

Who = All Users

What = Local Share Permissions Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Local share removed in last 30 days

Who = All Users

What = Local Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares removed in last 30 days

Who = All Users

What = Active Directory Share Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Access Management

### User account restrictions changed in last 30 days

Who = All Users

What = User Account Enabled; User Account Disabled; DACL Change on User Object; User Member-of Added; User Member-of Removed; User accountExpires Changed; User Password Changed; User logonHours Changed; User Account Locked; User Account Unlocked; Active Session Limit Changed for User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### User logon hours changed in last 30 days

Who = All Users

What = User logonHours Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users workstation access restrictions changed in last 30 days

Who = All Users

What = User userWorkstations Added; User userWorkstations Removed; Active Session Limit Changed for User Object; Allow Reconnection Changed for User Object; Delegation Authentication Protocol Changed for User Object; Enable Remote Control Changed for User Object; End a Disconnected Session Changed for User Object; Idle Session Limit Changed for User Object; Logon Script Changed for User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Computer Activity

### Computers added in last 30 days

Who = All Users

What = Computer Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers disabled in last 30 days

Who = All Users

What = Computer Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers enabled in last 30 days

Who = All Users

What = Computer Account Enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers moved in last 30 days

Who = All Users

What = Computer Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers removed in last 30 days

Who = All Users

What = Computer Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers renamed in last 30 days

Who = All Users

What = Computer Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers with a Service Pack applied in last 30 days

Who = All Users

What = Computer Service Pack Applied

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Computers with a Service Pack rolled back in last 30 days

Who = All Users

What = Computer Service Pack Rolled Back

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Computer Management

### AdminCount changed on computer objects in the last 30 days

Who = All Users

What = AdminCount attribute changed on computer object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Critical GPO Changes

### Default domain audit policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Event Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Default domain Kerberos policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Default domain password policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Enforce Password History Policy Changed; Maximum Password Age Policy Changed; Minimum Password Age Policy Changed; Minimum Password Length Policy Changed; Password Must Meet Complexity Requirements Policy Changed; Store Passwords Using Reversible Encryption Policy Changed

Group Policy subsystem – Default Domain Policy container

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Domain policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Linked Group Policy on Domain Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational unit policy changes in last 30 days

Report generated for each domain

Who = All Users

What = Linked Group Policy on OU Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Domain Controller Security

### Active Directory Database Events in last 30 days

Who = All Users

What = Active Directory Database facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to DNS settings in last 30 days

Who = All Users

What = DHCP Enabled; DHCP Disabled; Static IP Address Changed; Subnet Mask Changed; Default Gateway Changed; Contents of DNS Server List Changed; Use Primary and Connection Specific Suffixes Flag Changed; Append Parent Suffixes Option Changed; Connection Specific DNS Suffix Changed; Contents of DNS Suffix List Changed; Use Connection Suffix in DNS Registration Option Changed; Connection DNS Registration Option Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Changes to IP deny filter changes in last 30 days

Who = All Users

What = IP Deny List Entry Added; IP Deny List Entry Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Domain Controllers moved in last 30 days

Who = All Users

What = Domain Controller Moved to Another OU

Where = All sources

When = Last 30 days

Origin = All domain controllers

### Domain Controllers renamed in last 30 days

Who = All Users

What = Domain Controller Renamed

Where = All sources

When = Last 30 days

Origin = All domain controllers

### Global Catalog added to Domain Controller in last 30 days

Who = All Users

What = GC Added

Where = All sources

When = Last 30 days

Origin = All domain controllers

### Global Catalog removed from Domain Controller in last 30 days

Who = All Users

What = GC Removed

Where = All sources

When = Last 30 days

Origin = All domain controllers

### Hot fixes applied in last 30 days

Who = All Users

What = Hotfix Applied

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Hot fixes rolled back in last 30 days

Who = All Users

What = Hotfix Rolled Back

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Service Packs applied in last 30 days

Who = All Users

What = Domain Controller Service Pack Applied

Where = All sources

When = Last 30 days

Origin = All domain controllers

### Service Packs rolled back in last 30 days

Who = All Users

What = Domain Controller Service Pack Rolled Back

Where = All sources

When = Last 30 days

Origin = All domain controllers

### Shares added in last 30 days

Who = All Users

What = Active Directory Share Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Shares removed in last 30 days

Who = All Users

What = Active Directory Shared Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Domain Controller Configuration Changes

### All Basic Domain Controller changes in last 30 days

Who = All Users

What = Append Parent Suffixes Option Changed; Connection DNS Registration Option Changed; Connection-Specific DNS Suffixes Changed; Contents of DNS Server List Changed; Contents of DNS Suffix List Changed; Default Gateway Changed; DHCP Enabled; DHCP Disabled; Disk Size Changed; IP Deny List Entry Added; IP Deny List Entry Removed; IPSEC Settings Changed; Memory Amount Changed; NIC Added; NIC Removed; Processor Speed Changed; Raw IP Allowed Protocols List Changed; Static IP Address Changed; Subnet Mask Changed; Use Connection Suffix in DNS Registration Option Changed; Use of Dynamic DNS Changed; Use Primary and Connection Specific Suffixes Flag Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Allow raw IP allowed protocols list changed in last 30 days

Who = All Users

What = Raw IP Allowed Protocols List Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Changes to IP settings in last 30 days

Who = All Users

What = Append Parent Suffixes Option Changed; Connection DNS Registration Option Changed; Connection-Specific DNS Suffix Changed; Contents of DNS Server List Changed; Contents of DNS Suffix List Changed; Default Gateway Changed; DHCP Enabled; DHCP Disabled; Static IP Address Changed; Subnet Mask Changed; Use Primary and Connection-Specific Suffixes Flag Changed; Use Connection Suffix in DNS Registration Option Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Default gateway changes in last 30 days

Who = All Users

What = Default Gateway Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### DHCP disabled in last 30 days

Who = All Users

What = DHCP Disabled

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### DHCP enabled in last 30 days

Who = All Users

What = DHCP Enabled

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Disk size changes in last 30 days

Who = All Users

What = Disk Size Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### DNS server list changes in last 30 days

Who = All Users

What = Contents of DNS Server List Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### IPSec changes in last 30 days

Who = All Users

What = IPSEC Settings Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Memory size changes in last 30 days

Who = All Users

What = Memory Amount Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### NIC added/removed in last 30 days

Who = All Users

What = NIC Added; NIC Removed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Processor changes in last 30 days

Who = All Users

What = Processor Speed Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Static IP address changes in last 30 days

Who = All Users

What = Static IP Address Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### Subnet mask changes in last 30 days

Who = All Users

What = Subnet Mask Changed

Where = Domain Controller

When = Last 30 days

Origin = All domain controllers

### TCP/IP allowed in last 30 days

Who = All Users

What = IP Deny List Entry Added; IP Deny List Entry Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Use of dynamic DNS changed in last 30 days

Who = All Users

What = Use of Dynamic DNS Changed

Where = All sources

When = Last 30 days

Origin = All domain controllers

# Domain Security

### Changes to Domain account policies (GPO filter) in last 30 days

Who = All Users

What = Account Lockout Duration Policy Changed; Account Lockout Threshold Policy Changed; Enforce Password History Policy Changed; Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Password Age Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed; Minimum Password Age Policy Changed; Minimum Password Length Policy Changed; Password Must Meet Complexity Requirements Policy Changed; Store Passwords Using Reversible Encryption Policy Changed; Reset Account Lockout Counter After Change Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to Domain Audit policies (GPO filter) in last 30 days

Who = All Users

What = Audit Account Logon Events Policy Changed; Audit Account Management Policy Changed; Audit Directory Service Access Policy Changed; Audit Logon Events Policy Changed; Audit Object Access Policy Changed; Audit Policy Change Policy Changed; Audit Privilege Use Policy Changed; Audit Process Tracking Policy Changed; Audit System Event Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to Domain Kerberos policies (GPO filter) in last 30 days

Who = All Users

What = Enforce User Logon Restrictions Policy Changed; Maximum Lifetime for Service Ticket Policy Changed; Maximum Lifetime for User Ticket Policy Changed; Maximum Lifetime for User Ticket Renewal Policy Changed; Maximum Tolerance for Computer Clock Synchronization Policy Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### GPO Link changes on Domain objects in last 30 days

Who = All Users

What = DACL Changed on Group Policy Object; Group Policy Linked; Group Policy Unlinked; Group Policy Block Inheritance Setting Changed on Domain; Group Policy No Override Setting Changed on Domain; Group Policy Disabled Setting on Domain Changed; Owner Changed on Group Policy Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permission changes on domains in last 30 days

Who = All Users

What = DACL Changed on Domain Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions to AdminSDHolder Changes in last 30 days

Who = All Users

What = DACL Changed on AdminSDHolder Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Exchange

### All Exchange Administrative Group events in last 30 days

Who = All Users

What = Exchange Administrative Group facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### All Exchange Distribution List events in last 30 days

Who = All Users

What = Exchange Distribution List facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### All Exchange Organization events in last 30 days

Who = All Users

What = Exchange Organization facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### All Exchange Permission Tracking events in last 30 days

Who = All Users

What = Exchange Permission Tracking facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### All Exchange User events in last 30 days

Who = All Users

What = Exchange User facility

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Group Activity

### Critical Group Membership changes in last 30 days

Who = All Users

What = Member Added to Critical Enterprise Group; Member Removed from Critical Enterprise Group; Nested Member Added to Critical Enterprise Group; Nested Member Removed from Critical Enterprise Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group Membership changes in last 30 days

Who = All Users

What = Member Added to Group; Member Removed from Group; Nested Member Added to Group; Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Group Management

### AdminCount changed on group objects in the last 30 days

Who = All Users

What = AdminCount attribute changed on group object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group added in last 30 days

Who = All Users

What = Group Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group deleted in last 30 days

Who = All Users

What = Group Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group high severity sIDHistory changed in the last 30 days

Who = All Users

What = Well-known SID added to group object sIDHistory, Same domain SID added to group object sIDHistory

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member added changes in last 30 days

Who = All Users

What = Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group member removed changes in last 30 days

Who = All Users

What = Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group moved in last 30 days

Who = All Users

What = Group Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member added changes in last 30 days

Who = All Users

What = Nested Member Added to Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group nested member removed changes in last 30 days

Who = All Users

What = Nested Member Removed from Group

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group permissions changed in last 30 days

Who = All Users

What = DACL Changed on Group Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed (SAM account name) changes in last 30 days

Who = All Users

What = Group samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group renamed in last 30 days

Who = All Users

What = Group Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group sIDHistory changed in the last 30 days

Who = All Users

What = Different domain SID added to group object sIDHistory, Different domain SID removed from group object sIDHistory, Well-known SID added to group object sIDHistory, Well-known SID removed from group object sIDHistory, Same domain SID added to group object sIDHistory, and Same domain SID removed from group object sIDHistory

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group type changes in last 30 days

Who = All Users

What = Group Type Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Organizational Unit Management

### Organizational Units added in last 30 days

Who = All Users

What = Subordinate OU Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units deleted in last 30 days

Who = All Users

What = Subordinate OU Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units renamed in last 30 days

Who = All Users

What = Subordinate OU Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Organizational Units set to block GPO inheritance in last 30 days

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## Group Policy Changed last 30 days

### Group Policy block inheritance changes

Who = All Users

What = Group Policy Block Inheritance Setting Changed on OU; Group Policy Block Inheritance Setting Changed on Site; Group Policy Block Inheritance Setting Changed on Domain

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group Policy disabled setting changes

Who = All Users

What = Group Policy Disabled Setting on OU Changed; Group Policy Disabled Setting on Site Changed; Group Policy Disabled Setting on Domain Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Group Policy no override changes

Who = All Users

What = Group Policy No Override Setting Changed on OU; Group Policy No Override Setting Changed on Site; Group Policy No Override Setting Changed on Domain

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Severity Based Changes

### High severity changes in last 30 days

Who = All Users

What = Severity | High

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Low severity changes in last 30 days

Who = All Users

What = Severity | Low

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Medium severity changes in last 30 days

Who = All Users

What = Severity | Medium

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# Trust Activity

### Cross Forest level trust added in last 30 days

Who = All Users

What = Cross-forest Trust Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Cross Forest level trust deleted in last 30 days

Who = All Users

What = Cross-forest Trust Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Trusts added in last 30 days

Who = All Users

What = Trust Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Trusts deleted in last 30 days

Who = All Users

What = Trust Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# User Activity

### Users disabled in last 30 days

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users expiration date changed in last 30 days

Who = All Users

What = User accountExpires Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users locked in last 30 days

Who = All Users

What = User Account Locked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users unlocked in last 30 days

Who = All Users

What = User Account Unlocked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

## User Management

### AdminCount changed on user objects in the last 30 days

Who = All Users

What = AdminCount attribute changed on user object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Changes to user profiles in last 30 days

Who = All Users

What = Home Folder Changed on User Object; Home Folder Mapped Drive Changed on User Object; Level of Control Changed for User Object; Primary Group ID Changed for User Object; Profile Path Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Permissions on user accounts changed in last 30 days

Who = All Users

What = DACL Changed on User Object; Required User's Permissions Changed for User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users added in last 30 days

Who = All Users

What = User Object Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users added to group in last 30 days

Who = All Users

What = User Member-of Added

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users deleted in last 30 days

Who = All Users

What = User Object Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users disabled in last 30 days

Who = All Users

What = User Account Disabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users display name changed in last 30 days

Who = All Users

What = Display Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users enabled in last 30 days

Who = All Users

What = User Account Enabled; User Account Re-enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users first name changed in last 30 days

Who = All Users

What = First Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users high severity sIDHistory changed in the last 30 days

Who = All Users

What = Well-known SID added to user object sIDHistory, Same domain SID added to user object sIDHistory

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users last name changed in last 30 days

Who = All Users

What = Last Name Changed on User Object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users locked out in last 30 days

Who = All Users

What = User Account Locked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users logon hours changed in last 30 days

Who = All Users

What = User logonHours Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users moved in last 30 days

Who = All Users

What = User Object Moved

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users name(s) changed in last 30 days

Who = All Users

What = Display Name Changed on User Object; First Name Changed on User Object; User samAccountName Changed; Last Name Changed on User Object; User userPrincipal Name Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users principal name changed in last 30 days

Who = All Users

What = User userPrincipalName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users servicePrincipalName changed in the last 30 days

Who = All Users

What = ServicePrincipalName added to user object, ServicePrincipalName removed from user object

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users sIDHistory changed in the last 30 days

Who = All User

What = Different domain SID added to user object sIDHistory, Different domain SID removed from user object sIDHistory, Well-known SID added to user object sIDHistory, Well-known SID removed from user object sIDHistory, Same domain SID added to user object sIDHistory, and Same domain SID removed from user object sIDHistory

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users removed from group in last 30 days

Who = All Users

What = User Member-of Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users renamed in last 30 days

Who = All Users

What = Domain User Renamed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users SAM account name changed in last 30 days

Who = All Users

What = User samAccountName Changed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users status changed in last 30 days (Enabled, Disabled, Created, Deleted, Locked, Unlocked)

Who = All Users

What = User Account Enabled; User Account Disabled; User Object Added; User Object Removed; User Account Locked; User Account Unlocked; User Account Re-enabled

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users unlocked in last 30 days

Who = All Users

What = User Account Unlocked

Where = All sources

When = Last 30 days

Origin = All workstations/servers

### Users workstation access restrictions changed in last 30 days

Who = All Users

What = User userWorkstations Added; User userWorkstations Removed

Where = All sources

When = Last 30 days

Origin = All workstations/servers

# SharePoint

ℹ **NOTE:** By default, the SharePoint reports include the following information on the Search Results page: SharePoint Item Name, SharePoint List Name and SharePoint Web Name. These additional columns are defined using the Layout tab.

### All SharePoint events in the last 7 days

Who = All Users

What = SharePoint subsystem

Where = All sources

When = Last 7 day

Origin = All workstations/servers

### Document Content changes in the last 7 days

Who = All Users

What = Document added; Document check out canceled; Document checked in; Document checked out; Document deleted; Document metadata updated; Document updated

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Document Story changes in the last 7 days

Who = All Users

What = All document versions deleted; Document added; Document check out canceled; Document checked in; Document checked out; Document deleted; Document library added; Document library deleted (empty); Document library deleted (with contents); Document library renamed; Document library restored from recycle bin; Document metadata updated; Document moved; Document renamed; Document restored from recycle bin; Document updated; Document version deleted; Document viewed; SharePoint folder deleted; SharePoint folder moved; SharePoint folder renamed; SharePoint folder restored from recycle bin; SharePoint folder updated; Site collection deleted; Site deleted; Site moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Document Version changes in the last 7 days

Who = All Users

What = All document versions deleted; Document version deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### List item changes in the last 7 days

Who = All Users

What = All list item versions deleted; List item added; List item attachment added; List item attachment deleted; List item deleted; List item restored from recycle bin; List item updated; List item version deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Permission changes in the last 7 days

Who = All Users

What = All permission levels revoked; Permission level created; Permission level deleted; Permission level granted; Permission level permissions modified; Permission level revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Permission Inheritance changes in the last 7 days

Who = All Users

What = Permission inheritance broken; Permission inheritance restored; Permission level inheritance broken; Permission level permissions modified

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups created and deleted in the last 7 days

Who = All Users

What = Security group created; Security group deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Groups membership changes in the last 7 days

Who = All Users

What = Member added to security group; Member removed from security group

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collection Ownership changes in the last 7 days

Who = All Users

What = Site collection ownership granted; Site collection ownership revoked

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Site Collections created and deleted in the last 7 days

Who = All Users

What = Site collection created; Site collection deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Sites created and deleted in the last 7 days

Who = All Users

What = Site created; Site deleted

Where = All sources

When = Last 7 days

Origin = All workstations/servers

### Sites moved in the last 7 days

Who = All Users

What = Site moved

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# SQL Data Level

### SQL Data Level Events in the last 24 hours

Who = All Users

What = Check Constraint Added to a Table; Check Constraint Removed from a Table; Default Constraint Added to a Table; Default Constraint Removed from a Table; Default Object Added; Default Object Removed; Foreign Key Added to a Table; Foreign Key Removed from a Table; Function Added; Function Altered; Function Removed; Index Added to a Table; Index Removed from a Table; Object Renamed; Primary Key Added to a Table; Primary Key Removed from a Table; Procedure Added; Procedure Altered; Procedure Removed; Row Added to a Table; Row Removed from a Table; Row Updated in a Table; Rule Added; Rule Removed; Statistics Added to a Table; Statistics Removed from a Table; Table Added; Table Altered; Table Removed; Table Truncated; Trigger Added; Trigger Altered; Trigger Removed; Type Added; Type Removed; User Added; User Removed; View Added; View Altered; View Removed

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### SQL Data Level Row Change Events in the last 24 hours

Who = All Users

What = Row Added to a Table; Row Removed from a Table; Row Updated in a Table

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### SQL Data Level Structure Change Events in the last 7 days

Who = All Users

What = Check Constraint Added to a Table; Check Constraint Removed from a Table; Default Constraint Added to a Table; Default Constraint Removed from a Table; Default Object Added; Default Object Removed; Foreign Key Added to a Table; Foreign Key Removed from a Table; Function Added; Function Altered; Function Removed; Index Added to a Table; Index Removed from a Table; Object Renamed; Primary Key Added to a Table; Primary Key Removed from a Table; Procedure Added; Procedure Altered; Procedure Removed; Rule Added; Rule Removed; Statistics Added to a Table; Statistics Removed from a Table; Table Added; Table Altered; Table Removed; Table Truncated; Trigger Added; Trigger Altered; Trigger Removed; Type Added; Type Removed; User Added; User Removed; View Added; View Altered; View Removed

Where = All sources

When = Last 7 days

Origin = All workstations/servers

# SQL Extended Events

### All SQL Extended Events in the last 24 hours

Who = All Users

What = All audited extended events

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Operational Extended Events in the last 24 hours

Who = All Users

What = All audited operational extended events

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Analytic Extended Events in the last 24 hours

Who = All Users

What = All audited analytic extended events

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

### All SQL Admin Extended Events in the last 24 hours

Who = All Users

What = All audited admin extended events

Where = All sources

When = Last 24 hours

Origin = All workstations/servers

# Threat Detection

**All Threat Detection critical alert events in the last 24 hours**

What = Threat Detection subsystem

Where = N/A

When = Last 24 hours

Origin = Threat Detection server

Layout tab - Order By: Time Detected (Not Grouped)

**All Threat Detection critical risky user events in the last 24 hours**

What = Threat Detection subsystem

Where = N/A

When = Last 24 hours

Origin = Threat Detection server

Layout tab - Order By: Time Detected (Not Grouped)

### All Threat Detection events in the last 7 days

What = Threat Detection subsystem

Where = N/A

When = Last 7 days

Origin = Threat Detection server

Layout tab - Order By: Time Detected (Not Grouped)

### All Threat Detection risky user events in the last 7 days

What = Threat Detection - User facility

Where = N/A

When = Last 7 days

Origin = Threat Detection server

Layout tab - Order By: Time Detected (Not Grouped)

### All Threat Detection alert events in the last 7 days

What = Threat Detection - Alert facility

Where = N/A

When = Last 7 days

Origin = Threat Detection server

Layout tab - Order By: Time Detected (Not Grouped)

### All Threat Detection risky user and alert events in the last 24 hours

What = Risky user identified, Threat detection alert added events

Where = N/A

When = Last 24 hours

Origin = Threat Detection server

Layout tab - Order By: Time Detected (Not Grouped)

# 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 Microsoft 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.