



Quest® Identity Defense

# User Guide



© 2026 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

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

#### Legend

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

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

# Contents

<b>Introducing Quest Identity Defense</b> .....	<b>8</b>
About Security Management Platform .....	8
Accessing Quest Security Management Platform .....	9
Supported regions .....	9
Access Control .....	9
About Identity Defense .....	10
Functional Overview .....	12
Configuring Additional Components .....	13
Using the Dashboard .....	17
<b>Audit</b> .....	<b>19</b>
Configuring Audit .....	19
Working with tenants .....	20
Granting required consent .....	20
Configuring tenant auditing .....	21
Historical event collection .....	21
Change Auditor Integration .....	22
Customer data storage .....	23
Registering a Change Auditor Installation .....	23
Pausing Change Auditor event forwarding .....	25
Resuming Change Auditor event forwarding .....	26
Removing a Change Auditor Installation .....	26
Reviewing the status of your Change Auditor installation .....	26
SpecterOps BloodHound Enterprise Integration .....	26
Configure a SpecterOps BloodHound Integration .....	27
Working with Audit .....	28
Using the Audit Dashboard .....	28
Working with Activity Indicators .....	29
Monitoring Audit Health status .....	29
Identifying critical activity .....	30
Identifying the top active users .....	33
Working with My Favorite Searches .....	34
Monitoring sign-in trends .....	35
Searching for specific event data (Quick Search) .....	35
Working with critical activity .....	36
Working with searches .....	37
Working with private and shared searches .....	37
Running a search .....	38
Using built in searches .....	38
Filtering Searches .....	47
Creating a custom search .....	49

Copying an existing search .....	49
Exporting a search .....	50
Creating a search from an existing search .....	50
Customizing the search display .....	51
Viewing search results and event details .....	51
Copying event details .....	52
Modifying a search .....	52
Deleting a search .....	53
Working with categories .....	53
Working with alerts and notification templates .....	54
Using built in alerts and notification templates .....	56
Auditing Microsoft Entra .....	58
Event collection and Microsoft Entra subscription .....	58
Working with Microsoft Entra Searches .....	58
Working with Microsoft Entra events with multiple targets .....	59
Auditing risk events .....	60
Auditing Microsoft 365 .....	61
<b>Findings .....</b>	<b>62</b>
Investigating Findings .....	63
Investigating Tier Zero and Privileged Object Findings .....	64
Investigating Hygiene and Detected Indicators .....	66
Using Identity Defense Intelligence with Findings .....	68
Muting Findings for Hygiene and Detected Indicators .....	69
Dismissing Findings .....	70
Viewing Finding History .....	70
<b>Tier Zero Objects .....</b>	<b>72</b>
How Tier Zero Objects are Identified .....	72
Tier Zero Objects List .....	73
Viewing Tier Zero Object Details .....	74
Adding Tier Zero Objects Manually .....	75
Removing Manually-Added Tier Zero Objects .....	76
Certifying Tier Zero Objects .....	76
Protecting Tier Zero Objects .....	77
Exporting the Tier Zero Objects List .....	78
<b>Prevention (Shields Up Protection) .....</b>	<b>80</b>
Using Shields Up .....	80
Enabling Shields Up .....	81
Disabling Shields Up .....	82
Override Access for Protected Objects .....	82
<b>Privileged Objects .....</b>	<b>84</b>

Privileged Objects List .....	84
Viewing Privileged Object Details .....	85
Adding Privileged Objects Manually .....	86
Removing a Manually-added Privileged Object .....	86
Certifying Privileged Objects .....	87
Exporting the Privileged Objects List .....	88
<b>Managing Workload Identities .....</b>	<b>89</b>
Entra ID Workload Identities .....	89
Active Directory Workload Identities .....	90
Adding and Removing Active Directory Workload Identity .....	91
Classifying Active Directory Workload Identities .....	91
Setting Identification Criteria for Active Directory Workload Identities .....	92
Viewing Workload Identity Details .....	92
Setting Workload Identity Category .....	93
Reloading Workload Identities .....	94
<b>Assessments .....</b>	<b>95</b>
First Assessment Notification Email .....	95
Built-in Assessments .....	95
Using Identity Defense Intelligence with Assessments .....	96
All Assessments List .....	97
Creating an Assessment .....	98
Viewing, Editing, and Deleting an Assessment .....	99
Viewing Assessment Summary Information .....	99
Assessing Vulnerability Prevalence .....	100
Assessment Results .....	101
Viewing Details for an Assessed Vulnerability .....	103
Discoveries and Vulnerabilities .....	104
Discoveries List .....	104
Pre-Defined Active Directory Discoveries .....	105
Additional Permissions Required for Specific Vulnerabilities .....	105
Discovery for Credential Access Vulnerabilities .....	106
Discovery for Defense Evasion Vulnerabilities .....	122
Discovery for Discovery Vulnerabilities .....	124
Discovery for Initial Access Vulnerabilities .....	125
Discovery for Lateral Movement Vulnerabilities .....	126
Discovery for Persistence Vulnerabilities .....	129
Discovery for Privilege Escalation Vulnerabilities .....	131
Discovery for Reconnaissance Vulnerabilities .....	146
Pre-Defined Entra ID Discoveries .....	146
Entra ID Vulnerabilities that Require a Premium License .....	147
Discovery for Entra ID Credential Access Vulnerabilities .....	147

Discovery for Entra ID Discovery Vulnerabilities .....	153
Discovery for Entra ID Initial Access Vulnerabilities .....	154
Discovery for Entra ID Persistence Vulnerabilities .....	160
Discovery for Entra ID Privilege Escalation Vulnerabilities .....	160
Creating a Discovery .....	162
Viewing, Editing, and Deleting a Discovery .....	163
<b>Hybrid Audit .....</b>	<b>165</b>
Overview of the Hybrid Audit Workflow .....	165
Hybrid Audit Agent Deployment .....	166
Hybrid Audit Installation Notes .....	169
Working with Hybrid Audit Brokers .....	171
Enabling Hybrid Audit Brokers .....	171
Viewing Hybrid Audit Broker Details .....	171
Working with Audited Events .....	172
Creating and Deleting Custom Active Directory Events .....	173
Excluding Accounts from Events .....	174
Working with Protection Templates .....	174
Creating Custom User-defined Protection Templates .....	175
Viewing Protection Template Details .....	176
Enabling and Disabling Protection Templates .....	177
Editing Protection Templates .....	178
Duplicating Protection Templates .....	178
Deleting Protection Templates .....	179
<b>Identity Defense Settings .....</b>	<b>180</b>
Configuring a Forwarding Destination .....	180
Managing Indicators .....	181
Muting and Unmuting Indicators .....	182
Managing Data Collections .....	183
<b>Appendix - Available Audit Search Columns and Filters .....</b>	<b>185</b>
Available search filters and columns .....	185
Available meta filters .....	224
<b>Appendix - Identity Defense Indicator Details .....</b>	<b>227</b>
Indicators by Severity .....	227
Indicators by Source .....	236
Indicators from Audit .....	236
Indicators from Assessments .....	238
Indicators from Identity Defense and Protection for Tier Zero Objects .....	243
<b>Appendix - Data Collection Details .....</b>	<b>245</b>

Active Directory Data Collection Details .....	245
Microsoft Entra ID Data Collection Details .....	253
<b>Documentation Roadmap .....</b>	<b>258</b>
Additional resources .....	258
<b>About us .....</b>	<b>259</b>
Technical support resources .....	259

---

# Introducing Quest Identity Defense

- [About Security Management Platform](#)
- [About Identity Defense](#)
- [Audit](#)
- [Findings](#)
- [Tier Zero Objects](#)
- [Prevention \(Shields Up Protection\)](#)
- [Privileged Objects](#)
- [Managing Workload Identities](#)
- [Assessments](#)
- [Hybrid Audit](#)
- [Identity Defense Settings](#)

## About Security Management Platform

Quest Security Management Platform is a Software as a Service (SaaS) application, available through [quest-on-demand.com](https://quest-on-demand.com), that provides access to multiple Quest Software Microsoft management tools through a single interface.

Security Management Platform is based on the concepts of organizations, products, and Entra ID tenants. When you sign up for the Security Management Platform service, you create an organization that can subscribe to products. Organization administrators can use the tools provided by the Security Management Platform products to perform administrative actions on Entra ID tenants.

Currently, products are available for:

- Migration
- Identity Recovery

- Identity Defense

# Accessing Quest Security Management Platform

Security Management Platform management is based on the concepts of organizations. When you sign up for the Security Management Platform service, you create an organization and you become the organization administrator. The organization can then subscribe to modules.

## ***To access Security Management Platform***

1. Go to [quest-on-demand.com](https://quest-on-demand.com)
2. On the Welcome to Quest Security Management Platform page, click **Sign in with Microsoft**.
3. Sign in using your Microsoft MFA-enabled account.
4. As part of the login process with Microsoft Entra ID, users must consent to the set of minimal permissions. By default, all users are allowed to consent to applications for permissions that do not require administrator consent. This behavior might be disabled in some Microsoft Entra tenants and may require tenant administrators to enable user consent flow for the Quest Security Management Platform application.

For more details, see [Signing up for Quest On Demand](#) in Security Management Platform Global Settings User Guide.

## Supported regions

A Microsoft Azure region is a set of datacenters deployed within a geographic area. Selecting the correct region for your Security Management Platform organization enables you to achieve higher performance and supports your requirements and preferences regarding data location. Specifying the region for your organization determines the geographical region where your data is stored.

During sign up, you can choose the region where your Security Management Platform data will be hosted. The following regions are currently supported:

- Australia
- Canada
- Europe
- United Kingdom
- United States

## Access Control

Quest Security Management Platform uses the Role-based Access Control (RBAC) security policy that restricts information system access to authorized users. Your Quest Security Management Platform organization comes configured with a number of default roles which cannot be changed, but subscribers can create custom roles with the permissions to perform needed operations on the assets of the organization.

If you are the Security Management Platform administrator or the owner of the subscription, you can add users to an existing organization and assign the required roles. If you are not the subscription owner or administrator, contact your Security Management Platform administrator for access.

When you add a user to an organization, you also assign one or more roles. The role assignment determines what permission level a user has and ultimately, what tasks the user can perform. Assigning roles and setting user permissions is referred to as access control. For more information, see [Adding users to an organization](#).

Access control is a process by which users are granted access and certain privileges to systems, resources, or information. In Security Management Platform, you can grant authenticated users access to specific resources based on your company policies and the permission level assigned to the user.

**i** **NOTE:** Every user must be assigned to at least one role. You cannot remove all roles from a user. For information about the various roles that can be assigned to users, see [Users and Roles](#).

The Identity Defense Administrator role gives users full access to Identity Defense, as well as the following permissions for Security Management Platform global settings:

- Export data
- Read access control roles
- Read Activity Trails

The following default roles are available to help you manage your security and compliance auditing:

- Identity Defense for Audit Administrator role allows full access to Audit.
- Identity Defense for Audit Operator role allows users to manage searches and create alerts.
- Manage Identity Defense for Audit Organization Private Alerts and Private Alert Plans allows users to manage Audit alert plans

## About Identity Defense

Identity Defense is an integrated Security Management Platform solution that helps you keep the Active Directory domains and Entra ID tenants in your organization secure.

You can:

- Identify Tier Zero objects in Active Directory.
- Identify Privileged objects in Entra ID.
- Certify that objects are indeed Tier Zero or Privileged and, when Quest Change Auditor version 7.4 is integrated, protect Active Directory Tier Zero objects against unauthorized or accidental modification or deletion.
- Run pre-defined Security Assessments to identify vulnerabilities in Active Directory and Entra ID and create your own Assessments.
- Investigate Findings for Tier Zero and Privileged objects, vulnerabilities identified through Assessments, and Critical Activity from Audit.
- Have Findings forwarded to a SIEM tool and alerts sent to selected email recipients.

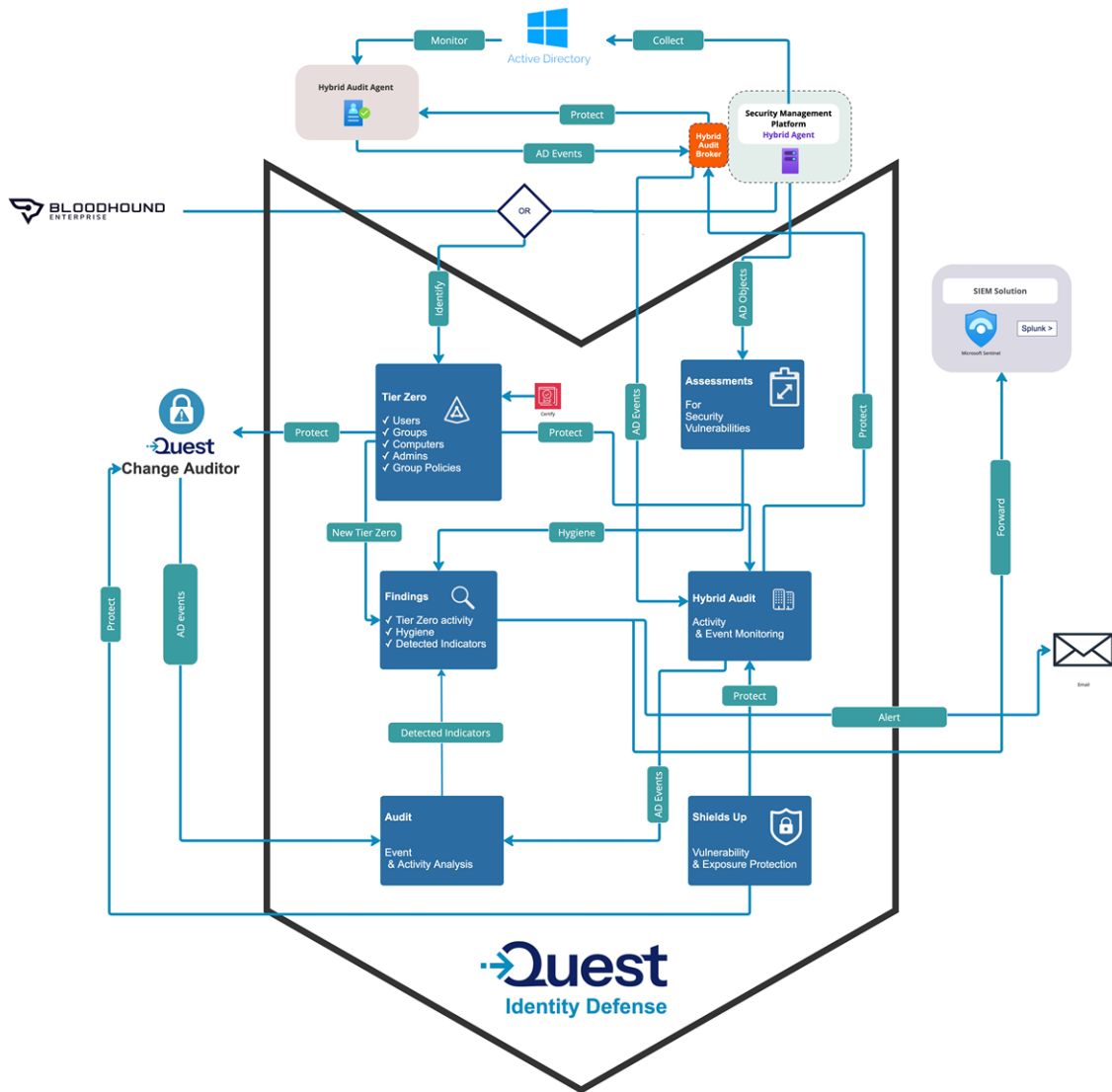
- Lock down critical Active Directory objects, preventing unauthorized or accidental changes using Shields Up. This feature enforces a highly restrictive, pre-configured lockdown on Tier Zero objects—such as users, groups, computers, and policies. While intended for temporary emergency use, Shields Up can also be deployed continuously as a proactive security measure.
- Audit and monitor critical activities and real-time alerts on important changes across Microsoft 365 services, including Exchange Online, SharePoint Online, Teams, OneDrive for Business, and Microsoft Entra.
- Integrate with Quest Change Auditor to search and correlate identities across both on premises and in the cloud to give a seamless view of activity in hybrid Microsoft environments. Specifically auditing enables:
  - Fast and flexible searches for easy investigation and accurate results across tenants and on premises environments.
  - Interactive visualizations and dashboards to summarize audit activity.
  - Easy to use customizable alerts based on audit event searches.
  - Long term storage of audit events outside of Microsoft 365 and Change Auditor for a retention period of up to 10 years.
- Review service principals and their associated security posture within your Entra ID environment to identify risky permissions, assess sign-in status, and monitor compliance with security.
- Monitor and analyze activity across both your on-premises and cloud-based Microsoft environments from a single, unified interface using Hybrid Audit.
- Use Identity Defense Intelligence AI assistance to:
  - Help you ask focused questions tailored to your environment.
  - Gain valuable insights into the security posture of your organization's Active Directory and Entra ID systems.
  - View critical vulnerabilities and issues identified during assessments and offers practical recommendations for remediation.

# Functional Overview

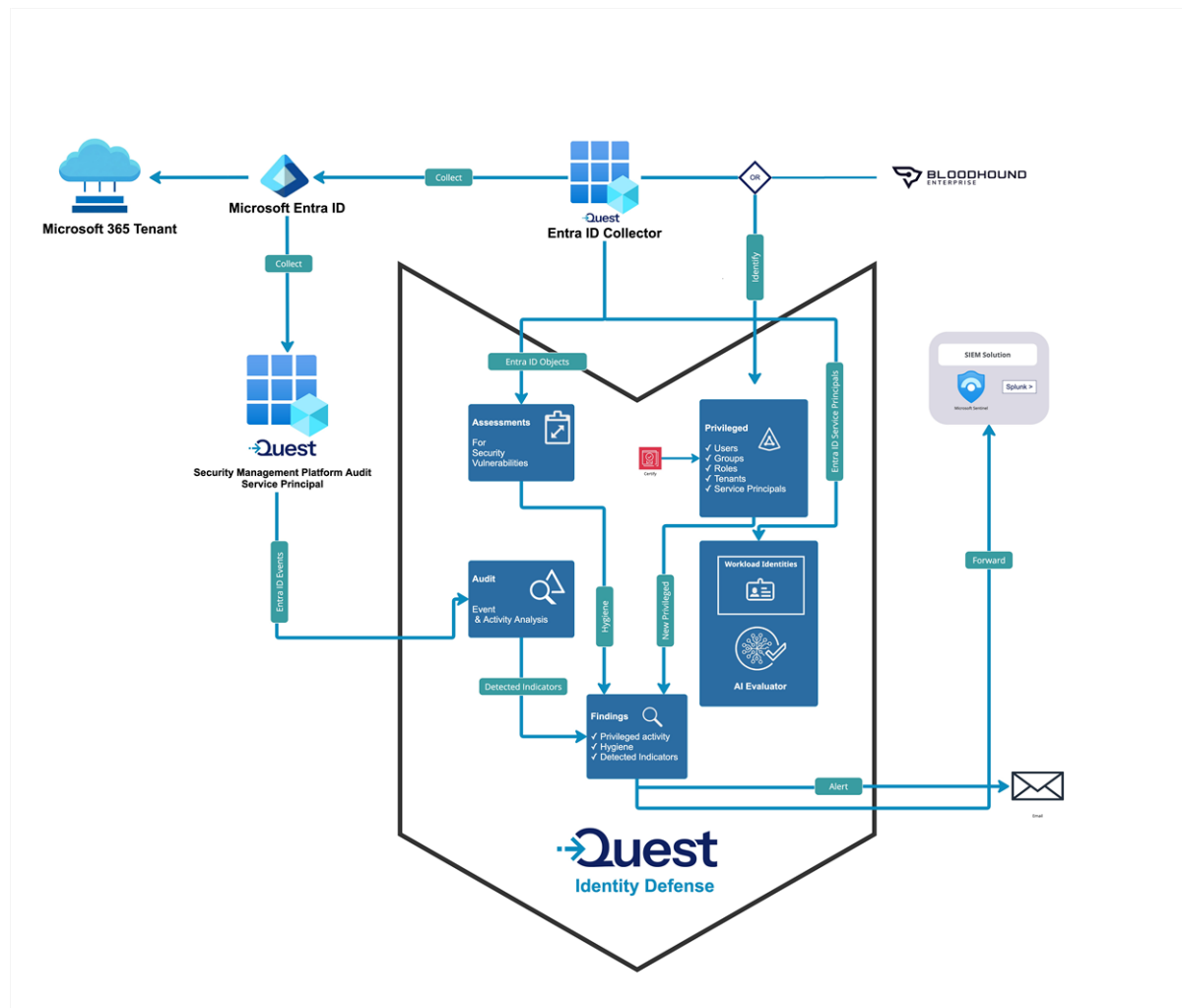
The diagrams below illustrate how Identity Defense functions for both Active Directory and Entra ID, including how [additional components](#) are integrated.

You can click on individual images within the diagram to link to the applicable topic in this guide.

## Functional Overview for Active Directory



## Functional Overview for Entra ID



## Configuring Additional Components

Additional components need to be configured to make Identity Defense fully functional.

### To configure additional components:

1. From the left navigation menu, choose **Defend | Dashboard**.
2. From the **Configuration Status** tile, configure the necessary components.

**i** **NOTE:** Once an additional component is configured in Security Management Platform, it's available to any other product that uses it.

Component	Purpose	Instructions
Hybrid Agent	Gives Identity Defense access to the Active Directory domains that you want to keep secure.	<a href="#">Security Management Platform Global Settings User Guide - Managing your on-premises domains</a> When configuring the agent, ensure that: <ul style="list-style-type: none"><li>the action <b>Collect Active Directory object data</b> is selected</li><li>any domain for which you want object data to be collected is added.</li></ul>

Component	Purpose	Instructions
Hybrid Audit Agent	Sends Active Directory events to Audit for reporting in Identity Defense Findings and allows you to protect Tier Zero objects.	<p data-bbox="778 264 802 297"><b>i</b></p> <p data-bbox="826 264 914 297"><b>NOTES:</b></p> <ul data-bbox="874 320 1394 1585" style="list-style-type: none"> <li data-bbox="874 320 1394 577">• The <b>Collect Active Directory object data</b> action uses Lightweight Directory Access Protocol (LDAP) by default. However, it will use Secure LDAP (LDAPS) if your environment is configured for it. Refer to the topic <a href="#">Secure LDAP Configuration and Deployment</a> in the On Demand Global Settings user guide for details.</li> <li data-bbox="874 589 1394 745">• In addition to the permissions required for the hybrid agent, the service account (which the <b>Collect Active Directory object data</b> action uses) requires <a href="#">an additional permission to assess certain vulnerabilities</a>.</li> <li data-bbox="874 757 1394 1003">• The service account running the Hybrid Agent/Broker must have the following permissions: <ul data-bbox="954 869 1394 1003" style="list-style-type: none"> <li data-bbox="954 869 1394 1003">• Active Directory permissions to create and modify SCP (Service Connection Point) objects under the computer object that is running the Broker.</li> </ul> </li> <li data-bbox="874 1014 1394 1137">• The Manage Identity Defense Hybrid Audit action enables the Hybrid Audit Broker process on the Hybrid Agent. See <a href="#">Working with Hybrid Audit Brokers</a>.</li> <li data-bbox="874 1149 1394 1585">• The Broker footprint: <ul data-bbox="954 1193 1394 1585" style="list-style-type: none"> <li data-bbox="954 1193 1394 1261">• Estimated disk-space for installation: 500MB + Log files.</li> <li data-bbox="954 1272 1394 1373">• Log files: By default, Broker related processes retain up to 10 log files (1MB each): 20MB.</li> <li data-bbox="954 1384 1394 1585">• Estimated disk-space for event storage: Up to 100,000 event batches waiting (max batch size is 1MB), 100GB space used or until 5% available free space on the drive where the Broker is installed.</li> </ul> </li> </ul>
Entra ID Data Collector	A Service Principal that gives	Security Management Platform Global Settings:

Component	Purpose	Instructions
	Identity Defense access to Entra ID objects in the tenants that you want to keep secure.	<ul style="list-style-type: none"> <li>• <a href="#">Adding tenants</a></li> <li>• <a href="#">Managing admin consent permissions</a></li> </ul> <p>When configuring the tenant, ensure that <b>Core   Collectors</b> consent is granted to each tenant for which you want Entra ID object data to be collected.</p> <p><b>i</b> <b>NOTE:</b> An additional consent, <b>Audit   Basic</b> is needed for the Security Management Platform - Audit Entra ID Service Principal to collect Critical Activity, which contributes to Detected Indicator findings in Identity Defense.</p>
Quest Change Auditor	<p>Sends Active Directory events to Security Management Platform for reporting in <a href="#">Findings</a> and allows you to <a href="#">protect</a> Tier Zero objects.</p> <p><b>i</b> <b>NOTE:</b> A minimum of version 7.3 is required to send critical activity events to Security Management Platform, and a minimum of version 7.4 is required to <a href="#">protect</a> Tier Zero objects.</p>	See <a href="#">Change Auditor Integration</a> .
SpecterOps BloodHound Enterprise (Optional)	<p>Identifies Tier Zero assets in your organization's Active Directory domains and Privileged assets in your Entra ID tenants, which you can monitor and <a href="#">assess</a> for security vulnerabilities in Identity Defense.</p> <p><b>i</b> <b>NOTE:</b> If BloodHound Enterprise is not configured, Identity Defense will be used as your organization's provider.</p>	See <a href="#">SpecterOps BloodHound Enterprise Integration</a> .

## Using the Dashboard

The Identity Defense dashboard displays a visual summary of the current security status of your organization's Active Directory and Entra ID.

### To access the Identity Defense dashboard:

From the left navigation menu, choose **Defend | Dashboard**. The dashboard contains tiles for each of the following components:

- Uncertified Tier Zero Objects (from Active Directory)
- Uncertified Privileged Objects (from Entra ID)
- Active Directory Tier Zero certification summary
- Entra ID Privileged Objects certification summary
- Highest Severity Findings
- Active Hygiene and Active Detected
- Configuration Status

The **Uncertified Tier Zero Objects** and **Uncertified Privileged Objects** tiles:

- display the last time the objects list was synchronized
- list the last ten uncertified objects of each type that were added to Identity Defense (you can click **View All** for an object type to view the complete list for each workload )

**i** | **NOTE:** Objects that have been certified are excluded from the lists.

- provide links that allow you to
  - view object details (by clicking an object name)
    - i** | **NOTE:** From within the Details view you can also certify the [Tier Zero](#) or [Privileged](#) object. Once an object is certified, it will no longer display in this tile.
  - [Investigate](#) the Finding for the object
  - add a new [Tier Zero](#) or [Privileged](#) object
  - if [BloodHound Enterprise is configured](#), log into BloodHound (if you have at least Read permissions) to open the Attack Paths page

**i** | **NOTE:** If Identity Defense is your provider, this link is hidden.

- view the [Tier Zero Objects list](#) or [Privileged Objects list](#) t.

The **Highest Severity Findings** tile displays the top five active findings of the highest severity. Information includes:

- the **Finding** name
- when the Finding was **Detected**
- the Finding **Type** (Tier Zero, Privileged Object, Hygiene, Detected TTP, or Detected Anomaly)
- the **Severity** indicator (Critical, High, or Medium)
- a link that allows you to **Investigate** the Finding

The View All link at the bottom of the tile allows you to view the list of all active **Findings** for the organization.

The **Active Directory Tier Zero Objects** and **Entra ID Privileged Objects** tiles display graphical representations of the number of certified vs. uncertified objects.

The **Active Hygiene and Active Detected** tile shows the total number of Hygiene and Detected (TTP and Anomaly) Findings in the organization by severity level (Critical, High, and Medium).

From the **Configuration Status** tile you can **configure additional components** and view existing configurations.

# Audit

Audit provides extensive, customizable auditing of critical activities and detailed alerts about vital changes taking place in Microsoft 365 Exchange Online, SharePoint Online, Teams, OneDrive for Business, and Microsoft Entra. Continually being in-the-know helps you to prove compliance, drive security, and improve uptime while proactively auditing changes to configurations and permissions. Specifically, you can audit:

- Exchange Online, OneDrive for Business, Teams, and SharePoint Online activity that corresponds to the events in the Microsoft 365 Security & Compliance Center unified audit log. See [Auditing Microsoft 365](#) for details.
- Microsoft Entra user, group, application, and directory activity that corresponds to the events in the audit logs, sign-in activity report, and risky sign-ins report. See [Auditing Microsoft Entra](#) for details.

Integrating with Change Auditor, provides a single view of activity across hybrid Microsoft environments and turns on-premise events into rich visualizations to investigate incidents faster. Events sent to Audit include historical events gathered up to 30 days prior to upgrade to Change Auditor 7.0.0 (or higher). See [Change Auditor Integration](#). You can audit:

- When Exchange Online mailboxes are created, deleted, and accessed.
- Permission changes to see which users are granted access to a mailbox.
- Mailbox activity by non-owner such as messages sent, read, deleted, and folders deleted
- Mailbox activity by owner for sensitive and high value mailboxes.
- When files and folders are accessed, created, deleted, uploaded, moved, renamed, and checked in and out of SharePoint Online and OneDrive for Business sites.
- When user and group attributes are changed.
- When users and groups are added to and removed from the directory.
- Successful and failed logins.
- Suspicious sign-in activity.
- Teams user and administrator activity.

## Configuring Audit

- [Working with tenants](#)
- [Granting required consent](#)
- [Configuring tenant auditing](#)
- [Historical event collection](#)
- [Change Auditor Integration](#)
- [SpecterOps BloodHound Enterprise Integration](#)

# Working with tenants

You must have a tenant in the organization to audit the Microsoft 365 and Microsoft Entra activity.

## **i** NOTE:

- For details on adding your first tenant, refer to the Security Management Platform Global Settings User Guide.
- GCC tenants are only supported by Audit in Security Management Platform organizations located the US region.
- When you remove a tenant, event collection stops. If you add the tenant back, you will need to select the services to audit again.

### **To add a tenant:**

1. Log in to Security Management Platform.
2. To add another tenant, navigate to **Defend | Audit**. From the **Configuration** tab, click **Add Microsoft Entra tenant**.
3. Sign in as a Global administrator account for the tenant on the Azure sign in page.
4. Read through the required permissions and select **Accept**.

Before you can audit the tenant, you need to grant Security Management Platform consent to audit its Microsoft 365 and Microsoft Entra activity. See [Granting required consent](#)

## Granting required consent

Before you can audit Microsoft 365 and Microsoft Entra activity and generate searches, Security Management Platform must be granted consent to audit the organization and its tenants.

## **i** NOTE: The Audit configuration page displays the status of the consent for the tenant:

- Need to grant admin consent - when consent is not granted.
- Admin consent granted - when consent is granted.

### **To grant the required consent:**

1. Log in to Security Management Platform, and select **Tenants | Office 365 Tenants**.
2. Click **Edit Consents** on the tenant
3. In **Audit | Basic**, click the **Grant Consent** button. The Azure sign in page opens. If you are signed in as the Global administrator for the tenant, you can grant consent to the Security Management Platform Audit application.
4. Read through the required permissions and select **Accept**.
5. Once this is complete, Entra ID and Microsoft 365 events are audited and can be searched in **Defend | Audit**.

# Configuring tenant auditing

Configure tenant auditing by choosing the services you want to monitor. You can audit the following:

- Audit all services
- Microsoft Entra - Audit Logs
- Microsoft Entra - Sign-ins. (Microsoft Entra - Sign-ins includes risk events.)
- Exchange Online - Administrative activity
- Exchange Online - Mailbox activity
- OneDrive for Business
- SharePoint Online
- Teams

**i** **NOTE:** You may need to turn on Microsoft 365 audit logging. For more information, see [Microsoft documentation](#).

**i** **NOTE:** You need to enable auditing of Microsoft 365 mailboxes to audit Exchange Online. For more information, see [Microsoft documentation](#).

**i** **NOTE:** You can audit multiple tenants, and each can have a distinct auditing configuration. If a tenant is added to multiple Security Management Platform organizations, the tenant auditing configuration is unique for each organization and events are collected and stored for each organization.

## To configure auditing

1. Log in to Security Management Platform, and select **Defend | Audit**.
2. Open the **Configuration** tab.
3. Select the services to audit for your tenant.
4. Click **Save**.

The configuration is added to Azure and events will be collected for the selected services. The configuration is checked every 5 minutes to see which activities to add to the database.

**i** **NOTE:** If a service is disabled or consent is revoked, events collection stops. If auditing is re-enabled, events are collected from the last collected event (or last available event).

## Historical event collection

Historical event collection is dependent on the type of license that you are using:

**i** **NOTE:** If you are currently auditing Microsoft 365 services, any additional service added at a later date will not have historical events gathered.

- For a trial license Microsoft Entra, Microsoft 365, and Change Auditor historical event collection is restricted to the 24 hours before the service is added.
- When you change to a paid subscription, historical event collection is based on when the Microsoft 365 and Microsoft Entra service is first enabled or the Change Auditor integration is configured.
  - Historical events are not collected for services that were enabled during a trial subscription.
  - Historical events are collected for services that were not enabled during the trial subscription period.
  - If you disable a service during a trial period, change to a paid subscription, and enable the service again historical events will not be collected

See the following table for historical event collection details:

Service	Changing from a trial license to a paid subscription
Microsoft 365 <ul style="list-style-type: none"> <li>• Exchange Admin activity</li> <li>• Mailbox activity</li> <li>• Sharepoint Online</li> <li>• OneDrive for Business</li> <li>• Teams</li> </ul>	For services that were not enabled with a trial license, historical events are collected for past 7 days.
Microsoft Entra <ul style="list-style-type: none"> <li>• Audit Logs</li> <li>• Sign-ins (and risk events)</li> </ul>	For services that were not enabled with a trial license, historical events are collected for either 7 or 30 past days, depending on the Microsoft Entra report retention policies.
Change Auditor <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Group Policy</li> <li>• Logon Activity</li> <li>• File System Activity</li> </ul>	For services that were not enabled with a trial license, all historical events are collected. Any events collected prior to Change Auditor 7.0.0 will not be included.

## Change Auditor Integration

Integrating with Change Auditor, provides a single view of activity across hybrid Microsoft environments and turns on-premise events into rich visualizations to investigate incidents faster. Events sent to Security Management Platform include all events gathered in Change Auditor. (Any events collected prior to Change Auditor 7.0.0 will not be included.)

Availability of historical events is dependent on how long Change Auditor has been deployed in the environment. To begin the integration, a connection between Change Auditor and your organization in Security Management Platform is configured in Change Auditor. Once the connection is made, Change Auditor will begin to send events.

- [Customer data storage](#)
- [Registering a Change Auditor Installation](#)
- [Pausing Change Auditor event forwarding](#)

- [Resuming Change Auditor event forwarding](#)
- [Removing a Change Auditor Installation](#)
- [Reviewing the status of your Change Auditor installation](#)
- [Active Directory Built in searches](#)

## Customer data storage

You can integrate one or more on premises installations of Change Auditor into a Security Management Platform organization. An organization must be selected for each connected Change Auditor installation. The selected organization determines the storage location of all customer data, and the Azure region to which Change Auditor will transmit on premises Change Auditor event data. In the same manner as other data is handled, Security Management Platform ensures that on premises data remains within the same Azure data center regions outlined above.

Customers must select an organization in the correct region for their data residency requirements depending on their individual requirements and configuration for each installation of Change Auditor. All on premises data from Change Auditor is transmitted and retained in the selected Security Management Platform organization and region. Depending on the configuration and global deployment of Change Auditor, customers can configure Security Management Platform so that the organization will store data from multiple on premises global locations in a single Security Management Platform organization region. In a similar manner, the customer could configure Security Management Platform to transmit data from on premises Change installations across a regional geographic boundary.

## Registering a Change Auditor Installation

Change Auditor installations are configured through the Change Auditor client. Once an installation is registered, Change Auditor will begin sending event data.

- i** **NOTE:** Once a configuration is in place, all coordinators which belong to the Change Auditor Installation will be registered with Security Management Platform.
- i** **NOTE:** To create the configuration, you must use the account that created the Security Management Platform subscription or an account that has been delegated the appropriate permissions from your Security Management Platform administrator.
  - If you do not own the Security Management Platform subscription, you need to contact your Security Management Platform administrator for access.
  - If you are the Security Management Platform administrator, you can delegate the required permissions by adding the required accounts to the Auditing Administrator role through the Security Management Platform Access page. See [Adding a user to an existing organization](#) for details.



**NOTE:** Required URL access

To create a configuration with Security Management Platform in the US region, Change Auditor clients and coordinators must be able to access:

- <https://quest-on-demand.com>
- <https://id.quest.com>
- <https://us.core.api.quest-on-demand.com>

To create a configuration with Security Management Platform in the Europe region, Change Auditor clients and coordinators must be able to access:

- <https://quest-on-demand.com>
- <https://id.quest.com>
- <https://eu.core.api.quest-on-demand.com>

To create a configuration with Security Management Platform in the Canada region, Change Auditor clients and coordinators must be able to access:

- <https://quest-on-demand.com>
- <https://id.quest.com>
- <https://canada.core.api.quest-on-demand.com>

To create a configuration with Security Management Platform in the UK region, Change Auditor clients and coordinators must be able to access:

- <https://quest-on-demand.com>
- <https://id.quest.com>
- <https://uk.core.api.quest-on-demand.com>

To create a configuration with Security Management Platform in the Australia region, Change Auditor clients and coordinators must be able to access:

- <https://quest-on-demand.com>
- <https://id.quest.com>
- <https://au.core.api.quest-on-demand.com>

To send events to Security Management Platform in the US region, Change Auditor coordinators must be able to access:

- <https://odauditprod-wus297293-iot.azure-devices.net>
- <https://odaudit97293data.blob.core.windows.net>

To send events to Security Management Platform in the Europe region, Change Auditor coordinators must be able to access:

- <https://odauditprod-neur5293-iot.azure-devices.net>
- <https://odaudit5293data.blob.core.windows.net>

To send events to Security Management Platform in the Canada region, Change Auditor coordinators must

be able to access

- <https://odauditprod-ccan4293-iot.azure-devices.net>
- <https://odaudit4293data.blob.core.windows.net>

To send events to Security Management Platform in the UK region, Change Auditor coordinators must be able to access

- <https://odauditprod-suk3293-iot.azure-devices.net>
- <https://odaudit3293data.blob.core.windows.net>

To send events to Security Management Platform in the Australia region, Change Auditor coordinators must be able to access

- <https://odauditprod-eau6293-iot.azure-devices.net>
- <https://odaudit6293data.blob.core.windows.net>

### ***To create a configuration***

1. From the Change Auditor client, select **View | Administration**.
2. Select **Configuration | On Demand Audit**.
3. Select **Sign in and Configure** to create the connection.
4. Enter your Quest account credentials to sign in to Security Management Platform.
5. Choose the required organization if prompted and click **Select Organization**.
6. By default, the current installation name is used for the configuration name. If required, you can enter a different name for the configuration. This is the configuration name used in Security Management Platform; it does not change the Change Auditor installation name.
7. By default, historical events from the past year will be forwarded. To set an alternative start date for historical events to be sent from Change Auditor, select the calendar icon and specify the required date.
8. Click **Finish**.

## **Pausing Change Auditor event forwarding**

### ***To pause the sending of Change Auditor events***

1. Navigate to **Audit**.
2. From the **Configuration** tab, select the ellipsis (...) on the Change Auditor tile and choose **Pause**.
3. Click **OK** to confirm.

## Resuming Change Auditor event forwarding

### *To begin sending Change Auditor events for a paused installation*

1. Navigate **Audit**.
2. From the **Configuration** tab, select the ellipsis (...) on the Change Auditor tile and choose **Resume Sending Events**.
3. Click **OK** to confirm.

## Removing a Change Auditor Installation

When you remove a Change Auditor installation that is registered with Security Management Platform (or delete the associated organization), Change Auditor will stop sending events.

### *To remove a Change Auditor installation*

1. Navigate to Defend | **Audit**
2. From the **Configuration** tab, select the ellipsis (...) on the Change Auditor tile and choose **Remove Installation**.
3. Click **OK** to confirm.

## Reviewing the status of your Change Auditor installation

From the Configuration tab, you can quickly see the status of your Change Auditor installation.

The information includes:

- Installation status - whether it is connected, disconnected, or paused.
- The time of the last update.
- The number of connected coordinators.
- The installed version of Change Auditor.

**i** **NOTE:** If the Change Auditor installation is disconnected, there may be an issue with the Change Auditor coordinators. The following steps may help reconnect the installation:

- Restart the coordinator to attempt to reconnect to Security Management Platform and check the coordinator logs for error messages. See Manage Change Auditor coordinators section in the Change Auditor User Guide for information on restarting the coordinator and accessing the logs.
- Search for the errors in the Change Auditor Knowledge Base: <https://support.quest.com/change-auditor/kb>.

If the installation is still disconnected, contact Customer Support.

## SpecterOps BloodHound Enterprise Integration

Attack path management is a critical component of defending Active Directory and Microsoft 365 environments from attacks. SpecterOps BloodHound Enterprise simplifies this process by prioritizing and quantifying attack path choke

points, giving you the information you need to identify and eliminate the paths with the most exposure and risk.

Integrating with SpecterOps BloodHound Enterprise helps you reduce the risk of attacks by enabling you to easily identify, prioritize and eliminate the most vital avenues that attackers can exploit.

Specifically administrators can monitor Tier Zero assets for their Active Directory and Microsoft Entra environment. Tier Zero is the highest level of the Active Directory tiered administrative model and includes administrative accounts, groups, domain controllers, and domains that have direct or indirect administrative control of the Active Directory forest.

Audit provides built-in searches that allow administrators to create alert-enabled search for historical changes to the Tier Zero objects to ensure real-time monitoring of critical assets.

- [Configure a SpecterOps BloodHound Integration](#)
- [BloodHound Tier Zero assets built in searches](#)
- [Monitoring Audit Health status](#)

## Configure a SpecterOps BloodHound Integration

Integrating with SpecterOps BloodHound Enterprise delivers a complete solution for risk assessment and threat monitoring. To enable this integration, add a SpecterOps BloodHound configuration.

### **i** NOTE:

- To manage a SpecterOps BloodHound Enterprise configuration, you must have the **Can Manage SpecterOps BloodHound Configuration** permission.
- Once the configuration has been added, you can select the three vertical dots in the upper right-corner to refresh the configuration immediately, to edit the notification template, or to read more about the benefits of integrating with SpecterOps BloodHound Enterprise.
- The configuration connection message details whether the connection the SpecterOps has been successful, and the status of the configuration.

### **To add a configuration:**

1. From the **Configuration** tab, select **Add BloodHound Enterprise** or click the **+** icon.
2. Enter the SpecterOps BloodHound URL, the Permanent Authorization Token (PAT) Token ID, and Key pair.
3. Click **Validate** to validate the URL format (<https://yourdomain.bloodhoundenterprise.io>), the Permanent Authorization Token (PAT) Token ID, and the Key pair.
4. Click **Save**. Once the configuration has been added, you can select to edit the Tier Zero notification template to configure who will be notified when an alert is triggered.

### **To edit a configuration:**

1. From the **Configuration** tab, select the BloodHound Enterprise card, and choose **Edit Configuration**.
2. Edit the SpecterOps BloodHound URL, Permanent Authorization Token (PAT) Token ID, and Key pair as required.

3. Click **Validate** to validate the URL format (https://yourdomain.bloodhoundenterprise.io.), the Permanent Authorization Token (PAT) Token ID, and the Key pair.
4. Click **Save**.

#### **To remove a configuration:**

**i** | **IMPORTANT:** When you remove a configuration, SpecterOps BloodHound Enterprise information will no longer be added to events in Audit.

1. From the **Configuration** tab, select the BloodHound Enterprise card, and choose **REMOVE**.
2. Click **YES** to remove the configuration.

## Working with Audit

- [Using the Audit Dashboard](#)
- [Searching for specific event data \(Quick Search\)](#)
- [Working with critical activity](#)
- [Working with searches](#)
- [Working with alerts and notification templates](#)
- [Auditing Microsoft Entra](#)
- [Auditing Microsoft 365](#)

## Using the Audit Dashboard

The Audit Dashboard displays a visual summary of the most important metrics of the Microsoft 365 and Microsoft Entra activity in your organization. The information is updated in real time, allowing you to quickly gain valuable insights into the activity taking place in your organization. You can also refresh the data by selecting the refresh icon in the top right of the dashboard.

The dashboard displays:

- Activity status indicators. For details, see [Working with Activity Indicators](#)
- Audit health status. For details, see [Monitoring Audit Health status](#).
- Microsoft Entra sign-in risk events
- Critical activity. For details, see [Identifying critical activity](#).
- Top active users. For details, see [Identifying the top active users](#).
- Favorite searches. For details, see [Working with My Favorite Searches](#).
- Log in trends. For details, see [Monitoring sign-in trends](#).

## Working with Activity Indicators

The indicators at the top of the dashboard allow you to quickly see if there has been a change in risky activity over a specific period of time. A red sidebar indicates an increase in activity; while a green sidebar indicates a reduction. You can then easily delve further into the details, by clicking the indicator to view an associated search.

**i** | **NOTE:** The indicators are updated each time that you open the dashboard or refresh the view.

The following indicators are available:

- Cloud-only Microsoft Entra users created in the last 7 days
- AD account lockouts in the last 24 hours  
If you do not have a configured Change Auditor integration, the Microsoft Entra critical directory role changes in the last 7 days indicator displays instead.
- Microsoft Entra risk events in the last 7 days  
This indicator displays when you have an Microsoft Entra ID Premium (P2) license.  
If you do not have the required license to audit risky events and Change Auditor integration is configured, the On-premises and Microsoft Entra failed sign-ins in the last 24 hours indicator displays instead.  
If you do not have the required license to audit risky events and have not configured a Change Auditor integration, the Microsoft Entra failed sign-ins in the last 24 hours indicator displays.
- Microsoft 365 external user actions in the last 24 hours

## Monitoring Audit Health status

The Audit Health tile allows you to easily see the status of your auditing configuration, identify any issues, and make the required updates to ensure you are keeping informed of the vital and critical changes to your organization.

From here, you can grant required consent for the tenant, view subscription information, view the auditing configuration settings, view results in a search, and subscribe to the built-in notification templates.

**i** | **NOTE:** Specific permissions are required for the following actions:

- Can Add and Remove Tenants is required to grant consent.
- Can Run Private Searches and Can Run Shared Searches are required to view associated results.
- Can Manage Microsoft Entra Tenant Configurations for Audit is required to view issues identified for tenants.
- Can Manage Change Auditor Installation Configuration is required to view issues identified for Change Auditor.
- Can Manage Shared Alerts and Shared Notification Templates and Can Run Shared Searches is required to subscribe to the notification templates.

**NOTE:**

- You have the option to hide items from the dashboard if they do not provide you any value, expose previously hidden items, and dismiss notifications as required.
- You have the option to dismiss the ability to subscribe to the available notification templates. Once it has been dismissed, it will no longer be displayed as an option in the Audit Health dashboard.

Possible issues that may be identified include:

- Tenant requires additional configuration
- Tenant has not been added for auditing
- Service subscription will expire soon
- Service is not enabled for event collection on the tenant
- Event collection has been disabled on the tenant
- No Microsoft 365 events have been received from the tenant in the last 24 hours
- No Microsoft Entra events have been received from the tenant in the last 24 hours
- No Microsoft Entra Sign-in events have been received from the tenant in the last 24 hours
- No Change Auditor events have been received in the last 24 hours
- Change Auditor installation has been paused
- Change Auditor installation was removed
- Change Auditor installation has not been connected in the last 24 hours
- Change Auditor upgrade is required
- Change Auditor upgrade is available
- Configure SpecterOps BloodHound Enterprise integration
- SpecterOps BloodHound Enterprise configuration was removed
- SpecterOps BloodHound Enterprise connection failed
- Subscribe to Tier Zero notification template

**To subscribe to a notification template from the Audit Health tile in the dashboard:**

1. Select **View Template** for the notification template that you want to subscribe to.
2. Edit the recipients as required, and click **Save**.

## Identifying critical activity

The Critical Activity tile highlights security-related activity, including anomaly detection for unusual spikes in activity, that may indicate a threat to your organization and require further investigation.



**NOTE:** Critical activity events are gathered and displayed based on the services that you have selected to audit.

See [Configuring tenant auditing](#) for details on selecting services to audit and [Change Auditor Integration](#) for details on accessing on premises events.

Audited Service	Critical activity
Change Auditor / Logon Activity	<ul style="list-style-type: none"> <li>• Local logons to Tier Zero computers</li> <li>• NTLM version 1 logons</li> <li>• Possible Golden Ticket Kerberos exploits</li> <li>• Potential kerberoasting or similar Kerberos attack detected</li> <li>• Tier Zero user logons to computers that are not Tier Zero</li> <li>• Unusual increase in AD account lockouts</li> <li>• Unusual increase in failed on-premises sign-ins</li> <li>• Unusual increase in successful on-premises sign-ins</li> </ul>
Change Auditor / Active Directory	<ul style="list-style-type: none"> <li>• Administrative privilege elevation detected</li> <li>• AD user ServicePrincipalName attribute changes detected</li> <li>• AD Replicating Directory Changes All domain permission granted</li> <li>• AD security changes that can prevent object enumeration detected</li> <li>• AD suspicious group ESX Admins created or member added</li> <li>• Active Directory critical group membership changes</li> <li>• Active Directory schema configuration changes</li> <li>• Active Directory forest configuration changes</li> <li>• Active Directory security changes</li> <li>• Attempt to access protected Active Directory database detected</li> <li>• Attempt to access protected Windows file or folder detected</li> <li>• Attempt to edit protected group policy object detected</li> <li>• Attempt to modify protected Active Directory object detected</li> <li>• Domain level group policy linked changes detected</li> <li>• Failed delegated managed service account migrations</li> <li>• Group Policy changes to scheduled task section</li> <li>• Group sIDHistory updates using a migration tool</li> <li>• Irregular AD replication activity detected</li> <li>• Irregular domain controller registration detected (DCShadow)</li> <li>• Potential sIDHistory injection detected</li> <li>• Security changes to Tier Zero computer objects</li> <li>• Security changes to Tier Zero domain objects</li> <li>• Security changes to Tier Zero group objects</li> <li>• Security changes to Tier Zero group policy objects</li> </ul>

Audited Service	Critical activity
	<ul style="list-style-type: none"> <li>• Security changes to Tier Zero user objects</li> <li>• SG previously reported inactive Tier Zero users that may have become active</li> <li>• Successful delegated managed service account migrations</li> <li>• Tier Zero computer changes</li> <li>• Tier Zero domain and forest configuration changes</li> <li>• Tier Zero group changes</li> <li>• Tier Zero group policy object changes</li> <li>• Tier Zero user changes</li> <li>• Unusual increase in failed AD changes</li> <li>• Unusual increase in permission changes to AD objects</li> <li>• User sIDHistory updates using a migration tool</li> </ul>
Change Auditor / Active Directory Federation Services	<ul style="list-style-type: none"> <li>• Unusual increase in successful AD Federation Services sign-ins</li> <li>• Unusual increase in failed AD Federation Services sign-ins</li> </ul>
Change Auditor / File System	<ul style="list-style-type: none"> <li>• AD Database (NTDS.dit) access attempt detected</li> <li>• AD Database (NTDS.dit) file modification attempt detected</li> <li>• All file changes with suspicious file extensions</li> <li>• Unusual increase in share access permission changes</li> <li>• Unusual increase in failed file access attempts</li> <li>• Unusual increase in file deletes</li> <li>• Unusual increase in file renames</li> </ul>
Change Auditor / Group Policy	<ul style="list-style-type: none"> <li>• Group Policy changes</li> </ul>
Microsoft Entra - Audit Logs	<ul style="list-style-type: none"> <li>• Microsoft Entra Tier Zero application changes</li> <li>• Microsoft Entra Tier Zero group changes</li> <li>• Microsoft Entra Tier Zero role changes</li> <li>• Microsoft Entra Tier Zero service principal changes</li> <li>• Microsoft Entra Tier Zero tenant level and directory activity</li> <li>• Microsoft Entra Tier Zero user changes</li> <li>• Microsoft Entra critical directory role changes</li> <li>• Microsoft Entra tenant level configuration changes</li> <li>• Microsoft Entra cloud-only users created</li> </ul>

Audited Service	Critical activity
Microsoft Entra - Sign Ins	<ul style="list-style-type: none"> <li>• Microsoft Entra Tier Zero principal logons</li> <li>• Microsoft Entra Tier Zero AD risk events</li> <li>• Unusual increase in tenant sign-in failures</li> <li>• Unusual increase in successful tenant sign-ins</li> </ul>
Exchange Online - Administrative Activity	<ul style="list-style-type: none"> <li>• OneDrive and SharePoint files shared with external users</li> <li>• OneDrive and SharePoint anonymous links</li> <li>• Microsoft 365 activity from external users</li> </ul>
Sharepoint Online or OneDrive For Business	<ul style="list-style-type: none"> <li>• Unusual increase in files shared from OneDrive and SharePoint</li> <li>• Unusual increase in Microsoft 365 activity by guest users</li> <li>• Unusual increase in Microsoft 365 activity by anonymous users</li> </ul>
Microsoft Teams	<ul style="list-style-type: none"> <li>• Unusual increase in Teams guest participants</li> </ul>

You can easily dive deeper into the activity by viewing the associated search. For details on the searches associated with the critical activity see [Working with searches](#), [Working with Microsoft Entra Searches](#) and [Using built in searches](#).

To view a full list of critical activity as well as visualizations to help understand the possible threat, see [Working with critical activity](#).

## Identifying the top active users

The Top Active Users tile displays the top five active users in the last 24 hours with each service represented by a different color bar. By default, data for all available services is displayed.

To view the exact number of events per service for a particular user, hover over a section of the bar. To dive deeper into the activity details, click the section of the bar that represents the service of interest.

**i** **NOTE** Other than Audit activity, which will always be included, the activity that is gathered and displayed is based on the services that you have selected to audit.  
See [Configuring tenant auditing](#) for details on selecting services to audit and [Change Auditor Integration](#) for details on accessing on premises events.

Audited Service	Activity
Change Auditor	<ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Active Directory Federation Services (Change Auditor version 7.1.2 or later)</li> <li>• Active Directory Database</li> </ul>

Audited Service	Activity
	<ul style="list-style-type: none"> <li>Group Policy</li> <li>Logon Activity</li> </ul>
OneDrive for Business	<ul style="list-style-type: none"> <li>OneDrive</li> </ul>
SharePoint Online	<ul style="list-style-type: none"> <li>SharePoint</li> </ul>
Microsoft Teams	<ul style="list-style-type: none"> <li>Teams</li> </ul>
Microsoft Entra - Audit Logs Microsoft Entra - Sign-ins	<ul style="list-style-type: none"> <li>Microsoft Entra ID</li> </ul>
Exchange Online - Administrative Activity Exchange Online - Mailbox Activity	<ul style="list-style-type: none"> <li>Exchange</li> </ul>

### **To view the top active users for a specific service**

1. Choose the required service from the dropdown list, and click **Select**.
2. To exclude users from being included in the calculations and display, select the Edit Excluded Users and add and remove users as required.
3. Click **Close** to save your selection.

## Working with My Favorite Searches

The My Favorite Searches section of the dashboard allows you to pin the top five searches that you have defined as having a high value in your organization. From here you can see the number of events, select to view the search details, and manage which searches to displayed in this view.

By default, the following searches are listed:

- Important changes for critical Microsoft Entra directory roles in the past 7 days
- Microsoft Entra role member changes in the past 7 days
- Cloud-only Microsoft Entra users created in the past 180 days
- Microsoft Entra tenant level configuration changes in the last 180 days
- Microsoft 365 events from EXT Users in the past 7 days

### **To manage the searches displayed on the dashboard:**

1. From My Favorite Searches, click **Edit Searches**.
2. Add and remove searches as required by selecting the category and associated search. You can also drag and drop to specify the search order on the dashboard based on priority.
3. Once you have made all your selections, click **OK**.

## Monitoring sign-in trends

The Sign-ins tile allows you to quickly see the successful and failed sign-ins over the last 7 days. You can select monitor trends for all sign-ins or select only those that you are interested in.

### To add and remove the types of sign-in trends displayed:

1. Expand the drop-down list and choose the type of sign-ins to display.
2. Select to show all or successful or failed Microsoft Entra sign-ins, Active Directory authentications, Active Directory Federation Services sign-ins, and Windows interactive logons.

If you have selected to show "All" sign-in types, any services added at a later date will automatically be selected and displayed in the dashboard.

**i** **NOTE:** Sign-in activity is gathered and displayed based on the services that you have selected to audit. See [Configuring tenant auditing](#) for details on selecting services to audit and [Change Auditor Integration](#) for details on accessing on premises events.

Audited Service	Sign in events
Change Auditor / Logon Activity	<ul style="list-style-type: none"><li>• Active Directory authentications - Successful events</li><li>• Active Directory authentications - Failed events</li><li>• Windows interactive logons - Successful events</li><li>• Windows interactive logons - Failed events</li></ul>
Change Auditor / Active Directory Federation Services	
Microsoft Entra - Sign-in	<ul style="list-style-type: none"><li>• Microsoft Entra sign-ins - Successful events</li><li>• Microsoft Entra sign-ins - Failed events</li></ul>

## Searching for specific event data (Quick Search)

Performing a quick search allows you to search through all events based on a specific value, term, or keyword. You can also modify which columns to display and how the content is displayed.

**i** **NOTE:** The results returned will only include activity from the last 365 days.

### To search for data within an event

1. Enter the search term in the **Quick Search** box and click the magnifying glass icon.

The resulting lists display all events that have a value matching the search term or value, sorted by the time detected and with the Donut chart displayed and grouped by Activity. The search terms are highlighted in the search results and event details to allow you to quickly scan for matches.



**NOTE:** You can also export the search results to a .csv or zip file by selecting the Export button. The location for the file is determined by your browser settings.

### **To edit the display layout**

1. Click **Edit Layout** to rearrange, add, and remove columns as required and select the visualization options.
  - a. Using the Columns menu, drag and drop the columns to change the order.
  - b. To add a column, click **Add Column**.
  - c. To remove a column, click the - next to the appropriate column.
  - d. Select the Visualize menu and choose how to visualize the results. You can choose between a **Chart & Grid**, **Grid** only, or **Chart** only. If you select to display as a chart, you can further refine the display by selecting the type of chart and how you want to group and summarize the data.
  - e. Click **Preview** when you are satisfied with the edits.

## Working with critical activity

The Critical Activity page displays a full list of security-related activity, including anomaly detection for unusual spikes in activity, that may indicate a threat to your organization.

By default, the activity is displayed based on priority from high to low. You can sort and filter the list based on priority, critical activity, and event count and select to hide or remove specific events from the display.

From this page, you can see tailored visualizations and metrics to provide more context about the activity and related search and a high-level overview of the item.

This information helps determine if the activity is expected behavior, an actual issue. Anomaly detection allows you to gain further insight into configuration issues which could impact user experience and service availability and help identify compromised devices or malicious activity.



### **NOTE:**

- Any detected anomalies include an exclamation point in the icon.
- As events are analyzed and the baselines are updated, the data in the charts will update accordingly. Because of this, some items may disappear in the critical activity pane if they no longer are included in the activity spike.
- Anomaly detection depends on the users' a time zone. As a result, users within the same organization may see a different set of anomalies.

### **To view critical activity and configure the display:**

1. Select **Critical Activity**, and click the activity of interest. When you select an activity, a chart displays information by percentage of user, target, or activity or by number of events per target. For anomalies and unusual spikes in activity, the resulting chart displays the baseline (predicted value), anomalies (unusual increase), and total amounts of activity. For all other critical activity the targets associated with the event are displayed in a donut chart. You can select which targets to include in the visualization by selecting (and de-selecting) entries from the legend.

2. Click on any section of the chart for specific search details, or select **View All Events** to see all related searches.
3. If you select a section of the donut chart or a data point on the time series chart for an anomaly, the filtered search will display the associated visualization so that you can quickly view the details of the activity.
4. If required, select **Dismiss Activity** to remove the reported results until the next activity is detected or just select to hide future occurrences of this event.
5. If you have hidden any events and want them added back to the display, select **Edit Hidden Items**, click the events that you want added back to the view, **Remove Selected Items**, and **Save**.
6. To filter the list of critical events, select **Filter**, choose if you want to filter on priority (High, Medium, Low), specific critical activity, or number of events.

## Working with searches

- [Working with private and shared searches](#)
- [Running a search](#)
- [Using built in searches](#)
- [Filtering Searches](#)
- [Creating a custom search](#)
- [Copying an existing search](#)
- [Exporting a search](#)
- [Creating a search from an existing search](#)
- [Creating or filtering a search based on event details](#)
- [Appendix - Available Audit Search Columns and Filters](#)
- [Customizing the search display](#)
- [Viewing search results and event details](#)
- [Copying event details](#)
- [Modifying a search](#)
- [Deleting a search](#)
- [Working with categories](#)

## Working with private and shared searches

When you create a search, you have the option of selecting whether it will be private or shared.

- Private searches are only visible to the individual who created them.
- Shared searches are visible to all Audit users and allow for collaboration with multiple users from the same organization.

**NOTE:**

- The ability to set the search type as private or shared depends on your assigned access role. For details, see [Access Control](#)
- Private search names must be unique among all categories for each user.
- Shared search name must be unique among all shared searches in all categories in the organization
- All private searches (as well as searches under the My Searches category) are listed under the All Private Searches category.
- Shared searches include an information icon that allows you to see when they were created, last saved, and by whom.

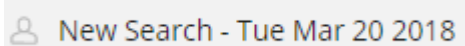
See [Creating a custom search](#), [Creating a search from an existing search](#), and [Modifying a search](#)

## Running a search

Once an event is captured, you can view all available event data through searches. You can use custom searches based on your own criteria or built-in searches that are configured to meet the most common requests. See [Creating a custom search](#) and [Using built-in searches](#).



**NOTE:** Custom user-built searches are identified by the following icon to the left of the search.



### ***To run a previously saved or built-in search***

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. To run the search, simply click it or highlight it and click the run (arrow) icon.

From here you can:

- Select an event to see all the event details.
- Modify the search (Custom user-built searches only). See [Modifying a search](#).
- Refresh the display.
- Select a column to sort the search results by column.
- Create a new search or filter the search based on a specific event detail. See [Creating or filtering a search based on event details](#).
- Create and disable alerts. See [Working with alerts and notification templates](#).

## Using built-in searches

Built-in searches provide quick access to important configuration change details from multiple perspectives. These are shared searches.

While you cannot modify a built-in search directly, you can create a new search based on it and customize the settings to meet your requirements. See [Creating a search from an existing search](#).

The following built in searches are available:

- All Events category
  - All events in the past 24 hours
  - All events in the past 7 days
- [Active Directory Built in searches](#)
- [Active Directory Database built in searches](#)
- [Active Directory Federation Services built in searches](#)
- [Anomaly Activity built in searches](#)
- [Audit Health built in searches](#)
- [Microsoft Entra built in searches](#)
- [Best Practices built in searches](#)
- [BloodHound Tier Zero assets built in searches](#)
- [File System built in searches](#)
- [Group Policy built in searches](#)
- [Logon Activity built in searches](#)
- [Microsoft 365 built in searches](#)
- [Security Management Platform Audit built in searches](#)
- [Teams built in searches](#)
- [Identity Defense built in searches](#)

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

1. Select the **Searches** tab.
2. Locate the search in the required category.
3. Highlight the search and click the arrow icon to run it.

From here you can:

- Select an event to see all the event details.
- Refresh the display.
- Create an alert for the search. See [Working with alerts and notification templates](#)

## **Active Directory Built in searches**

If you have a Change Auditor installation registered with Security Management Platform, you will have access to the following Active Directory built-in searches:

- AD all account lockout events in the past 7 days
- AD all adminCount attribute changed events in the past 30 days
- AD all attribute changes in the past 7 days
- AD all computer events in the past 7 days

- AD all domain controller events in the past 7 days
- AD all events in the past 24 hours
- AD all events in the past 7 days
- AD all events including ActiveRoles/GPOAdmin initiator in the past 7 days
- AD all forest configuration events in the past 7 days
- AD all inheritance settings changed events in the past 30 days
- AD all objects deleted in the past 7 days
- AD all OU events in the past 7 days
- AD all replication events in the past 7 days
- AD all schema configuration events in the past 7 days
- AD all security changes in the last 30 days
- AD all sIDHistory attribute changed events in the past 30 days
- AD all high severity sIDHistory attribute changed events in the past 30 days
- AD all site events in the past 7 days
- AD all user events in the past 7 days
- AD computers added in the past 30 days
- AD computers disabled in the past 30 days
- AD computers enabled in the past 30 days
- AD computers moved in the past 30 days
- AD computers removed in the past 30 days
- AD computers renamed in the past 30 days
- AD critical group membership changes in the past 30 days
- AD group added in the past 30 days
- AD group deleted in the past 30 days
- AD group member added changes in the past 30 days
- AD group member removed changes in the past 30 days
- AD group moved in the past 30 days
- AD group nested member added changes in the past 30 days
- AD group nested member removed changes in the past 30 days
- AD group renamed in the past 30 days
- AD irregular domain controller registration events in the past 30 days
- AD irregular domain replication detected events in the past 30 days
- AD user ServicePrincipalName attribute changes in the past 30 days
- AD users added in the past 30 days
- AD users added to group in the past 30 days
- AD users deleted in the past 30 days

- AD users disabled in the past 30 days
- AD users enabled in the past 30 days
- AD users locked out in the past 30 days
- AD users moved in the past 30 days
- AD users removed from group in the past 30 days
- AD users renamed in the past 30 days
- AD users unlocked in the past 30 days

See [Change Auditor Integration](#) for details on adding on-premises event data to your Security Management Platform deployment.

## Active Directory Federation Services built in searches

Audit provides the following Active Directory Federation Services built in searches:

- AD FS All claims provider trust events in the past 30 days
- AD FS All relying party trust events in the past 30 days
- AD FS All endpoint events in the past 30 days
- AD FS All authentication method changes in the past 30 days
- AD FS All server farm events in the past 30 days
- AD FS Authentication method registered and unregistered events in the past 30 days

## Active Directory Database built in searches

Audit provides the following Active Directory Database built in search:

- AD DB all events in the past 7 days

## Anomaly Activity built in searches

Audit provides the following anomaly activity built in searches:

- All anomaly detected events in the past 30 days
- Unusual increase in AD account lockout events in the past 30 days
- Unusual increase in failed AD change events in the past 30 days
- Unusual increase in failed AD Federation Services sign-ins in the past 30 days
- Unusual increase in failed file access attempts in the past 30 days
- Unusual increase in file deletes in the past 30 days
- Unusual increase in file renames in the past 30 days
- Unusual increase in files shared from OneDrive and SharePoint events in the past 30 days
- Unusual increase in Microsoft 365 activity by guest user events in the past 30 days
- Unusual increase in Microsoft 365 activity by anonymous user events in the past 30
- Unusual increase in permission changes to AD object events in the past 30 days

- Unusual increase in share access permission changes in the past 30 days
- Unusual increase in successful AD Federation Services sign-ins in the past 30 days
- Unusual increase in successful tenant sign-in events in the past 30 days
- Unusual increase in tenant sign-in failure events in the past 30 days
- Unusual increase in Teams guest participant events in the past 30 days
- Unusual increase in successful on-premises sign-ins in the past 30 days
- Unusual increase in failed on-premises sign-ins in the past 30 days

## **Audit Health built in searches**

Audit provides the following Audit Health built in searches:

- Change Auditor Installation activity changes in the past 30 days
- Change Auditor Installation connectivity events in the past 30 days
- Change Auditor Installation setting changes in the past 30 days
- Change Auditor Installation upgrade events in the past 30 days
- Service activity changes in the past 30 days
- Service auditing enabled or disabled events in the past 30 days
- SpecterOps BloodHound Enterprise connectivity events in the past 30 days
- SpecterOps BloodHound Enterprise configuration changes in the past 30 days
- Subscription expiring events in the past 90 days

## **Microsoft Entra built in searches**

Audit provides the following Microsoft Entra built-in searches that are based on the most common and complex requests for information:

- Microsoft Entra application events in the past 7 days
- Microsoft Entra directory events in the past 7 days
- Microsoft Entra events in the past 7 days
- Microsoft Entra failed sign-in events in the past 7 days
- Microsoft Entra group events in the past 7 days
- Microsoft Entra group member changes in the past 7 days
- Microsoft Entra group owner changes in the past 7 days
- Microsoft Entra risk events in the past 7 days
- Microsoft Entra role events in the past 7 days
- Microsoft Entra role member changes in the past 7 days
- Microsoft Entra self-service password management events in the past 7 days
- Microsoft Entra sign-in events in the past 7 days
- Microsoft Entra successful sign-in events in the past 7 days
- Microsoft Entra tenant level configuration changes in the last 180 days

- Microsoft Entra user created events in the past 7 days
- Microsoft Entra user deleted events in the past 7 days
- Microsoft Entra user events in the past 7 days
- Important changes for critical Microsoft Entra directory roles in the past 7 days
- Objects added/removed from Microsoft Entra groups in the past 7 days
- Objects added/removed from Microsoft Entra roles in the past 7 days
- Users added/removed as owner of Microsoft Entra groups in the past 7 days

## Best Practices built in searches

Audit provides the following Best Practices built in searches:

- Microsoft Entra successful application consent events in the past 30 days
- Sharing operations on important file types within past 7 days
- Teams guest access enabled or disabled in the past 30 days

## BloodHound Tier Zero assets built in searches

Audit provides the following BloodHound Tier Zero assets built in searches:

- All Microsoft Entra Tier Zero AD risk events in the past 60 days
- All Microsoft Entra Tier Zero application changes in the past 60 days
- All Microsoft Entra Tier Zero group changes in the past 60 days
- All Microsoft Entra Tier Zero principal logons in the past 60 days
- All Microsoft Entra Tier Zero role changes in the past 60 days
- All Microsoft Entra Tier Zero service principal changes in the past 60 days
- All Microsoft Entra Tier Zero tenant level and directory activity in the past 60 days
- All Microsoft Entra Tier Zero user changes in the past 60 days
- All Tier Zero computer changes in the past 60 days
- All Tier Zero domain and forest configuration changes in the past 60 days
- All Tier Zero group changes in the past 60 days
- All Tier Zero group policy item and object changes in the past 60 days
- All Tier Zero user changes in the past 60 days
- Local logons to Tier Zero computers in the past 60 days
- Security changes to Tier Zero domain objects in the past 60 days
- Security changes to Tier Zero group objects in the past 60 days

- Security changes to Tier Zero group policy objects in the past 60 days
- Security changes to Tier Zero computer objects in the past 60 days
- Security changes to Tier Zero user objects in the past 60 days
- Tier Zero user logons to computers that are not Tier Zero in the past 60 days

## File System built in searches

Audit provides the following File System built in searches:

- FS all events in the past 7 days
- FS all permission and ownership changes to SYSVOL on domain controllers in the past 30 days
- FS all local share changes in the past 30 days
- FS all file and folder creates, deletes, and moves in the past 30 days
- FS all file and folder attribute changes, modifications, and renames in the past 30 days
- FS all file and folder auditing changes in the past 30 days
- FS all file and folder ownership changes in the past 30 days
- FS all file and folder permission changes in the past 30 days
- FS all file and folder failed access attempts in the past 30 days
- FS all file changes with suspicious file extensions in the past 30 days

## Group Policy built in searches

Audit provides the following Group Policy built in searches:

- Group Policy all events in the past 7 days
- Group Policy all restricted group changes in the past 30 days
- Group Policy all security changes in the past 30 days
- Group Policy domain level linked changes in the past 30 days

## Logon Activity built in searches

Audit provides the following logon activity built in searches:

- AD FS All Active Directory Federation Services sign-ins in the past 24 hours
- AD FS All Failed Active Directory Federation Services sign-ins in the past 7 days
- AD FS All Successful Active Directory Federation Services sign-ins in the past 24 hours
- Logon Activity all authentication activity in the past 7 days
- Logon Activity all excessive Kerberos ticket lifetime events in the past 30 days
- Logon Activity all failed logon activity in the past 7 days
- Logon Activity all interactive logon activity in the past 24 hours
- Logon Activity all Kerberos authentication activity in the past 24 hours

- Logon Activity all Kerberos service tickets created with unsafe encryption type in the past 30 days
- Logon Activity all logon activity in the past 24 hours
- Logon Activity all logon session activity in the past 24 hours
- Logon Activity all NTLM version 1 logons in the past 7 days (Note: The associated event class is disabled by default in Change Auditor.)
- Logon Activity all remote logon activity in the past 24 hours

## Microsoft 365 built in searches

Identity Defense provides the following Microsoft 365 built-in searches that are based on the most common and complex requests for information

- Email forwarding enabled in the past 7 days
- Microsoft 365 activity from ad-hoc external recipients in the past 7 days
- Microsoft 365 events from EXT Users in the past 7 days
- Microsoft 365 events in the past 7 days
- Microsoft 365 Exchange Online administrative cmdlets executed in the past 7 days
- Microsoft 365 Exchange Online events in the past 7 days
- Microsoft 365 Exchange Online mailbox events in the past 7 days
- Microsoft 365 Exchange Online mailbox login activity in the past 24 hours
- Microsoft 365 Exchange Online mailbox non-owner activity in the past 7 days
- Microsoft 365 OneDrive for Business events in the past 7 days
- Microsoft 365 OneDrive for Business file activity events in the past 7 days
- Microsoft 365 OneDrive for Business folder activity events in the past 7 days
- Microsoft 365 SharePoint Online events in the past 7 days
- Microsoft 365 SharePoint Online file activity events in the past 7 days
- Microsoft 365 SharePoint Online folder activity events in the past 7
- OneDrive for Business and SharePoint Online anonymous link events in the past 180 days

## Security Management Platform Audit built in searches

Audit provides the following Security Management Platform Audit built in searches:

- All Security Management Platform Audit configuration events in the past 30 days
- All Security Management Platform Audit events in the past 30 days
- Security Management Platform Audit notification template management events in the past 30 days
- Security Management Platform Audit alert ran events in the past 30 days
- Security Management Platform Audit alert rule management events in the past 30 days
- Security Management Platform Audit all shared search and shared category management events in the past 30 days

## Teams built in searches

Audit provides the following Teams searches:

- Teams app events in the past 7 days
- Teams bot events in the past 7 days
- Teams channel events in the past 7 days
- Teams client configuration changes in the past 30 days
- Teams connector events in the past 7 days
- Teams events in the past 7 days
- Teams guest access configuration changes in the past 30 days
- Teams guest members added in the past 7 days
- Teams member role changes in the past 7 days
- Teams member changes in the past 7 days
- Teams notification and feeds policy changes in the past 30 days
- Teams organization setting changes in the past 30 days
- Teams tab events in the past 7 days
- Teams targeting policy changes in the past 30 days
- Teams team created events in the past 30 days
- Teams team deleted events in the past 30 days
- Teams team setting changes in the past 7 days
- Teams user sign-in events in the past 7 days

## Identity Defense built in searches

Audit provides the following Identity Defense built in searches:

- All Identity Defense events in the past 24 hours
- All Identity Defense events in the past 7 days
- Identity Defense Detected Anomaly indicators in the past 30 days
- Identity Defense Detected TTP indicators in the past 30 days
- Identity Defense Hygiene indicators in the past 30 days
- Identity Defense Detected Protected indicators in the past 30 days
- Identity Defense Privileged Microsoft Entra objects added in the past 30 days
- Identity Defense Privileged Microsoft Entra objects certified in the past 30 days
- Identity Defense Privileged Microsoft Entra objects removed in the past 30 days
- Identity Defense Privileged Microsoft Entra objects uncertified in the past 30 day
- Identity Defense Tier Zero objects added in the past 30 days
- Identity Defense Tier Zero objects removed in the past 30 days
- Identity Defense Tier Zero objects certified in the past 30 days

- Identity Defense Tier Zero objects uncertified in the past 30 days
- Identity Defense all indicators muted and unmuted in the past 30 days
- Identity Defense all objects muted and unmuted in the past 30 days
- Identity Defense all Tier Zero objects protected in the past 30 days
- Identity Defense all AD DB objects protected in the past 30 days
- Shields Up enabled in the past 30 days
- Shields Up disabled in the past 30 days
- Shields Up override account changes in the past 30 days

## Filtering Searches

To streamline and customize your search experience, you can construct queries using groups of clauses with flexible logic options. Each group allows you to define whether clauses within it are evaluated using AND or OR logic, and you can also choose how multiple groups interact with one another. Within each clause, you specify a field, condition, and value, and you can easily add or remove clauses and groups to refine your results.

For a complete list of available columns, filters, and predefined values, refer to [Appendix - Available Audit Search Columns and Filters](#). These resources will help you locate the information you need to effectively secure your environment.



### TIP: Tips for Effective Searching

- Use All of when you're looking for very specific matches.
- Use Any of when you're exploring broader patterns or possibilities.
- Combine multiple clauses within a group to refine logic before applying group-level connectors.
- You can choose only one type of connector between clause groups: Either all ANDs (narrow search, or all ORs (broader search). You cannot mix AND and OR between groups.

### What Are Clause Groups?

Clause groups are sets of conditions (clauses) that define what data you're looking for. Each clause typically includes:

- A field (such as, Time Detected, Action, Country)
- A condition.
 

The available string operators include: equals, does not equal, contains, does not contain, in, not in, starts with, does not start with, ends with, does not end.

The available integer operators for sign-in events include equals\_number, does\_not\_equal\_number, greater\_than, greater\_than\_or\_equals, less\_than, less\_than\_or\_equals, and between\_number.

The available date and time operators include during last number of days or hours (By default, this is set to the last 7 days for all new searches.), between, before, and after.
- A value (such as, 7 days, Delete Object, Canada)

You can add multiple clauses to a group, and multiple groups to a query.

### Using "Any of" vs. "All of" in Clause Group Filters

When building advanced search queries, clause groups allow you to organize multiple conditions. The connector option—Any of or All of—controls how these groups are evaluated together.

At the top of the clause group section, use the + to choose how groups are connected:

- **All of (and)**

All clause groups must be true for a result to match. Use this when you want to narrow your search.

Example:

Time Detected during last 7 days

AND Action equals Delete Object

AND Country equals Canada

Only results that meet all three conditions will be shown.

- Any of (or)

At least one clause group must be true for a result to match. Use this when you want to broaden your search.

Example:

Time Detected during last 7 days

OR Action equals Delete Object

OR Country equals Canada

Results that meet any one of these conditions will be shown.

### **Example Use Case: Filtering Events by Access Policy**

Goal: A security analyst wants to find events from the last 7 days that match either of two access control policies.

#### **Step-by-Step Setup:**

- Create Clause Group 1:

Time Detected → during last → 7 days

Access Control Policy → contains → "AdminAccess"

- Create Clause Group 2:

Time Detected → during last → 7 days

Access Control Policy → contains → "GuestAccess"

- Set Clause Group Connector:

Use the top clause group connector menu to select Any of or).

This ensures the query returns events that match either group.

- Result:

The system will return:

Events from the last 7 days with AdminAccess, or

Events from the last 7 days with GuestAccess

### To use the search filter:

1. Under the **Searches** tab, select the search.
2. Click the pencil icon to modify the search. The type of search (private or shared) and the current category is displayed at the top of the search.
3. Edit the search filter as required.

Add the required search filter and select either **Any of (or)** or **All of (and)** to set how the filters are to be evaluated together.

Add any required additional sets of conditions (clause groups) for the filter by selecting **Add New Clause Group**, and choosing whether they should be ALL or OR conditions between the clauses.

## Creating a custom search

Custom searches allow you to locate and report on the data that is of interest to you. The associated search preview updates as you construct a search to ensure you are getting the desired results. For options, see [Customizing the search display](#).

### **i** NOTE:

- Private search names must be unique among all categories for each user.
- Shared search name must be unique among all shared searches in all categories in the organization

### To create a search

1. Under the **Searches** tab, click **New Search**.
2. Enter a name for the search.
3. Click **Add** to enter the required search criteria.
4. Select as many filters as required. Search terms are highlighted in the preview (and search results and event details) to allow you to quickly scan for matches. See [Filtering Searches](#) and [Appendix - Available Audit Search Columns and Filters](#) for details.
5. Click **Edit Columns** to arrange, add, and remove the columns displayed in the search. See [Customizing the search display](#).
6. Click **Save**. By default, the new search will be created in the category you have selected when clicking **New Search**. If required select a different category.
7. Select whether this is a private or shared search. [Working with private and shared searches](#).
8. Click **Save**.
9. If required, click **Alert**, select the required notification template (or create a new one) to notify the required individuals, click **Save**. See [Working with alerts and notification templates](#)

## Copying an existing search

Copying an existing search allows you to take advantage of existing settings and modify as required.

1. Under the **Searches** tab, select the search.
2. Click the copy icon. The search is created with "Copy" appended to its name.

3. Enter a new name and change the category, if required, by selecting a new category from the drop don list.
4. Select whether this is a private or shared search. See [Working with private and shared searches](#).
5. Click **Copy**.

The new search is now available to edit as required.

## Exporting a search

### **i** NOTE:

- 50 000 is the maximum number of results that can be exported at once. You will need to refine the search before exporting if the results exceed this number.
- The maximum download size is 250 MB. If this size is reached, only complete results will be included, the rest will be truncated. For searches with a large number of results, the ZIP option should be used.

### **To export a search**

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. Run the search.
4. From the **Export** button, select to export to a CSV or CSV as ZIP file. The location for the file is determined by your browser settings.

## Creating a search from an existing search

Creating a search based on an existing search allows you to add granularity by adjusting the filters, category, and columns to suit your specific needs.

### **To create a new search based on an existing custom or built in search**

1. Under the **Searches** tab, select the search.
2. Click the pencil icon to modify the search.
3. Remove, add, edit search criteria as required. Search terms are highlighted in the preview (and search results and event details) to allows you to quickly scan for matches. See [Filtering Searches](#) and [Appendix - Available Audit Search Columns and Filters](#) for details.
4. If required, click **Edit Columns** to rearrange, add, and remove columns. See [Customizing the search display](#).
5. Select **Save As**.
6. Edit the search name and select the category.
7. Select whether this is a private or shared search. [Working with private and shared searches](#).
8. Click **Save**.
9. If required, click **Alert**, select the required notification template (or create a new one) to notify the required individuals , click **Save**. See [Working with alerts and notification templates](#)

## Customizing the search display

When you create a search, a preview displays to help ensure the search criteria meet your needs. You can easily customize the columns that display in the generated report and set how you want the report results displayed through the visualization settings.

**i** **NOTE:** Some columns are included by default, such as Time Detected, User (Actor), Activity, Target, Origin IP, Service, Status, and Tenant Name. For a list of available columns, see [Appendix - Available Audit Search Columns and Filters](#)

### ***To customize the display of the search results***

1. As you create a search, click **Edit Columns**.
2. Drag and drop the columns to change the order.
3. To remove a column, click the - next to the appropriate column.
4. To add a column, click **Add Column**.
5. Select the Visualize menu and choose how to visualize the results. You can choose between a **Chart & Grid**, **Grid** only, or **Chart** only.
6. If you select to display as a chart & Grid or Chart, you can further refine the display by selecting the type of chart (horizontal bar chart, time series, or donut) and how you want to group and summarize the data.
7. Click **Preview** to view your changes.
8. Click **Save** to save your changes.

If you have selected to visualize the search in a donut or bar chart, you can add and remove items from the display by clicking to clear or enable them from the legend, and select a section of the donut or bar to view more details.

## Viewing search results and event details

When selecting an event that has been returned from a search, you can view all the details of the activity that triggered the event. If the search contains string filters, the string is highlighted in the search results and event details to allow you to quickly scan for matches.

A summary of important event details is displayed at the top of the event details that includes:

- Activity Name
- Service
- Time Detected
- User display name
- Target
- Location
- Status (Successful/Failed)

For Microsoft Entra, Active Directory, and Group Policy events, the summary also displays the following:

- Property After Value
- Property Before Value
- Property Name

### **To view event details**

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. Highlight the search and click the arrow icon to run it.
4. Click an event to open a new window that contains all the event details.
5. Click the **Event Link** to create a dedicated page for the event details. Once created you can view the information, copy the URL to share with others, or bookmark it for future use.

## Copying event details

When selecting an event that has been returned from a search, you can copy the event details to clipboard to paste into another application.

### **To copy event details**

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. Highlight the search and click the arrow icon to run it.
4. Click an event to open a new window that contains all the event details.
5. Select **Copy to clipboard** to copy all event details to a clipboard.

## Modifying a search

You can easily modify a search to gather the information your require as long you have the right to do so.

### **i NOTE:**

- Only custom searches can be modified.
- Built in searches cannot be modified. However, you can create a new search based on it and customize the settings to suit your needs. See [Creating a search from an existing search](#).

### **To modify a search**

1. Under the **Searches** tab, select the search.
2. Click the pencil icon to modify the search. The type of search (private or shared) and the current category is displayed at the top of the search.
3. Edit the search name, remove, add, edit search criteria as required. Search terms are highlighted in the preview (and search results and event details) to allows you to quickly scan for matches. See [Filtering Searches](#) and [Appendix - Available Audit Search Columns and Filters](#) for details.

4. Change the category, if required by selecting a new category from the drop down list.
5. Click **Edit Columns** to rearrange, add, and remove columns as required and select the visualization options.
  - a. Drag and drop the columns to change the order.
  - b. To add a column, click **Add Column**.
  - c. To remove a column, click the - next to the appropriate column.
  - d. Select the Visualize menu and choose how to visualize the results. You can choose between a **Chart & Grid**, **Grid** only, or **Chart** only. If you select to display as a chart, you can further refine the display by selecting the type of chart and how you want to group and summarize the data.
  - e. Click **Apply** when you are satisfied with the edits.
6. Select whether this is a private or shared search. [Working with private and shared searches](#).
7. Click **Save** to apply the changes.
8. If required, click **Alert**, select the required notification template (or create a new one) to notify the required individuals, click **Save**. See [Working with alerts and notification templates](#)

## Deleting a search

### *To remove a search*

1. Select the **Searches** tab.
2. Locate the required search in the list of categories.
3. Highlight the search and click the **X** icon to delete it.
4. Click **Delete** to confirm the removal.

## Working with categories

When you create a category, you have the option of selecting whether it will be private or shared.

- Private categories are only visible to the individual who created them.
- Shared categories are visible to all Audit users and allow for collaboration with multiple users from the same organization.

By default, the following categories are available:

- All Private Searches: All private searches belonging to the signed-in user.
- All Searches: All configured searches.
- Active Directory: All Active Directory events in the last 24 hours, 7 days, and 30 days.
- Active Directory Federation Services: Sign-ins and configuration changes made through Active Directory Federation Services.
- All Events: All events in the last 24 hours and 7 days.
- Microsoft Entra: Microsoft Entra application, directory, group, role, self-service password, user created, user deleted, and user events in the last 7 days.
- Best Practices: Sharing operations on important file types and Teams guest access events.

- Group Policy: Group Policy events.
- Logon Activity: Logon activity events.
- Microsoft 365: Microsoft 365 and SharePoint online events.
- Security Management Platform Audit: All Security Management Platform audit and alert events.
- Teams: Teams user and administrator activity events.
- My searches: A built-in private category.

### **To create a category**



#### **NOTE:**

- Private category names must be unique among all categories for each user.
  - Shared category name must be unique among all shared searches in all categories in the organization.
1. Under the **Searches** tab, click **Add** in the Categories field.
  2. Enter the category name.
  3. Select whether the category is private or shared.
  4. Click **Add**.

### **To assign a search to a new category**

1. Under the **Searches** tab, select the search.
2. Click the pencil icon to modify the search.
3. Drop down the **Category** field and select the required category.
4. Click **Save**.

### **To edit the name of a category**

1. Under the **Searches** tab, select the category.
2. Highlight the category, and click the pencil icon to the left of the category.
3. Enter a new name for the category and click **Save**.

## **Working with alerts and notification templates**

Alerts allow those responsible for the security of your environment to receive detailed information about vital changes and activities as they occur. The associated notification templates allow you to configure who will receive the alerts so that they can take the appropriate action to address the outlined risks to your environment.

From the Alerts tab you can:

- View the number of alerts created in the last 24 hours for each search.
- View the number of associated notification templates.
- Enable, disable, and remove alerts.
- Review searches that have alerts created for them.

- Review the associated notification templates.
- Select an information icon to see when shared alerts were created, last saved, and by whom.

Notification templates are managed through Security Management Platform global settings. Select **Settings | Notification** to manage notification templates. From here you can:

- View all the alerts associated with each notification template and the number of alerts it includes.
- See whether the notification template is private (only visible to the individual who created it) or shared (visible to all Audit users allowing for collaboration with multiple users from the same organization).
- See who added the notification template and when it was created.
- Select an information icon to see when notification templates were created, last saved, and by whom.
- Add, edit, and remove notification templates.

For details on working with notification templates, see [Notifications](#) in the Security Management Platform Global Settings User Guide.

**i NOTE:**

- You can select to assign any number of notification templates to an alert.
- When you create or modify a notification template, you have the option of selecting whether it will be private or shared.
- When enabling or editing an alert for a private search, only private notification templates can be used or created.
- When enabling or editing an alert for a shared search, only shared notification templates can be used or created.
- A notification template cannot be removed until all alerts linked to it are removed or reassigned.

***To create an alert and associate it with an existing notification template***

1. Under the **Searches** tab, select the search.
2. Click **Alert**.
3. Select an existing notification template, and click **Save**.
4. Select **View Template** to review and manage the notification template settings.

***To create an alert and associate it with a new notification template***

1. Under the **Searches** tab, select the search.
2. Click **Alert**.
3. Select **Create new shared notification template**, enter a name for it, and click **Save**.

4. Click **Edit** to specify or modify the notification template recipients and control whether the system sends email alerts.
  - a. When the Email Notifications toggle is On, email notifications are enabled, and emails will be sent for relevant updates. To disable notifications, click the toggle so it switches to Off.
  - b. Add recipients by role or by entering the required email addresses and click **Add Recipients** as needed.
  - c. remove recipients from the **Selected Recipients** list select to **Remove** as needed.
5. Select to **Send Test Email** as needed.
6. Click **Save**.

### **To edit an alert**

1. Under the **Alerts** tab, select the required alert.
2. Click **Edit Alert** to add and remove the notification template associate with the alert as required.
3. Click **Save**.
4. Select **View Template** to review and manage the notification template settings.

### **To remove an alert**

1. Under the **Alerts** tab, select **Alerts**.
2. Select the required alert, and click the **X** icon to delete it.
3. Click **OK** to confirm the deletion.

## **Using built in alerts and notification templates**

Built in alerts and notification templates are available to ensure that you are kept up to date on critical activity within your organization. All searches within the Audit Health, Anomaly Activity, and Bloodhound Tier Zero assets categories are alert-enabled and linked to the associated built in notification templates.



### **NOTE:**

- You need to add yourself to receive notifications. For details on working with notification templates, see [Notifications](#) in the Security Management Platform Global Settings User Guide.
- Built in notification templates cannot be deleted; you can, however, enable and disable the alerts as required.

The following built in notification templates are available:

- Audit Health
- Anomaly Activity
- Tier Zero

The following built in alerts are available and enabled:

- All anomaly detected events in past 30 days

- All Microsoft Entra Tier Zero AD risk events in the past 60 days
- All Microsoft Entra Tier Zero application changes in the past 60 days
- All Microsoft Entra Tier Zero group changes in the past 60 days
- All Microsoft Entra Tier Zero principal logons in the past 60 days
- All Microsoft Entra Tier Zero role changes in the past 60 days
- All Microsoft Entra Tier Zero service principal changes in the past 60 days
- All Microsoft Entra Tier Zero tenant level and directory activity in the past 60 days
- All Microsoft Entra Tier Zero user changes in the past 60 days
- All Tier Zero computer changes in the past 60 days
- All Tier Zero domain and forest configuration changes in the past 60 days
- All Tier Zero group changes in the past 60 days
- All Tier Zero group policy item and object changes in the past 60 days
- All Tier Zero user changes in the past 60 days
- Local logons to Tier Zero computers in the past 60 days
- Security changes to Tier Zero domain objects in the past 60 days
- Security changes to Tier Zero group objects in the past 60 days
- Security changes to Tier Zero group policy objects in the past 60 days
- Security changes to Tier Zero computer objects in the past 60 days
- Security changes to Tier Zero user objects in the past 60 days
- Tier Zero user logons to computers that are not Tier Zero in the past 60 days
- Change Auditor Installation connectivity events in the past 30 days
- Change Auditor Installation setting changes in the past 30 days
- Change Auditor Installation upgrade events in the past 30 days
- Service activity changes in the past 30 days
- Service auditing enabled or disabled events in the past 30 days
- Subscription expiring events in the past 90 days
- Unusual increase in tenant sign-in failure events in the past 30 days
- Unusual increase in AD account lockout events in the past 30 days
- Unusual increase in successful tenant sign-in events in the past 30 days
- Unusual increase in failed AD change events in the past 30 days
- Unusual increase in permission changes to AD object events in the past 30 days
- Unusual increase in files shared from OneDrive and SharePoint events in the past 30 days
- Unusual increase in Microsoft 365 activity by guest user events in the past 30 days
- Unusual increase in Microsoft 365 activity by anonymous user events in the past 30
- Unusual increase in Teams guest participant events in the past 30 days

# Auditing Microsoft Entra

Audit simplifies tracking, auditing, and reporting on activity that corresponds to the events in the Microsoft Entra audit logs, sign-in activity report, and risky sign-ins report.

**i** | **NOTE:** An Microsoft Entra ID Premium (P1) license or higher is required for to audit sign-in and Microsoft Entra ID Premium (P2) license or higher to audit risky sign-in activity.

You can generate intelligent and in-depth reports, protecting you against policy violations and avoiding the risks and errors associated with day-to-day modifications.

For example, you can easily track and report on activities such as:

- When users and groups are added to and removed from the directory.
- When user and group attributes are changed.
- Successful and failed logins.
- Suspicious sign-in activity.

## Event collection and Microsoft Entra subscription

Historical auditing is dependent on your Microsoft Entra subscription.

Subscription	Event Collection
Microsoft Entra ID license	Microsoft Entra- Audit Log historical events in the last 7 days
Microsoft Entra ID premium license (Optional)	Microsoft Entra- Audit Log historical events in the last 30 days
Microsoft Entra ID premium license (Required)	Microsoft Entra- Sign-ins historical events in the last 30 days
Microsoft Entra ID Premium license (Required)	Microsoft Entra- Risky Sign-ins historical events in the last 90 days

**i** | **NOTE:** Microsoft Entra ID Premium P2 subscription is required to include the Risk Level and Risk Detail information in events.

## Working with Microsoft Entra Searches

Numerous [Microsoft Entra built in searches](#) are available that allow you to locate and report on the Microsoft Entra data. If required, you can also easily create custom searches to locate specific information that is of interest to you.

There are numerous columns, filters, and pre-defined values that you can use to help you find the information you need to secure your environment.

See [Creating a custom search](#) and [Appendix - Available Audit Search Columns and Filters](#) for more details.

### Microsoft Entra- specific columns

The following columns are available to display additional Microsoft Entra information:

Audit module	Columns
Microsoft Entra - Audit Log	<ul style="list-style-type: none"> <li>Microsoft Entra Activity Type</li> <li>Microsoft Entra Activity Operation Type</li> <li>Microsoft Entra Result Description</li> <li>Microsoft Entra Category</li> </ul>
Microsoft Entra Sign-ins	<ul style="list-style-type: none"> <li>Error Code</li> <li>Failure Reason</li> <li>Location</li> </ul>
Microsoft Entra Risky Sign-ins	<ul style="list-style-type: none"> <li>RiskEventStatus</li> <li>RiskEventId</li> <li>RiskEventType</li> <li>RiskLevel</li> <li>RiskEventDateTime</li> <li>PreviousCity (impossible travel risk events only)</li> <li>PreviousState (impossible travel risk events only)</li> <li>PreviousCountry (impossible travel risk events only)</li> <li>PreviousSignInDateTime (impossible travel risk events only)</li> <li>PreviousIpAddress (impossible travel risk events only)</li> <li>PreviousLocation (impossible travel risk events only)</li> <li>RiskEventDetails</li> <li>MalwareName</li> <li>isAtypicalLocation</li> </ul>

## Working with Microsoft Entra events with multiple targets

To help filter searches and fine tune the results, the following Microsoft Entra group membership, group ownership, and role membership activity has been split so that a single event is reported based on the target and subject

Group Membership Event	Target	Subject
Add member to group	Group being modified	User or group added to a group
Add group membership	User or group added to a group	Group being modified
Remove member from group	Group from which a user or group is removed	User or group being removed from a group
Remove group membership	User or group being removed from a group	Group from which the user or group is removed

Group Membership Event	Target	Subject
Add owner to group	Group that is modified	User added as group owner
Group ownership assigned	User added as group owner	Group that is modified
Remove owner from group	Group that is modified as a result of a removed owner	User removed as group owner
Group ownership removed	User removed as group owner	Group that is modified as a result of a removed owner

Role Event	Target	Subject
Add member to role	Role to which a user is added	User added to the role
Role assignment added	User added to a role	Role to which a user is added
Remove member from role	Role from which a user is removed	User removed from a role
Role assignment removed	User removed from a role.	Role from which a user is removed
Add eligible member to role	Role to which a user is added	User added to a role
Role assignment added to eligible member	User added to a role	Role to which a user is added

### Additional filters

You can, for example, create a search for all group membership events and see distinct events for both the group you are adding a user to and the user you are adding to the group. Using the target to filter your searches allows you to pinpoint the activity by specific users, and changes to critical groups and roles. See [Appendix - Available Audit Search Columns and Filters](#) for a complete list of available filters.

## Auditing risk events

Audit captures both the risk event as well as when an administrator takes action on the detected risk.

**i** **IMPORTANT:** To capture and view this information, ensure that you have enabled auditing of the Microsoft Entra - Audit Logs module.

The following information is listed in the Microsoft Entra risk event's activity.:

- "New risk event detected" event when the Microsoft Entra Identity Protection portal creates a new risk event.
- "Admin dismisses risk event", "Admin reactivates risk" event, and "Admin resolves risk" when the Microsoft audit logs creates an event for an administrator's actions.

# Auditing Microsoft 365

Audit captures activity for Exchange Online, OneDrive for Business, Teams, and SharePoint Online that corresponds to the events in the Microsoft 365 Security & Compliance Center unified audit log.

You can easily track and identify important activities such as:

- When Exchange Online mailboxes are created, deleted, and accessed.
- Permission changes to see which users are granted access to a mailbox.
- Mailbox activity by non-owner such as messages sent, read, deleted, and folders deleted
- Mailbox activity by owner for sensitive and high value mailboxes.
- When files and folders are accessed, created, deleted, uploaded, moved, renamed, and checked in and out of SharePoint Online and OneDrive for Business sites.
- Teams user and administrator activity such as when teams (and associated settings, members, and applications) are created, updated, removed and when users sign in.

For details on running the searches and creating custom searches based off the built in searches, see:

- [Using built in searches](#)
- [Microsoft 365 built in searches](#)

# Findings

Findings allow you to view and investigate notable events in your organization's Active Directory and Entra ID, including:

- Active Directory Tier Zero and Entra ID Privileged object activity, including the identification of unprotected Tier Zero objects.
- Hygiene indicators detected by Assessments.
- Detected TTP and Detected Anomaly Indicators collected by Audit.

**i** **NOTE:**


- Hygiene indicators identified by Assessments show that certain objects may be vulnerable to adversary attacks.
- Detected indicators suggest that an action occurred which could potentially be an adversary attack. Detected TTPs (tactics, techniques, and procedures) are indicators found through search-based detection, while Detected Anomalies are indicators identified through statistical analysis.

**To view Findings:**

- From the left navigation menu, choose **Defend | Findings**.

The Findings list displays the following information for each finding:

- **Finding** name
- **Severity** level

 **NOTE:** Identity Defense calculates severity levels by a range of values (for example, the lower the value, the higher severity). If you sort by this column, you can see the Findings in order of most to least severe.



**Critical**

Generally reserved for Hygiene and Detected Indicators that are changes to Tier Zero and Privileged object security, have significant potential impact to the Active Directory or Entra ID environment, and are not part of the default Active Directory or Entra ID configuration.

Generally reserved for:

- Hygiene and Detected Indicators that are of high concern but impact single objects.
- the discovery of new Tier Zero domain objects and Privileged tenant objects.
- changes to Tier Zero and Privileged objects that occur more often through normal business operations or are part of the default Active Directory or Entra ID configuration.



**High**


Generally reserved for the discovery of:

- Tier Zero user, computer, group, and Group Policy objects.
- Privileged user, role, group, and service principal objects.



**Medium**

- **Type** (Tier Zero, Hygiene, Detected TTP, or Detected Anomaly)
- **Workload** (Active Directory or Entra ID)
- **Last Detected** date and time. (This field displays the signed-in user's local date and time.)
- **Status** (Active or Inactive)

 **NOTE:** If you click the **Filter** button, you can filter displayed results by one or more of the following criteria:

- Finding
- Severity
- Type
- Status

(Active Findings display by default. You can choose to display *either* Active *or* Inactive Findings in the list, but not both.)

From the Findings list you can [dismiss](#) one or more Findings and [view Finding history](#).

## Investigating Findings

From the [Findings list](#), select a Finding to investigate in more detail:

- **Tier Zero** and **Privileged** objects that have been identified by the provider (Identity Defense or BloodHound Enterprise) or added manually by a user.
- **Hygiene and Detected Indicators** that have been found through Identity Defense Assessments and Audit Critical Activity.

From the Investigate Finding page, you can:

- View a summary of the Finding key elements
- Access Identity Defense Intelligence to answer your questions and provide a high-level overview of your environment, including identified Findings and recommended actions to resolve issues.

**i** | **NOTE:**

- Before you can access the Identity Defense Intelligence assistance, you need to read and accept the AI Terms of Use.
- To refresh the Identity Defense Intelligence content in the flyout, click the AI icon next to a different user object.

- Access guiding questions:

- **What Happened?**, or for Hygiene, **What Is Wrong?**
- **How Do I Fix This?**

**i** | **NOTE:** Navigate between questions either by clicking a the name or using the **Next** and **Back** buttons.

## Investigating Tier Zero and Privileged Object Findings

The top of a Tier Zero or Privileged object Investigation page identifies the object being investigated, along with the following information:

- the **Severity** of the Finding
- the Finding **Type** (Tier Zero)
- the **Certification Status** (Certified or Not Certified)
- the **Finding Status** (Active or Inactive)
- **Last Updated** (that is, the last time the Finding was detected)

**i** | **NOTE:** Last Updated displays a relative time. However, if you hover over the clock icon you can see an exact date and time. This field displays the signed-in user's local date and time.

- options to [certify](#) the object, [dismiss](#) the Finding, and [view history](#) of the Finding. and access Identity Defense Intelligence.

### Identity Defense Intelligence

From here you can enter your question directly or select from the following to get started.

- **Summary** offers a concise overview of a specific Finding, including an explanation, the affected objects, real-world examples of similar issues, and suggested follow-up questions to guide further investigation.
- **Related Findings** highlights other active Findings that are connected by object type or potential attack paths, helping you understand broader security implications and offering additional follow-up questions.
- **Additional Information** provides a detailed risk overview, including severity levels, affected objects, potential security threats, real-world exploit incidents, and a security risk review, along with relevant follow-up questions.
- **Remediation** outlines recommended remediation steps, including detailed instructions, and follow-up questions to support implementation.

### What Happened?

This section indicates why a Finding was raised for the object, as well why the object is considered Tier Zero or Privileged and the number of other Tier Zero or Privileged objects that it impacts and is impacted by.

**i** | **NOTE:** If BloodHound Enterprise is the provider, it can return a *maximum* of 1000 related objects for each category.

The What Happened? section also includes a series of links to help you complete your investigation, as described in the following table.

Link	Description
View Details	<p>The properties of the object, including whether it was added by the system (Identity Defense or BloodHound Enterprise) or by a user, identifiers used for the object within Active Directory or Entra ID, the date the object was added and the date its information was last updated.</p> <p><b>i</b>   <b>NOTE:</b> The Date Added field displays the signed-in user's local date and time.</p>
View Relationships	<p>If <a href="#">BloodHound Enterprise is configured</a>, this link enables you to log into BloodHound (if you have at least Read permissions) and view attack paths between the object being investigated and other objects.</p> <p><b>i</b>   <b>NOTE:</b> If Identity Defense is the provider, this option will be hidden.</p>
View Recent Activity	This link opens the <a href="#">Quick Search page</a> , which lists event data for the selected object.
<b>Escalate this Finding</b>	
Copy	This link allows you to copy the text of the Finding to the clipboard so that you can share it with others.
Send email	This link allows you to prepare and send an escalation email to recipients with whom you want to share the Finding.

### How Do I fix this?

This section provides recommendations for investigation and remediation.

**i** | **NOTE:** If BloodHound Enterprise is the provider, the **View Relationships** link to BloodHound Enterprise is also provided in this section.

## Investigating Hygiene and Detected Indicators

Findings for Hygiene and Detected Indicators are raised when:

- vulnerabilities are detected when a Identity Defense Assessment is run

AND/OR


- critical activity anomalies are detected by Audit.

**i** | **NOTE:** **Hygiene** indicates that objects are susceptible to an adversary attack. **Detected** indicates that an action took place that could possibly be an adversary attack.

- **Detected TTP** (tactics, techniques and procedures) Indicators are search-based.
- **Detected Anomaly** Indicators are based on statistical analysis.

The top of an Investigation page identifies the object being investigated, along with the following information:

- Finding **Severity**
- Finding **Type** (Hygiene, Detected TTP, Detected Anomaly)
- **Finding Status** (Active or Inactive)
- MITRE ATT&CK TTP (if applicable)

**i** | **NOTE:** Up to three TTPs may be returned for the finding. If "+ [number]" is shown to the right of the displayed TTP, hover over the  icon to view the additional values.

- Number of **Affected Objects**
- **Last Updated** The last time the Finding was detected)

**i** | **NOTE:** Last Updated displays a relative time. However, you can hover over the clock icon to see an exact date and time (which displays the local date and time of the signed-in user).

- options to **dismiss** the Finding and **view history** of the Finding..

### Identity Defense Intelligence

From here you can enter your question directly or select from the following to get started.

- **Summary** offers a concise overview of a specific Finding, including an explanation, the affected objects, real-world examples of similar issues, and suggested follow-up questions to guide further investigation.
- **Related Findings** highlights other active Findings that are connected by object type or potential attack paths, helping you understand broader security implications and offering additional follow-up questions.

- **Additional Information** provides a detailed risk overview, including severity levels, affected objects, potential security threats, real-world exploit incidents, and a security risk review, along with relevant follow-up questions.
- **Remediation** outlines recommended remediation steps, including detailed instructions, and follow-up questions to support implementation.

### What Happened?/What Is Wrong?

The What Happened? (for Detected Indicators) or What Is Wrong? (for Hygiene) page provides a description of the Finding and lists the objects that are affected. The following information is included for each object:

- **Object Name** (with a link that allows you to display object details.)

User objects also include access to Identity Defense Intelligence.

**i** | **EXCEPTION:** If an Object Type is trustedDomain, Container or dnsZone, object details cannot be displayed from the Investigation page and the Object Name link will be disabled.

- **Principal Name** (which is searchable)

- **Object Type**

- **First Discovered** date and time

**i** | **NOTE:** This field displays the signed-in user's local date and time.


- **Certification Status**, which may be

- Certified or Not Certified (for [Tier Zero](#) or [Privileged](#) objects)  
OR
- Not Tier Zero

**i** | **NOTE:** A status of "Status Not Available" may occur if the object has been deleted from Active Directory/Entra ID or the Object ID cannot otherwise be identified.

This section also includes a series of links to help you complete your investigation, as described in the following table.

Link	Description
<i>For Selected Objects in the list</i>	
Object Name (for a single object)	<p>The properties of the object, including whether or not it is Tier Zero/Privileged, identifiers used for the object within Active Directory or Entra ID, the date the object was added and the date its information was last updated.</p> <p><b>i</b>   <b>NOTE:</b> This field displays the signed-in user's local date and time.</p> <p>For user objects, select the Identity Defense Intelligence icon to view a detailed security overview of the user, including summary information, recent activity, user object changes, location details, related findings, activity analysis, conclusions, and follow-up questions.</p>
Mute Object button	See <a href="#">Muting Findings for Hygiene and Detected Indicators</a> .

Link	Description
View Activity button (for a single object)	This link opens the <a href="#">Quick Search page</a> , which lists event data for the object being investigated.
View Assessment button (for a single object)	<b>If the indicator was raised by a Identity Defense Assessment</b> , this link opens the Assessment Results <a href="#">Vulnerability Detail</a> page that includes the selected object.   <b>NOTE:</b> This button is enabled only when a single object is selected.
View critical activity link	<b>If the indicator was raised by an Audit critical activity event</b> , this link opens <a href="#">Critical Activity event details</a> .
<b>Escalate this Finding</b>	
Copy	This link allows you to copy the text of the Finding to the clipboard so that you can share it with others.
Send email	This link allows you to prepare and send an escalation email to recipients with whom you want to share the Finding.

### How Do I fix this?

This section provides the recommended remediation.

## Using Identity Defense Intelligence with Findings

Identity Defense Intelligence can quickly answer your questions and provide a high-level overview of your environment, including identified Findings and recommended actions to resolve issues.



### NOTE:

- Before you can access the Identity Defense Intelligence assistance, you need to read and accept the AI Terms of Use.
- You can also click the Identity Defense Intelligence icon next to a user account to view a review of the account and ask questions.

### To access Identity Defense Intelligence from findings:

1. From the left navigation menu, choose **Defend | Findings**.
2. Select a Finding and click the Identity Defense Intelligence tab.

3. You can enter your question directly or select from the following to get started.
  - a. **Summary** offers a concise overview of a specific Finding, including an explanation, the affected objects, real-world examples of similar issues, and suggested follow-up questions to guide further investigation.
  - b. **Related Findings** highlights other active Findings that are connected by object-type or potential attack paths, helping you understand broader security implications and offering additional follow-up questions.
  - c. **Additional Information** provides a detailed risk overview, including severity levels, affected objects, potential security threats, real-world exploit incidents, and a security risk review, along with relevant follow-up questions.
  - d. **Remediation** outlines recommended remediation steps, including detailed instructions, and follow-up questions to support implementation.

## Muting Findings for Hygiene and Detected Indicators

You can mute Findings for Hygiene, Detected TTP, and Detected Anomaly Indicators, or individual objects within those Findings, to prevent future Findings from being raised.

**i** | **NOTE:** If you want to mute an indicator entirely, you can do so from the [All Indicators page](#).

### To mute Findings:

From the Findings Investigation page or Findings list (if you are dismissing multiple Findings), [dismiss the Finding](#). When prompted to confirm the dismissal, check the **Mute this Finding** box.

### **i** | NOTES:

- Tier Zero [*object*] Detected Findings cannot be muted. If your selection includes these the mute option will be unavailable.
- Because Findings are muted at the time they are dismissed and therefore no longer display in the Findings list, they can only be [unmuted](#) from the All Indicators page.

### To mute Findings for individual objects:

1. From the Findings Investigation What Happened?/What Is Wrong? section, select the object(s) you want to mute.
2. Click **Mute Object**.

**i** | **NOTE:** You can **unmute** muted objects from the [Findings Investigation](#) What Happened?/What Is Wrong? page or from the [Indicator Details](#) view.

# Dismissing Findings

When you dismiss a Finding, the Finding will no longer display in the active [Findings list](#).

- For a Hygiene, Detected TTP, or Detected Anomaly Indicator, the Finding will continue to be monitored and any new Finding for the indicator will be raised unless it is [muted](#).
- For a Tier Zero indicator, the Finding will not be raised again unless the object is re-added as a Tier Zero or Privileged object.

## NOTES:

- Only certified [Tier Zero](#) and [Privileged](#) objects can be dismissed. If a Tier Zero/Privileged object is not certified, the Dismiss option will be disabled. However, you can dismiss a Tier Zero/Privileged Finding as part of the certification process.
- When you dismiss a Finding, the Finding Status is changed from Active to Inactive and can be viewed when the Findings list is filtered by Status = Inactive.


### **To dismiss a Finding after investigation:**

From the [Investigate Finding](#) page, click **Dismiss Finding**.

You will be prompted to confirm the dismissal. For a Hygiene, Detected TTP, or Detected Anomaly Indicator, the confirmation dialog also includes a check box that allows you to [mute the Finding](#) at the same time.


### **To dismiss one or more Findings from the Findings list:**

1. Select the Finding(s) you want to dismiss.
2. Click the **Dismiss** button.

 **NOTE:** If your selection contains only Hygiene, Detected TTP, and/or Detected Anomaly Indicators, you will also have the option to [mute](#) the Finding(s). If the selection includes Tier Zero Findings, the option to mute will be unavailable. Any [uncertified](#) Tier Zero objects in the selection will not be dismissed.


# Viewing Finding History

You can view the history of all actions associated with a Finding from the [Findings list](#) or the [Findings Investigation](#) page.

 **NOTE:** Once a Finding is dismissed, history will no longer be recorded, although it still can be viewed. If a new Finding is raised for the same indicator, a new history for the Finding will be created.

### **To view a Finding's history from the Findings list:**

1. Select the Finding whose history you want to view.
2. Click the **View History** button.


 **NOTE:** If more than one Finding in the list is selected, the button will be disabled.

### **To view a Finding's history from the Findings Investigation page:**

Click the **View History** button.

For each action associated with the Finding (listed from newest to oldest), the following information displays:

- **Date**

 **NOTE:** This field displays the signed-in user's local date and time.

- **Action**
- **Source**
- **Actor**

For a **Tier Zero [object]** indicator, the history will include:

- when the object was detected and whether the source was the provider (Identity Defense or BloodHound Enterprise) or Manually added.
- when the Finding was created by Identity Defense.

For a **Hygiene, Detected TTP, or Detected Anomaly Indicator** the history will include:

- when a Hygiene, Detected TTP, or Detected Anomaly object was detected and whether the source was Assessments or Audit.
- when the Finding was created by Identity Defense.
- when any objects within the Finding were muted/unmuted.
- for an unprotected Active Directory Tier Zero object Finding, when the object was protected (if applicable).

# Tier Zero Objects

Tier Zero objects are the most critical assets within an organization's Active Directory. Within the Microsoft enterprise access model, Tier Zero objects in Active Directory include accounts, groups, and other assets that have direct or indirect administrative control of Active Directory and the assets within it.

Currently, Identity Defense supports the following Tier Zero object types:

- Domains
- Computers
- Groups
- Group Policies
- Users
- Foreign Security Principals

The [Tier Zero provider](#) (Identity Defense or BloodHound Enterprise) identifies Tier Zero objects within the organization's Active Directory domains. These objects are then collected by and displayed in Identity Defense.

You can also add Tier Zero objects to Identity Defense [manually](#).

## How Tier Zero Objects are Identified

Following are the criteria that the Identity Defense Tier Zero provider uses to identify Tier Zero objects in Active Directory.

**i** | **NOTE:** For the criteria that BloodHound Enterprise uses, refer to the BloodHound support article [Tier Zero: Members and Modification](#).

- **Domains:** The Domain object is identified as Tier Zero because it is a domain partition in the Active Directory forest which supports replication and administrative functions.
- **Groups:** May be identified as Tier Zero if they are a Default AD Security Group which has access to Tier Zero objects in the domain, or if they are a member of another Tier Zero group (either directly or indirectly).

The default AD Security Groups considered Tier Zero are:

- √ Account Operators
- √ Administrators
- √ Backup Operators
- √ Cert Publishers
- √ Cloneable Domain Controllers
- √ Cryptographic Operators
- √ DnsUpdateProxy
- √ DnsAdmins
- √ Domain Admins
- √ Domain Controllers
- √ Enterprise Key Admin
- √ Enterprise Admins
- √ Enterprise Read-Only Domain Controllers
- √ Group Policy Creators Owners
- √ Hyper-V Administrators
- √ Incoming Forest Trust Builders
- √ Key Admins
- √ Network Configuration Operators
- √ Performance Log Users
- √ Print Operators
- √ Read-Only Domain Controllers
- √ Remote Management Users
- √ Schema Admins
- √ Server Operators
- √ Storage Replica Administrators

- **Users:** May be identified as Tier Zero if they are a member of a Tier Zero group (either directly or indirectly).
- **Computers:** May be identified as Tier Zero if they are a Domain Controller, Read-Only Domain Controller, or are a member of a Tier Zero group (either directly or indirectly).
- **Group Policies:** May be identified as Tier Zero if they are linked to
  - the Domain
  - an AD site or an organizational unit (OU) that contains a Domain Controller, a Read-Only Domain Controller, or other Tier Zero user or computer.
- **Foreign Security Principals:** May be identified as a Tier Zero foreign security principal because it is a member of a Tier Zero group.

It is recommended that some additional objects, which may not be identified by the Tier Zero provider, be [added manually](#).

## Tier Zero Objects List

The Tier Zero Objects list displays all of the Tier Zero objects that have been collected by the Tier Zero provider (Identity Defense or BloodHound Enterprise) as well as any that have been [manually-added](#) by users.

**i** **NOTE: If BloodHound Enterprise is configured and you see the message No New Tier Zero Objects,** check the BloodHound Enterprise Configuration Status. Review the configuration connection message details to determine whether the connection to SpecterOps has been successful. Review the Last Configuration Received, Next Configuration Synchronization, and the status of the configuration.

### **To access the Tier Zero Objects list:**

From the left navigation menu, choose **Defend | Tier Zero Objects**. The following information is listed for each Tier Zero object:

- Display Name
- Principal Name
- Distinguished Name
- Object Type
- Date Added

**i** | **NOTE:** This field displays the signed-in user's local date and time.

- Added By (Identity Defense, BloodHound Enterprise or [User](#))
- [Certification Status](#)
- [Protection Status](#)

**i** | **NOTE:** If you click the **Filter** button, you can filter displayed results by any one of these criteria.

From the Tier Zero Objects list, you can:

- [view an object's details](#)
- [export the list to a .csv file](#)
- [add objects manually](#)
- [remove objects that have been added manually](#)
- [certify objects](#)
- [enable protection](#)

## Viewing Tier Zero Object Details

### **To view a Tier Zero object's details:**

From the [Dashboard](#) Uncertified Tier Zero Objects tile or the [Tier Zero Objects list](#), click the object's Principal Name.

The following information displays for the selected Tier Zero object:

- **Object Properties:**
  - **Certification Status**
  - **Added By** (Identity Defense, BloodHound Enterprise or User)
  - **Distinguished Name**
  - **Object ID**
  - **Object Type**
  - **Principal Name**

- Domain FQDN
- Domain SID
- Date Added

**i** | **NOTE:** This field displays the signed-in user's local date and time.

- Information Last Updated

- **for a User object**, local admin privileges
- **for a Group object**, any other groups it is a member of
- **for a Group Policy object**, objects affected by the Group Policy

**i** | **NOTE:** BloodHound Enterprise classifies domains affected by a Group Policy as OUs.

- objects that the selected object can control
- objects that have control over the selected objects.

**i** | **NOTE:** BloodHound Enterprise returns a *maximum* of 1,000 related objects for each Tier Zero category.

### Why Tier Zero?

This section provides the reason why the object is considered Tier Zero. If the object was added by the provider (Identity Defense or Bloodhound Enterprise), the reason is returned by the provider. If the object was manually added by a user, the reason is "Manually added as Tier Zero by <user\_principal\_that\_added\_object>".

## Adding Tier Zero Objects Manually

You can add Tier Zero objects manually for AD objects that were not identified as Tier Zero by the Tier Zero provider but are considered critical assets in your organization.

In addition to the Tier Zero objects [identified by the Tier Zero provider](#), it is recommended that the following objects be added manually:

- Microsoft Entra Connect servers, including:
  - servers with PTA agents if Pass-Through Authentication (PTA) is enabled
  - the "AZUREADSSO" computer account
- Active Directory Federation servers
- Distributed COM Users
- Privileged access management (PAM) systems
- Certificate Authorities and Subordinates
- Computers that host Quest Recovery Manager and other Active Directory management software and their backups
- Computers that host GPOAdmin, Active Administrator, and other group policy management software

- Microsoft Exchange Servers (if split permissions are not configured)
- Microsoft System Center Configuration Manager (SCCM) servers or equivalent
- Microsoft Exchange Groups (if default permissions are still configured)
- Microsoft SQL server or equivalent if hosting a database from a Tier Zero system
- Active Directory Management and auditing software, such as Change Auditor or Active Roles Server

**To add a Tier Zero object manually:**

1. Use one of the following options:
  - From the [Dashboard](#), select **Add New Tier Zero Object**.
  - From the [Tier Zero Objects list](#), select **Add Tier Zero**.
2. For each Tier Zero object you want to add:
  - a. Enter the object's Principal Name, or type at least two characters then select the object from the drop-down. (Note that a message will display if the object is already Tier Zero.)  
The object will be added to the Principal Name list.
  - b. In the Principal Name list, select object(s) you want to add.
3. Click **Save**.

## Removing Manually-Added Tier Zero Objects

You can remove Tier Zero objects that have been manually added by a user from the [Tier Zero Objects list](#).

**i** **NOTE:** Tier Zero objects added by the Tier Zero provider (Identity Defense or BloodHound Enterprise) cannot be removed via Security Management Platform.

Note that, if you remove a manually-added object from the Tier Zero list, it will no longer be monitored and if re-added, it will revert to being Not Certified, regardless of its status when it was removed.

**To remove a manually-added Tier Zero object:**

1. From the [Tier Zero Objects list](#), the object(s) you want to remove.
2. Click **Remove Tier Zero**.

**i** **NOTE:** If any Tier Zero objects added by the Tier Zero provider are in the selection, the Remove Tier Zero option will be disabled.

You will be prompted to confirm the action.

## Certifying Tier Zero Objects

Certification is a means by which you can verify that any object identified by the Tier Zero provider or added manually by a user as Tier Zero qualifies as Tier Zero. Once certified, it will be used to establish a baseline for generating Findings for Detected and Hygiene Indicators.

By default, when an object is added as Tier Zero (which includes objects in the initial list collected by the Tier Zero provider), its status is Not Certified. This encourages you, as a Identity Defense administrator, to review each object for Tier Zero account security risks.

**i** | **EXCEPTION:** Because they pose the highest security risk to your Active Directory environment, Tier Zero **Domain** objects identified by the Tier Zero provider (Identity Defense or BloodHound Enterprise) are certified automatically and cannot be uncertified.

You can certify one or multiple objects from the [Tier Zero Objects list](#), or individually from the [Investigate Finding](#) page or within an Uncertified Tier Zero Object's Details view on the [Dashboard](#).

It is strongly recommended that any manually-added Tier Zero objects that, after review, have not been certified as Tier Zero be [removed](#).

You can also uncertify any Tier Zero object, except a Domain object, that has been previously certified from the Tier Zero Objects list.

**To certify Tier Zero objects from the Tier Zero Objects list:**

1. Select the object(s) you want to certify.
2. Click **Certify Tier Zero**.

**To certify a Tier Zero object from the Findings Investigation page:**

Click **Certify Tier Zero Object**.

You will be prompted to confirm the certification. The confirmation dialog also includes a check box that allows you to [dismiss the Finding](#) at the same time.

**i** | **NOTE:** Once a Tier Zero object has been certified, it will no longer display in the Uncertified Tier Zero Objects tile on the [Dashboard](#).

**To uncertify a Tier Zero Object from the Tier Zero Objects list:**

1. Select the object you want to uncertify.

**i** | **NOTE:** Only one certified object can be uncertified at a time. If more than one object is selected, or if a Domain object is selected, the option to uncertify will not be available.

2. Click **Uncertify Tier Zero**.

## Protecting Tier Zero Objects

If Change Auditor version 7.4 or Hybrid Audit is integrated with Security Management Platform, you can protect Tier Zero objects from unauthorized or accidental modifications or deletions from the Identity Defense interface.

You can protect Tier Zero objects from the Findings Investigation page if one or more unprotected Tier Zero objects have been detected as a Detected TTP or Hygiene Indicator, or from the Tier Zero list.

## **i** NOTES:

- Currently, you cannot unprotect objects in Identity Defense when integrated with Change Auditor. However, Change Auditor can be used to unprotect objects. Once an object is unprotected, a new Finding will be raised in Identity Defense.
- When Identity Defense is integrated with Hybrid Audit, Tier Zero protection templates can be managed in Hybrid Audit | Protection.
- When an object within a Finding is protected, it no longer displays in the Findings investigation page. However, object protection status details can be viewed in Change Auditor.

### **Tier Zero Protection Status**

The Tier Zero protection status is displayed in the **Protection Status** column of the [Tier Zero Objects List](#). The status may be:

- Not Protected
- Applying Protection
- Protected
- Pending Evaluation

## **i** NOTE:

- When protection is enabled for a Tier Zero object, it is removed from investigation findings and immediately marked as Applying Protection until it is confirmed that protection is applied.
- A Pending Evaluation status indicates that either Hybrid Audit/Change Auditor has not completed processing the protection request or that Hybrid Audit/Change Auditor 7.4 or later is not integrated with Security Management Platform.

### **To protect Tier Zero objects from the Tier Zero list:**

1. Select the unprotected object(s) you want to protect.
2. Click the **Enable Protection** button.

### **To protect Tier Zero objects from the Findings Investigation page (if applicable):**

1. On the Findings Investigation page What Happened? section, select the Tier Zero object(s) that you want to protect.
2. Click the **Enable Protection** button.

# Exporting the Tier Zero Objects List

You can export the complete, unfiltered Tier Zero objects list to a .csv file, which can be shared with stakeholders and used for security assessment engagements.

### **To export the Tier Zero objects list:**

From the Tier Zero Objects page, click **Export to CSV**.

The file is exported to your Downloads folder with the file name `export_{timestamp}_{a GUID}.csv` and includes the following information:

- Display Name
- Principal Name
- Distinguished Name
- Object Type
- Date Added
- Added By
- Certification Status
- Protection Status

# Prevention (Shields Up Protection)

In times of heightened cyber threat—whether due to intelligence suggesting an imminent attack or signs of an ongoing breach—organizations may need to temporarily enforce stricter controls over their Active Directory environments. The Shields Up feature provides a rapid-response mechanism to lock down critical Active Directory objects, preventing unauthorized or accidental changes during a security incident.

This emergency posture is designed to be short-lived but highly restrictive, offering a pre-configured protection template that can be activated instantly. By doing so, it helps safeguard Tier Zero assets and other vital components of the Active Directory infrastructure until the threat subsides.

While intended for temporary emergency use, Shields Up can also be deployed continuously as a proactive security measure.

Shields Up safeguards critical Tier Zero assets and configurations by preventing unauthorized deletion, modification, or policy changes including the following:

- Prevents deletion and modification of Tier Zero users, computers, groups, and group policies.
- Prevents deletion and modification of foreign security principals and well-known security principals.
- Prevents domain head from linking and unlinking group policies, modification of security, and modification of ms-DS-MachineAccountQuota.
- Prevents linking and unlinking of group policies for Domain Controllers Organizational Unit (OU).
- Prevents creation, deletion, and modification of certification templates.
- Prevents security modifications and changes to the DsHeuristics attribute of Directory Service Objects.
- Prevents modification of the AdminSDHolder container.

**i** | **NOTE:** Protection is limited to a maximum of 200 Tier Zero users, 200 Tier Zero groups, 200 Tier Zero computers, and 200 Tier Zero group policies.

A domain is eligible for Shields Up if:

- It is configured with either BloodHound Enterprise or the Hybrid Agent as a Tier Zero data provider actively collecting from the domain.
- It has Change Auditor version 7.6 or later deployed within the domain.

## **To access Shields Up functionality:**

1. From the left navigation menu, choose **Defend | Prevention**.
2. Select the **Shields Up** tab.

## Using Shields Up

The Shields Up tab provides a centralized view and control panel for managing emergency protection across Active Directory domains. It includes action buttons and a data table with key domain-level details.

From here, you can:

- Enable Shields Up – Activates Shields Up protection for the selected domain. See [Enabling Shields Up](#)
- Disable Shields Up – Deactivates Shields Up protection. See [Disabling Shields Up](#)
- Add Override Access – Allows administrators to specify users, groups, or computers that can bypass Shields Up restrictions. See [Override Access for Protected Objects](#)

The display includes the following details:

Column Name	Description
Domain	Displays the name of the domain. This column is filterable.
Forest	Displays the name of the forest. This column is filterable.
Shields Up Status	Displays the current status of Shields Up for the domain: Enabled, Enabling, Disabled, or Disabling. This column is filterable.
Date Enabled	Displays the date and time when Shields Up was enabled for the domain.
Enabled By	Displays the user principal name of the person who enabled Shields Up. This column is filterable.
Override Accounts	Displays the number of accounts that have been granted override access to bypass Shields Up protections.

## Enabling Shields Up

Shields Up is a security feature that locks down Tier Zero and other critical Active Directory system objects to prevent unauthorized or accidental changes during a potential or active cyber threat.

When Shields Up is activated:

- Tier Zero and critical system objects are protected from modification.
- Any objects newly identified as Tier Zero while Shields Up is active are automatically added to the protection list.
- Objects removed from Tier Zero during this time are no longer protected.

Additionally, enabling Shields Up triggers an alert that is sent to all configured email recipients, ensuring that key stakeholders are informed of the change in security posture.

Once the threat has passed or the emergency posture is no longer required, Shields Up can be safely disabled to restore normal administrative access.

For more information, see:

- [Configuring a Forwarding Destination](#)
- [Disabling Shields Up](#)

### ***To activate Shields Up for a domain***

1. From the left navigation menu, choose **Defend | Prevention**.
2. Select the **Shields Up** tab.

3. Select a domain from the list of Active Directory domains configured in your organization.
4. Review the list of critical system objects that will be protected under Shields Up.
5. Click the **Enable Shields Up** button on the Shields Up tab.
6. Acknowledge that you understand the significance of the action and click **Enable Shields Up**.

After Shields Up is initiated, the domain's status will change to Enabling. Once activation is complete, the status will update to Enabled.

An email alert will be automatically sent to all designated stakeholders to notify them that Shields Up is now active.

## Disabling Shields Up

Disabling Shields Up will remove the temporary restrictions and restore standard permissions for Tier Zero and other protected objects and will trigger an alert to the configured email recipients.

### *To disable Shields Up for a domain*

1. From the left navigation menu, choose **Defend | Prevention**.
2. Select the **Shields Up** tab.
3. Navigate to the Prevention section and open the Shields Up tab.
4. Select the domain where Shields Up is currently enabled.
5. Click **Disable Shields Up**.
6. Acknowledge that you understand the significance of the action and click **Disable Shields Up**.

## Override Access for Protected Objects

You can grant specific Active Directory users, groups, computers, and service accounts permission to access objects protected by Shields Up. This allows for controlled exceptions during a Shields Up activation, ensuring that essential accounts retain access to critical resources.

Removing an object from the Override Access list revokes its ability to access protected Tier Zero and system resources when Shields Up is enabled.

### *To override access:*

1. From the left navigation menu, choose **Defend | Prevention**.
2. Select the **Shields Up** tab.
3. Click the **Add Override Access** button in the action bar or select a protected domain.

4. From the Add Override Access flyout, enter Active Directory users, groups, computers, and service accounts that should be allowed to access protected objects while Shields Up is active. Selecting an object will add it to the grid.
5. Use the **Remove** button to delete entries from the grid.
6. Click **Save** to confirm your selections.

**To remove override access:**

1. From the left navigation menu, choose **Defend | Prevention**.
2. Select the **Shields Up** tab.
3. Select a domain.
4. From the domain details, select the required user, computer, group, or service account and select **Remove**.
5. Select **Remove Override Access** to confirm the action and revoke the override access.

# Privileged Objects

Privileged objects are the most critical assets within Microsoft Entra ID. Within the Microsoft enterprise access model, Privileged objects in Entra ID include permissions that can delegate management of resources, modify credentials, authentication or authorization policies, and access restricted data.

Identity Defense supports the following Privileged types:

- Groups
- Roles
- Service Principals
- Tenants
- Users

The [Privileged Objects provider](#) (Identity Defense or BloodHound Enterprise), identifies Entra ID Privileged objects within the Microsoft 365 tenant(s). These objects are then collected and displayed in Identity Defense.

## Privileged Objects List

The Privileged Objects list displays all of the Privileged objects that have been collected by the [Privileged objects provider](#) (Identity Defense or BloodHound Enterprise) as well as any that have been [manually-added](#) by users.

**i** **NOTE: If BloodHound Enterprise is configured and you see the message No New Privileged Objects**, check the BloodHound Enterprise Configuration Status. Review the configuration connection message details to determine whether the connection to SpecterOps has been successful. Review the Last Configuration Received, Next Configuration Synchronization, and the status of the configuration.

### **To access the Privileged Objects list:**

From the left navigation menu, choose **Defend | Privileged Objects**. The following information displays for each Privileged object:

- Display Name
- Principal Name
- Tenant
- Object Type
- Date Added

**i** **NOTE:** This field displays the signed-in user's local date and time.

- Added By (Identity Defense, BloodHound Enterprise, or User)
- Certification Status

**i** **NOTE:** If you click the **Filter** button, you can filter displayed results by any one of these criteria.

From the Privileged Objects list, you can:



- [view an object's details](#)
- [export the list to a .csv file](#)
- [add objects manually](#)
- [remove objects that have been added manually](#)
- [certify objects](#)

## Viewing Privileged Object Details

### **To view a Privileged object's details:**

From the [Dashboard](#) Uncertified Privileged Objects tile or from the [Privileged Objects list](#), click the object's Display Name.

The following **Object Properties** are identified for the selected Privileged object:

- **Certification Status**
- **Added By** (Identity Defense, BloodHound Enterprise or User)
- **Display Name**
- **Object ID**
- **Object Type**
- **Principal Name, Tenant, and Tenant ID** (for Tenant objects)
- **Service Principal type** (for Service Principal objects)
-  **NOTE:** This field *may* be populated only if On Premises Sych is enabled.
- **Role Template ID** (for Role objects)
- **User Type** (for User objects)
- **Security Identified** (for Group objects)
- **Principal Name**
- **On Premises Name** (for User and Group objects, if On Premises Synch is enabled)
- **On Premises SID** for User and Group objects, if On Premises Synch is enabled)
- **On Premises Domain** (for User and Group objects, if On Premises Synch is enabled)
- **Date Added**
-  **NOTE:** This field displays the signed-in user's local date and time.
- **Information Last Updated**

Below the object properties are one or more object-specific sections:

**For Tenants:** Objects with control of <tenant\_name>

**For Roles:** Active Assignments

**For Service Principals and Users:**

- Objects <object\_name> can control
- Objects with control of <object\_name>
- Roles

**For groups:**

- Member of
- Object with control of <group name>
- Roles

### Why Privileged?

This section provides the reason why the object is considered Privileged. If the object was added by the provider (Identity Defense or Bloodhound Enterprise), the reason is returned by the provider. If the object was manually added by a user, the reason is "Manually added as Tier Zero" or "manually added as Privileged" by <user\_principal\_that\_added\_object>".

## Adding Privileged Objects Manually

You can add Privileged objects manually for Entra ID objects that were not identified as Privileged by the provider (Identity Defense or BloodHound Enterprise) but are considered critical assets in your organization.

1. Use one of the following options:
  - From the [Dashboard](#), select **Add New Privileged Object**.
  - From the [Privileged Objects list](#), select **Add Privileged**.
2. For each Privileged object you want to add:
  - a. Enter the object's Principal Name, or type at least two characters then select the object from the drop-down. (Note that a message will display if the object is already Privileged.)  
The object will be added to the Principal Name list.
  - b. In the Principal Name list, select object(s) you want to add.
3. Click **Save**.

## Removing a Manually-added Privileged Object

You can remove Privileged objects that have been manually added by a user from the [Privileged Objects list](#).

**i** | **NOTE:** Privileged objects added by the provider (Identity Defense or BloodHound Enterprise) cannot be removed via Security Management Platform.

Note that, if you remove a manually-added object from the Privileged list, it will no longer be monitored and if re-added, it will revert to being Not Certified, regardless of its status when it was removed.

**To remove a manually-added Privileged object:**

1. From the [Privileged Objects list](#), the object(s) you want to remove.
2. Click **Remove Privileged**.

**i** | **NOTE:** If any Privileged objects added by the provider are in the selection, the Remove Privileged option will be disabled.

You will be prompted to confirm the action.

## Certifying Privileged Objects

Certification is a means by which you can verify that any object identified by the provider (Identity Defense or BloodHound Enterprise) or added manually by a user as Privileged qualifies as Privileged. Once certified, it will be used to establish a baseline for generating Findings for Detected and Hygiene Indicators.

By default, any object added as Privileged (which includes objects in the initial list collected by the provider), its status is Not Certified. This encourages you, as a Identity Defense administrator, to review each object for Privileged account security risks.

**i** | **EXCEPTION:** Because they pose the highest security risk to your Entra ID environment, Privileged **Tenant** objects identified by the provider are certified automatically.

You can certify one or multiple objects from the [Privileged Objects list](#), or individually from the [Investigate Finding](#) page or within an Uncertified Privileged Object's Details view on the [Dashboard](#).

It is strongly recommended that any manually-added Privileged objects that, after review, have not been certified as Privileged be [removed](#).

You can also uncertify any Privileged object, except a Tenant object, that has been previously certified.

**To certify Privileged objects from the Privileged Objects list:**

1. From the Privileged Objects list, select the object(s) you want to certify.
2. Click **Certify Privileged**.

**To certify a Privileged object from the Findings Investigation page:**

Click **Certify Privileged Object**.

You will be prompted to confirm the certification. The confirmation dialog also includes a check box that allows you to [dismiss the Finding](#) at the same time.

**i** | **NOTE:** Once a Privileged object has been certified, it will no longer display in the Uncertified Privileged Objects tile on the [Dashboard](#).

**To uncertify a Privileged Object from the Privileged Objects list:**

1. From the Privileged list, select the object you want to uncertify.

**NOTE:** Only one certified object can be uncertified at a time. If more than one object is selected, or if a Tenant object is selected, the option to uncertify will not be available.

2. Click **Uncertify Privileged**.

**i** | **NOTE:** Once a Privileged object has been uncertified, it will display in the Uncertified Privileged Objects tile on the [Dashboard](#).

## Exporting the Privileged Objects List

You can export the complete, unfiltered Privileged objects list to a .csv file, which can be shared with stakeholders and used for security assessment engagements.

### **To export the Privileged objects list:**

From the Privileged Objects page, click **Export to CSV**.

The file is exported to your Downloads folder with the file name `export_{timestamp}_{a GUID}.csv` and includes the following information:

- Display Name
- Principal Name
- Tenant
- Object Type
- Date Added
- Added By
- Certification Status

# Managing Workload Identities

The Workload Identities page provides visibility into service principals and their associated security posture within your Entra ID and Active Directory environment. This feature helps administrators identify risky permissions, assess sign-in status, and monitor compliance with security standards.

## Best Practices

- Regularly review identities with Critical or High risk.
- Ensure all Entra ID identities have at least one owner.
- Rotate secrets and remove expired credentials promptly.
- Limit privileged access to essential identities only.

For more details, see:

- [Entra ID Workload Identities](#)
- [Active Directory Workload Identities](#)

## Entra ID Workload Identities

### To access *Entra ID Workload Identities*:

- From the left navigation menu, choose **Defend | Workload Identities | Entra ID**. The following information displays all service principals with key security attributes:

Column	Description
Service Principal Name	The name of the service principal registered in Entra ID.
Application Tenant	The tenant ID or tenant name of the application for the workload identity and whether the application is local or external.
Category	Compliance category (such as FISMA, GDPR, HIPAA).
Owners	Number of assigned owners for the identity.
Risky Permissions	Count of permissions flagged as risky.
Sign-In Status	Displays if the identity has successfully signed-in in the last 30 days.
Secret Status	Indicates the state of credentials (for example, None, Current, Expired).
Assessed Risk	Risk level based on configuration and permissions (Critical, High, Medium, Low).
Last Reloaded	The last time the information was retrieved and from Entra ID and assessed.
Tenant	Tenant where the Service Principal resides.
Account Status	Indicator whether the workload identity is enabled or disabled.
Service Principal Type	Indicator showing the type of workload Identity (Application, Managed Identity, AI Agent).

From this page you can:

- Assign compliance categories to selected identities. [Setting Workload Identity Category](#).
- Refresh identity data from Entra ID. See [Reloading Workload Identities](#).
- View workload identities details. See [Viewing Workload Identity Details](#).
- Apply filters to narrow down results.
- Export the table contents to CSV.
- Customize visible columns through the Gear icon.

# Active Directory Workload Identities

## To access Active Directory Workload Identities:

- From the left navigation menu, choose **Defend | Workload Identities | Active Directory**. The following information displays all service principals with key security attributes:

Column	Description
Principal Name	The name of the service principal registered in Active Directory.
Object Type	Displays the object type (User, Computer, or Service Account).
Category	Compliance category (such as FISMA, GDPR, HIPAA).
Managed By	Principal name of the manager of the workload identity.
Confidence	Indicates the level of certainty the object is a workload identity (High, Medium, Low).
Classification	Classification set by the user to confirm that the object is a workload identity (Suspected, Confirmed, Rejected).
Classified By	Principal name of the logged in user that set the classification.
Findings	The total number of Findings for the object (Color icon: 0 - green, 1-5 - yellow, more than 5 - red).
Added By	Indicates whether the workload identity was added automatically or manually (Identity Defense, User).
Last Reloaded	The last time the data for the service principal was updated.
Domain	Domain where the Service Principal resides.
Account Status	Indicator whether the workload identity is enabled or disabled.

From this page you can:

- Add and remove Active Directory user, computer, and service account objects as workload identities. See [Adding and Removing Active Directory Workload Identity](#).
- Assign compliance categories to selected identities. See [Setting Workload Identity Category](#).
- Set or update the classification of selected workload identities. See [Classifying Active Directory Workload Identities](#).

- Define additional rules used to identify potential workload identities in Active Directory. See [Setting Identification Criteria for Active Directory Workload Identities](#).
- Refresh identity data from Active Directory. See [Reloading Workload Identities](#).
- View workload identities details. See [Viewing Workload Identity Details](#).
- Apply filters to narrow down results.
- Export the table contents to CSV.
- Customize visible columns through the Gear icon.

## Adding and Removing Active Directory Workload Identity

In addition to workload identities that are automatically discovered, you can manually add Active Directory user, computer, and service account objects as workload identities.

### ***To add an Active Directory Identity Workload:***

1. Navigate to **Security | Workload Identities | Active Directory**.
2. Select **Add Identity** to add Active Directory objects as workload identities.
3. Enter an object principal to add.
4. Save and confirm your changes.

### ***To remove an Active Directory Identity Workload:***

1. Navigate to **Security | Workload Identities | Active Directory**.
2. Select the box beside the principle and choose **More | Remove Identity**.
3. Select **Remove Workload Identity**.

## Classifying Active Directory Workload Identities

The Classify option lets administrators set or update the classification of selected workload identities.

### ***To classify an Active Directory workload Identity:***

1. Navigate to **Security | Workload Identities | Active Directory**.
2. Select the checkbox beside the principal and select **Classify**.
3. Confirm or reject whether the selected Active Directory objects are workload identities. Classifying objects as **Suspected** removes it from the criteria used to detect new workload identities. This status indicates that more investigation is needed before confirming the object as a workload identity.
4. Save and confirm your changes.

# Setting Identification Criteria for Active Directory Workload Identities

Setting Identification criteria allows you to define additional rules used to identify potential workload identities in Active Directory.

## **i** NOTE:

- Criteria are set per domain.
- The button is enabled only when a single domain is selected in the domain drop-down.

### **To set identification criteria:**

1. Navigate to **Defend | Workload Identities | Active Directory**.
2. Select **Set Identification Criteria**.
3. Under **Workload Identity Names**, enter keywords that should be considered when evaluating user object names as potential workload identities, and click **Add**.
4. Under **Workload Identity OUs**, enter keywords that should be considered when evaluating Organizational Unit (OU) names that may contain workload identity objects, and click **Add**.
5. Under **Workload Identity Attributes**, select or enter the attributes and their values to be considered when evaluating user objects to identify workload identities, and click **Add**.
6. Under **Consider Password Expiration**, choose how the “password never expires” setting should be treated when identifying potential workload identities.
7. Save your selections.

## Viewing Workload Identity Details

The Workload Identity Details panel provides in-depth information about a selected service principal, including its properties, risk classification, ownership, and permissions. This helps administrators assess potential security risks and take corrective actions. It also provides an AI generated risk analysis assessment.

### **Best Practices**

- Review Critical or High risk identities immediately.
- Determine if inactive identities should be disabled or removed.
- Investigate permissions that are high risk or flagged for review.
- Ensure ownership is assigned to avoid orphaned identities.
- Rotate secrets regularly and remove expired credentials.

### **To review Entra ID workload identity details:**

1. Navigate to **Defend | Workload Identities | Entra ID**.
2. Click on a service principal in the list to view the following information:
  - Key identifiers and metadata including Object ID, Category, Application Name, Application ID, Application Tenant ID, AI Agent Source, Azure Resource ID, and Malicious Indicator.

- Risk Analysis: The risk analysis evaluates configuration and behavior to determine if the identity poses a security risk.
- Sign-ins: Shows sign-in activity.
- Owners: Lists assigned owners.
- Certificates and Secrets: Displays credential status.
- Permissions: Lists granted permissions.

**To review Active Directory workload identity details:**

1. Navigate to **Defend | Workload Identities | Active Directory**.
2. Click on a service principal in the list to view the following information:
  - Key identifiers and metadata including Display Name, Object ID, Object SID, Distinguished Name, Category (all assigned categories), Domain FQDN, Added By (either "Identity Defense" or principal name of the user that added the workload identity manually), Date Added, Information last updated date and time.
  - Principal Name: Service Principal Name and Application.
  - Applied Group Policies: The name of the applied GPO and the Organizational Unit where the GPO is linked.
  - Findings: Describes the issue that was detected and a link to Investigate for more details.

# Setting Workload Identity Category

Categories help administrators classify service principals in Entra ID and Active Directory based on compliance, security tiers, or functional roles. This classification improves filtering, reporting, and risk management.

**Best Practices**

- Assign categories consistently across similar identities.
- Use Tier levels to indicate privilege and risk.
- Regularly review categories for accuracy.

**To access category setting:**

1. Navigate to **Defend | Workload Identities**.
2. From the **Entra ID** or **Active Directory** tab, select one or more service principals from the list.
3. Click **Set Category** in the toolbar.
4. From the Set Category window, assign up to five labels from a predefined list.
5. Click **Save** to apply the changes.

**Available Categories**

Category	Description
Agentic AI	AI-related workloads or agents.

FISMA	Federal Information Security Management Act compliance.
GDPR	General Data Protection Regulation compliance.
GLBA	Gramm-Leach-Bliley Act compliance.
HIPAA	Health Insurance Portability and Accountability Act compliance.
PCI	Payment Card Industry standards.
SAS	Statistical Analysis System or similar workloads.
Security Scanning	Identities used for vulnerability or compliance scanning.
SOX	Sarbanes-Oxley Act compliance.
Tier 0–Tier 4	Security tiers indicating privilege level and criticality.

## Reloading Workload Identities

The Reload Identity feature allows administrators to refresh the details of selected service principals from Entra ID without waiting for a full data collection cycle. This ensures that recent changes in are immediately reflected in Identity Defense.

### Best Practices

- Use Reload Identity after making changes to ensure data accuracy.
- Avoid frequent reloads for large selections to minimize API load.
- Monitor Last Reloaded timestamps for auditing and troubleshooting.
- A maximum of 10 workload identities can be selected at once.

### *To reload workload identity properties:*

1. Navigate to **Defend | Workload Identities**.
2. Select up to 10 service principals from the list.
3. Click **Reload Identity** in the toolbar.
4. Click **Reload Now** to collect and view latest property values for the selected workload identities.

# Assessments

Assessments are a set of Discoveries that are evaluated against collected data to identify vulnerabilities in your organization's Active Directory domains and Entra ID tenants. They run automatically once added, and then run periodically, depending on how often data is collected. This allows you to identify which objects within scope contain vulnerabilities that require further investigation and remediation.

**To access Assessments functionality:**

From the left navigation menu, choose **Defend | Assessments**.

## First Assessment Notification Email

If [email is configured](#) for Identity Defense, after the first Assessment is completed for the organization, a notification email is sent which includes the total number of the following:

- Findings without vulnerable objects
- Findings with vulnerable objects
- Findings with inconclusive results
- Findings that returned an error

**i** **NOTE:** This notification applies only for the first Assessment that is completed for an organization. If email is configured after the first Assessment has run, a notification will not be sent. Subsequent emails will be sent advising that the Assessment has been completed and vulnerable objects have grown in scope.

## Built-in Assessments

Identity defense includes built-in Security Assessments for Active Directory and/or Entra ID. They contain all pre-defined Discoveries provided by Quest and are run on all domains and/or tenants configured in Security Management Platform for your organization.

**i** | **NOTE:** If no domains or tenants are [configured for data collection](#), the status message **Configuration Required** will display in the [All Assessments list](#).

Pre-defined Discoveries are added automatically to Assessments as they are released by Quest.

**i** | **NOTE:** Built-in Assessments cannot be edited or deleted.

# Using Identity Defense Intelligence with Assessments

Identity Defense Intelligence helps you ask focused questions tailored to your environment, providing valuable insights into the security posture of your organization's Active Directory and Entra ID systems. It highlights critical vulnerabilities and issues identified during assessments and offers practical recommendations for remediation. You can choose to view a high-level summary across all your organizations or dive into detailed findings for specific domains or tenants.

**i** | **NOTE:**

- Before you can access the Identity Defense Intelligence assistance, you need to read and accept the AI Terms of Use.
- To refresh the Identity Defense Intelligence content in the flyout, click the AI Icon next to the Active Directory domain name or Entra ID tenant name.

To access Identity Defense Intelligence for Assessments:

1. From the left navigation menu, choose **Defend | Assessments**.
2. Select the Identity Defense Intelligence button or the icon in the Results column.
3. Select one of the following to access more information:
  - Type your question.
  - Click **Summary** to view an overview of all Active Directory and Entra ID assessments.
  - Click the Identity Defense Intelligence icon next to the Active Directory domain or Entra ID tenant to view only the associated Assessment summary information.
4. Review the provided information and delve deeper into the issue if needed.

The summary information includes:

- The analyzed workload, including the number of issues found and the total objects collected for the Assessment.
- Security Posture Summary.
- Top vulnerabilities identified.
- Suggested follow-up questions to guide further investigation.

# All Assessments List

The All Assessments tab displays a list of all Assessments (both built-in and user-created) for the organization along with the following information for each:

- **Assessment** name (with a link to [Assessment Details](#))
- Active Directory domain or Entra ID tenant containing the assessed objects (with the option to [Link to Results](#))
- **Identity Defense Intelligence**: Access Identity Defense Intelligence by clicking the icon next to the Active Directory domain or Entra ID tenant in the Link to Results column. See [Using Identity Defense Intelligence with Assessments](#).
- **Assessment Summary**: The Assessment Summary is an AI-generated report that provides insights and a high-level overview of assessment results across your organization. See [Viewing Assessment Summary Information](#).
- **Workload** (Active Directory or Entra ID)
- **Created By** either:
  - **System** (for a [built-in Assessment](#) provided by Quest)  
OR
  - **User** (for a [user-created Assessment](#))
- **Status** of the Assessment:

## Configuration Required



**NOTE:** This status is used to indicate the absence of an Active Directory domain or Entra ID tenant in Security Management Platform for the organization. This may be because:



- A domain or tenant has not yet been added to Security Management Platform, which will prevent the built-in Assessment from running.
- The domain or tenant selected for the Assessment has since been removed from Security Management Platform.
- When the Assessment was created, all available domains or tenants were excluded.



**Agent Required** (See [Configuring Additional Components -Hybrid Agent](#))



**No Data Collected**



**No Vulnerabilities Found**



**n Vulnerabilities Found**

- Date and time when data was **Last Collected**



**NOTE:** This field displays the signed-in user's local date and time.

# Creating an Assessment

In addition to using the built-in Assessment provided by Quest, you can create your own Assessments based on available [Discoveries](#).

## To create an Assessment:

1. From the All Assessments tab click **Create**.
2. Select the **Workload** (Active Directory or Entra ID)
3. Enter an **Assessment Name** and **Description**.
4. If you want to **Automatically add Discoveries as they are released by Quest**, check this box.

**i** | **NOTE:** If you check this box and all pre-defined Discoveries that are provided by Quest will be added to the Assessment as they become available.

5. Click **Select Discoveries** to display a list of available Discoveries for the workload.
6. Select each Discovery you want to add to the Assessment, then click **Select**.
7. For **Domains** or **Tenants** (depending on the workload you selected), select the Active Directory domains or Entra ID tenants that you want to **Run this Assessment for**. Use the information in the following table for guidance.

Option	Steps to Complete
Only selected domains OR Only selected tenants	<ul style="list-style-type: none"> <li>• Select <b>Only selected domains</b> or <b>Only selected tenants</b> from the drop-down.</li> <li>• Click <b>Select Domains</b> or <b>Select Tenants</b> and select each domain or tenant you want to add to the Assessment, then click <b>Select</b>.</li> </ul> <p>The selected domain(s) or tenant(s) will display in the list.</p>
All except selected domains OR All selected tenants	<ul style="list-style-type: none"> <li>• Select <b>All except selected domains</b> or <b>All except selected tenants</b> from the drop-down.</li> <li>• Click <b>Exclude Domains</b> or <b>Exclude Tenants</b></li> <li>• Select the domain(s) or tenant(s) you want to exclude from the Assessment.</li> <li>• Click <b>Exclude</b>.</li> </ul> <p>Excluded domains or tenants will display in the list. However, when you view the Assessment, all domains or tenants will display and those that are excluded are identified in the Status column.</p>
All domains OR All tenants	<p>Select <b>All domains</b> or <b>All tenants</b>.</p> <p>All domains or tenants configured for your organization will display in the list.</p>

8. Click **Save**.

# Viewing, Editing, and Deleting an Assessment

From the [All Assessments list](#), you view Assessment details and summary information. You can also edit or delete a user-created Assessment.

**i** | **NOTE:** You cannot edit or delete a built-in Assessment, so the Edit and Delete options will be disabled.

## **To view an Assessment:**

- Click the Assessments link.

## **To edit a user-created Assessment:**

1. Either
  - In the [All Assessments list](#), select the Assessment that you want to edit.OR
  - Open the Assessment that you want to edit.
2. Click **Edit**.
3. Update the Assessment as needed.
4. Click **Save**.

## **To delete a user-created Assessment:**

**i** | **NOTE:** Currently, you can only delete one Assessment at a time

1. Either
  - In the [All Assessments list](#), select the Assessment that you want to delete.OR
  - Open the Assessment that you want to delete.
2. Click **Delete**. You will be prompted to confirm the deletion.

# Viewing Assessment Summary Information

The Assessment Summary is an AI-generated report that analyzes your organization's assessment data to identify patterns and provide a clear, high-level overview of results. The summary reflects the assessments you've selected and includes all related domains and tenants.

The report includes the following sections:

- Summary Overview
- Key Findings
- Assessment Workload Details – including discovered objects and vulnerabilities
- Affected Workloads
- Violations by Vulnerability Type
- Violations by Workload Type
- Collection History
- Assessment History

**i** | **NOTE:** The Summary Report is powered by AI and may display differently each time it is generated.

**To view Assessment Summary information:**

1. From the left navigation menu, choose **Defend | Assessments**.
2. In the [All Assessments list](#), do one of the following:
  - Select the checkbox next to **Active Directory Security Assessment** and/or **Entra ID Security Assessment**, then click **Assessment Summary**.
  - OR
  - Select the desired domain or tenant, then click **Assessment Summary**.
3. Click the **Technical Summary** button to generate the report.
4. You can ask questions about the results or request changes to the summary format. For example, “Can you tell me more about the AD vulnerabilities?” Type your question or instruction in the provided text box and click **Send**.
5. Use the **Print** or **Copy** options to save or share the report.

## Assessing Vulnerability Prevalence

Identity Defense helps you understand how common each vulnerability in your environment is among other organizations. This comparison provides valuable context so you can better prioritize remediation efforts. For every vulnerability detected in your organization, Identity Defense reports how frequently that same vulnerability appears in other organizations.

Comparisons are based on organization size (for example, small, medium, and large), allowing you to assess your risk relative to peers with similar environments and operational scale. Your organization is assigned to a size category based on:

- Fewer than 10,000 users (Small)
- 10,000 to 200,000 users (Medium)
- Over 200,000 users (Large)

When vulnerability prevalence is reported, the data is focused on organizations of the same size as yours to ensure you are receiving peer-relevant insight. For each vulnerability, you will see the percentage or number of peer organizations that also have this vulnerability. See [Assessment Results](#) for details.

### Why This Matters

Not all vulnerabilities carry the same urgency. A vulnerability that is rare among organizations your size may indicate a configuration gap or emerging risk that deserves immediate attention. Conversely, a widely prevalent vulnerability may suggest an industry-wide issue that can be addressed through planned remediation.

By comparing your environment with peers, Identity Defense helps you:

- Prioritize remediation based on real-world prevalence
- Identify vulnerabilities that are unusually concentrated in your environment
- Communicate risk more effectively to stakeholders using comparative data

## Assessment Results

You can access the results of an Assessment from the [All Assessments list](#).

**i** **NOTE:** You can only view Assessment results for one Active Directory domain or Entra ID tenant at a time. If the Assessment was run on more than one, you can switch to a different domain or tenant from the drop-down in the upper right corner of the Results page for the Assessment.

### To access results for a selected Assessment:

- Click the corresponding Active Directory domain name or Entra ID tenant name in the **Link to Results** column.

The Results page for the Assessment provides the following information:




#### Summary of Assessment Vulnerabilities

From here you can access a summary of the last run of the selected Assessment, including:

- the date and time the vulnerabilities within the Assessment were **Assessed on**
- the date and time the data used to assess the vulnerabilities was **Collected on**.

**i** **NOTE:** These fields display the signed-in user's local date and time.

Of the total number of **Evaluated Vulnerabilities**, a graph depicts color-coded results, as described below.

	<b>With Vulnerable Objects (n)</b>
	<b>Without Vulnerable Objects (n)</b>
	<b>With Inconclusive Results (n)</b>




#### Summary of Assessment Prevalence

When vulnerability prevalence is reported, the data is focused on organizations of the same size as yours to ensure you are receiving peer-relevant insight. For each vulnerability, you will see the percentage or number of peer organizations that also have this vulnerability.

You can assess vulnerability prevalence by organization size to provide meaningful benchmarks, allowing you to see not just what vulnerabilities you have, but how common they are among organizations like yours—helping you focus your security efforts where they matter most.

#### Summary of Last 7 Days

The summary shows the following information for the past seven days that the Assessment was run:

- $n$   Assessments in compliance
- $n$   Assessments with vulnerable objects
- $n$   Vulnerabilities found

### Assessment Summary

The summary will reflect the specific assessment and the domain and tenant results currently being viewed.

### Assessment Trends

Select the Assessment Trends tab to monitor assessments results over time to understand how vulnerabilities change across recent days (7, 30, 60, or 90), weeks (26, 52, or 78), or months (12, 24, 36, or 48) and filter the view to focus on all vulnerabilities or vulnerable objects.

Interacting with the chart:

- Hover over a point to view the exact value for that date.
- Show/Hide series: Click a legend item (such as Avg. Failed Vulnerabilities) to toggle that line on or off. This helps focus on a single series without clutter.


Read common patterns

- High red line with flat gray/yellow: Many items evaluated, few failures or inconclusives—generally positive.
- Rising gray line: Failures are increasing—investigate recent configuration changes or new findings.
- Rising yellow line: Inconclusive results are increasing—review assessment prerequisites.



### Evaluated Vulnerabilities

A list of evaluated vulnerabilities, which provides the following information:


- **Discovery Type** in which the vulnerability is defined
- **Vulnerability** name, which links to [vulnerability-specific detail](#), including any objects the vulnerability was detected in.
- **Identity Defense Intelligence**: Click the Identity Defense Intelligence icon next to the vulnerability to view a detailed summary, including recent trends, key highlights, recommended remediation steps, and suggested follow-up questions to support further investigation.
- Date and time when the vulnerability was **Last Detected**

 **NOTE:** This field displays the signed-in user's local date and time.

- Number of **Vulnerable Objects** found

 **NOTE:** A  icon indicates that an error occurred while the vulnerability was being evaluated.

- **Prevalence**: Percentage of similar size organizations where this vulnerability is reported.
- Number of **Inconclusive** results
- **Created by** either:
  - System (for pre-defined Discoveries and Vulnerabilities)

- User (for user-created Discoveries and Vulnerabilities)
- a graphical representation of the **7 Day Trend** for the Vulnerability
  -  **TIP:** Hover over the line graph to see the number of vulnerabilities (if any) detected per day.

## Viewing Details for an Assessed Vulnerability

When you select a **Vulnerability** from an Assessment's [Results](#) page, detail about the assessed vulnerability is displayed. The left side of the page includes detailed information about the vulnerability as defined in the [Discovery](#).

### Assessment Trend

A graph depicts color-coded results over the past days, weeks, or months that the Assessment was run.

The default value is the past 7 days. You can, however, select to view the trends by day (7, 30, 60, or 90), by weeks (26, 52, or 78), or by months (12, 24, 36, or 48). When the selected range is greater than 7 days, the chart shows average values for the chosen time unit (such as day, week, or month), and the grid below does not display individual vulnerable objects. The trending information presented is per Vulnerability.



**Compliant objects**



**Vulnerable objects**



**Error**



**NOTE:** An Error state indicates that an error occurred during data collection (for example, the server containing the objects to be evaluated could not be reached).

If an error occurred, the appropriate message displays.




**Inconclusive**



**NOTE:** An Inconclusive state indicates that data could not be collected for a non-error-related reason. The reason may be:

- The scope of an Assessment includes Tier Zero or Privileged objects but no Tier Zero or Privileged objects were found.
- An Assessment involves both Active Directory and Entra Id workloads, but both are not configured.
- The number of Tier Zero or Privileged objects exceeded the maximum number (10,000) that could be evaluated,
- [Permissions were insufficient](#) to collect the data.
- [The Assessment requires a Premium license](#), but the Organization has a free license.

If results were inconclusive for individual objects, hover over the  icon for a description of the reason.

### **i** TIPS:

- Select the Identity Defense Intelligence icon to view a summary of the vulnerability. The summary includes trend information, key points, recommended remediation steps, and follow-up questions to help with implementation.
- Use State Filtering to show only the states you want to focus on in the graph. (Note: The Compliant Objects state is always hidden by default.)
- Hover over the graph to see the number of vulnerable objects detected for each day.
- Click on an area of the graph to display details about that Assessment.

Below the graph is a list of the **Vulnerable Objects** (up to 100,000) found out of the total number of **Assessed Objects** for the selected area of the graph.

### **i** NOTES:

- If a group is identified as vulnerable, all of the members of that group (including via nested groups) are included in the Vulnerable Objects total. Click the link to view the list of the affected objects.
- If more than 100,000 vulnerable objects are returned, it is advisable to investigate why so many objects are found to be vulnerable. For example, all users may have been added to a group they don't belong in.
- For User and Computer vulnerabilities, the column **Is Account Enabled?** is included, allowing you to prioritize enabled accounts when implementing a remediation.
- For certain vulnerabilities, you can click the Principal Name or Display Name link to view detailed information about the object. This may include object properties, any affected Tier Zero objects, and group members (for group objects only).

#### **To download the Vulnerable Objects list to a CSV file:**

- From the details page for the vulnerable objects, click **Export to CSV**.

The file will include all of the objects displayed in the Vulnerable Objects list.

## Discoveries and Vulnerabilities

Discoveries are evaluated by Assessments to identify vulnerabilities in your organization's Active Directory and/or Entra ID. Identity Defense comes with several pre-defined Discoveries for [Active Directory](#) and [Entra ID](#), and you can also [create your own Discoveries](#).

## Discoveries List

The Discoveries tab displays a list of all Discoveries, both pre-defined and user-created, for the organization along with the following information for each:

- the **Discovery Type** (with a link to Discovery Details)
- **Created By** either:
  - **System** (for a pre-defined Discovery provided by Quest)  
OR
  - **User** (for a user-created Discovery)
- the **In Assessment** number
- each **Vulnerability** in the Discovery

## Pre-Defined Active Directory Discoveries

Identity Defense comes with the following pre-defined Discoveries for Active Directory vulnerabilities.

**i** | **NOTE:** "System" displays in the Created By field of the Discoveries list when a Discovery type is pre-defined.

Discovery Type	Description
<a href="#">Credential Access</a>	Techniques deployed by adversaries on systems and networks to steal usernames and credentials for re-use.
<a href="#">Defense Evasion</a>	Techniques used by adversaries to avoid detection. Evasion techniques include hiding malicious code within trusted processes and folders, encrypting or obfuscating adversary code, or disabling security software.
<a href="#">Discovery</a>	Techniques used by adversaries to obtain information about systems and networks that they are looking to exploit or use for their tactical advantage.
<a href="#">Initial Access</a>	Techniques used by adversaries to obtain a foothold within a network, such as targeted spear-phishing, exploiting vulnerabilities or configuration weaknesses in public-facing systems.
<a href="#">Lateral Movement</a>	Techniques that allow adversaries to move from one system to another within a network.
<a href="#">Persistence</a>	Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
<a href="#">Privilege Escalation</a>	Techniques used by adversaries to gain higher-level privileges on a system, such as local administrator or root.
<a href="#">Reconnaissance</a>	Techniques used by adversaries to gain a thorough understanding and complete mapping of your environment for later use.

## Additional Permissions Required for Specific Vulnerabilities

In addition to the permissions required for the hybrid agent, the service account (which the **Collect Active Directory object data** action uses) must be a member of the **Domain Admins** group for the following pre-defined vulnerabilities and any vulnerabilities [created](#) using the same template.

- Domain Controller is running SMBv1 protocol
- Printer Spooler service is enabled on a domain controller
- DNS zone configuration allows anonymous record updates

For the vulnerability gMSA root key access, the account must be a member of the **Domain Admins** or **Enterprise Admins** group.

If the required permission is not granted, Assessment results for these vulnerabilities will return as **Inconclusive**.

## Discovery for Credential Access Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Active Directory Discovery for Credential Access.

**i** **NOTE:** Credential Access techniques are deployed by adversaries on systems and networks to steal usernames and credentials for re-use.

Vulnerability Template	Vulnerability	Risk	What to find
User accounts with Service Principal Names using default encryption type	<p><b>Name:</b> User accounts with Service Principal Names using default encryption type</p> <p><b>Default Scope:</b> All users that have Service Principal values</p>	<p>Users that do not have configured encryption types rely on the default encryption type. As of April 2026, the default encryption type for service tickets is changing from RC4 to AES. While this will improve security by reducing exposure to Kerberoasting attacks, it may cause authentication issues with certain legacy platforms or applications.</p> <p><b>Remediation:</b> Determine if the platform or application accessed by the user account requires RC4, and either update the platform or application to support AES (preferred) or reach out to Microsoft at <a href="mailto:stillneedrc4@microsoft.com">stillneedrc4@microsoft.com</a> with information about the device and scenario.</p>	User accounts in scope with Service Principal Name and msds-SupportedEncryptionTypes set to <b>0</b> or <b>Not Set</b>
Users DES encryption attribute status	<p><b>Name:</b> User accounts using DES encryption to log in</p> <p><b>Default scope:</b></p>	DES encryption is weak and easy for an adversary to crack. User accounts configured to use DES encryption for authentication	User accounts in scope that have "Use only Kerberos DES encryption types for this account <b>enabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
	All users	<p>are particularly vulnerable to being compromised.</p> <p><b>Remediation:</b> To resolve vulnerability, in the account's Account tab - Account options, uncheck "Use only Kerberos DES encryption types for this account".</p>	
Account password reversible encryption status	<p><b>Name:</b> User accounts have a reversible password</p> <p><b>Default scope:</b> All users</p>	<p>User accounts with the "Store password using reversible encryption" enabled will have their passwords stored in a manner that can be easily harvested by an adversary looking for an entry point to the directory.</p> <p><b>Remediation:</b> To resolve vulnerability, in the account's Account tab - Account options, uncheck "Store password using reversible encryption".</p>	User accounts in scope that have "Store password using reversible encryption" <b>enabled</b>
	<p><b>Name:</b> Computer accounts with reversible password</p> <p><b>Default scope:</b> All computers</p>	<p>Computer accounts with the "Store password using reversible encryption" enabled will have their passwords stored in a manner that can be easily harvested by an adversary looking for an entry point to the directory.</p> <p><b>Remediation:</b> Disable "Store password using reversible encryption" unless the setting is required for the Challenge Handshake Authentication Protocol (CHAP) through remote access or Internet Authentication Services (IAS) or Digest Authentication in Internet</p>	Accounts in scope that have "Store password using reversible encryption" enabled

Vulnerability Template	Vulnerability	Risk	What to find
		Information Services (IIS). Set the "Store password using reversible encryption" to false on all Computer accounts either through the computer's local security policy or the assigned group policy.	
Users Kerberos preauthentication status	<p><b>Name:</b> User accounts with Kerberos pre-authentication disabled</p> <p><b>Default scope:</b> All users</p>	<p>User accounts with Kerberos pre-authentication disabled can be compromised as part of ASREP-Roasting attacks.</p> <p><b>Remediation:</b> To resolve vulnerability, in the account's Account tab - Account options, uncheck "Do not require Kerberos preauthentication".</p>	User accounts in scope that have "Do not require Kerberos preauthentication" <b>enabled</b>
Users Service Principal Name status	<p><b>Name:</b> Non-Tier Zero user accounts with Service Principal Names</p> <p><b>Default scope:</b> All except Tier Zero users</p>	<p>User accounts with Service Principal Names (SPNs) defined are exposed to Kerberos-based authentication attacks, providing an adversary with an entry point to the directory.</p> <p><b>Remediation:</b> To resolve vulnerability, remove the Service Principal Name from the user object if possible. If the Service Principal Name cannot be removed, enforce a very strong password on the user object which contains 32 characters with upper case, lower case, numeral, and special characters.</p>	User accounts in scope that have "Service Principal Name" <b>not empty</b>
Users delegated account attribute status	<p><b>Name:</b> Tier Zero account can be delegated</p> <p><b>Default scope:</b> Tier Zero users</p>	<p>Administrator accounts that are not configured to disallow delegation can be delegated and taken control of by an adversary.</p> <p><b>Remediation:</b></p>	User accounts in scope which have "This account is sensitive and cannot be delegated" <b>disabled</b> and are not members of the "Protected Users" group

Vulnerability Template	Vulnerability	Risk	What to find
		To resolve vulnerability, ensure that administrator accounts are configured so that the "This account is sensitive and cannot be delegated" option is enabled or the accounts are added to the Protected Users group.	
Users Password Never Expires status	<p><b>Name:</b> Non-Tier Zero user accounts configured for Password Never Expires</p> <p><b>Default scope:</b> All except Tier Zero users</p>	<p>User accounts with passwords that are not cycled regularly are more susceptible to brute force password cracking attempts. Accounts that are configured to never require a password change should be remediated accordingly.</p> <p><b>Remediation:</b> To resolve vulnerability, on the user properties Account tab, ensure the "Password never expires" option is unchecked.</p>	User accounts in scope that have "Password Never Expires" <b>enabled</b>
	<p><b>Name:</b> Tier Zero user accounts configured for Password Never Expires</p> <p><b>Default scope:</b> Tier Zero users</p>	<p>Administrative accounts with passwords that are not cycled regularly are more susceptible to brute force password cracking attempts. Accounts that are configured to never require a password change should be remediated accordingly.</p> <p><b>Remediation:</b> To resolve vulnerability, on the user Properties Account tab, make sure Password never expires is unchecked.</p>	
Protected Users group membership status	<p><b>Name:</b> Protected Users group is not being used</p> <p><b>Default scope:</b> Tier Zero users</p>	The Protected Users group should be used to protect Tier Zero user accounts from attacks to steal their credentials. If the group is not in use, Tier Zero accounts are exposed to possible	User accounts in scope that <b>are not</b> members of the "Protected Users" group

Vulnerability Template	Vulnerability	Risk	What to find
		<p>credential theft.</p> <p><b>Remediation:</b></p> <p>Members of the Protected Users group are blocked from using NTLM authentication. Therefore, do not add Tier Zero users to the Protected Users group if they require access to resources that require NTLM to authenticate. In addition, accounts for services and computers should never be members of the Protected Users group as it will cause authentication to fail.</p> <p>To resolve this vulnerability, consider adding any Tier Zero account that does not require NTLM and is not a service account to the Protected Users group.</p>	
Account last used	<p><b>Name:</b> Enabled Tier Zero user accounts that are inactive</p> <p><b>Default scope:</b> Tier Zero users</p>	<p>The number of Tier Zero accounts in a domain should be limited and closely monitored. Tier Zero accounts that are not regularly used are ripe targets for being compromised without detection, allowing an adversary more time to perform reconnaissance in the environment.</p> <p><b>Remediation:</b></p> <p>After inactive accounts are identified, it is recommended to disable those user accounts, wait several weeks, and then delete the accounts if no issues have been reported.</p>	<p>Accounts in scope that were last used <b>more than 90</b> days ago</p> <p>NOTE: The number of days is editable.</p>
	<p><b>Name:</b> Tier Zero computers</p>	<p>Tier Zero computers such as domain controllers will</p>	<p>Accounts in scope that were last used <b>more than 30</b> days ago</p>

Vulnerability Template	Vulnerability	Risk	What to find
	<p>that have not recently authenticated to the domain</p> <p><b>Default scope:</b> Tier Zero computers</p>	<p>authenticate with the domain regularly. Domain controllers that are not authenticating and offline are susceptible to having password hashes stolen or used to introduce nefarious changes to the directory.</p> <p><b>Remediation:</b> Tier Zero computers that are offline for extended periods of time should be investigated. Domain controllers that are out of sync with the domain over 30 days should be reinstalled or removed.</p>	<p>NOTE: The number of days is editable.</p>
<p>Domain controller SMBv1 protocol status</p> <p><b>i</b> <b>NOTE:</b> For vulnerabilities that use this template, the hybrid agent service account must be a <a href="#">member of the Domain Admins group</a>.</p>	<p><b>Name:</b> Domain Controller is running SMBv1 protocol</p> <p><b>Default scope:</b> N/A</p>	<p>The SMBv1 protocol supports legacy insecure authentication protocols. If running, it can allow an adversary to access a domain controller and harvest credentials or execute commands.</p> <p><b>Remediation:</b> Disable the SMBv1 protocol on the impacted domain controllers.</p>	<p>Computers in scope that have the SMBv1 protocol enabled</p>
<p>Domain controller Print Spooler status</p> <p><b>i</b> <b>NOTE:</b> For vulnerabilities that use this template, the hybrid agent service account must be a <a href="#">member of the Domain Admins group</a>.</p>	<p><b>Name:</b> Printer Spooler service is enabled on a domain controller</p> <p><b>Default scope:</b> N/A</p>	<p>If an account has unconstrained delegation configured over the Printer Spooler service on a domain controller, an adversary can use that attack path to gain access to the domain controller and leverage the Printer Spooler service vulnerability to remotely execute code or obtain the password hashes contained on the domain controller.</p> <p><b>Remediation:</b> Disable the Printer Spooler</p>	<p>Domain controller that has the Print Spooler service <b>enabled</b></p>

Vulnerability Template	Vulnerability	Risk	What to find
		service on all domain controllers.	
Group Policy "Store passwords using reversible encryption" setting	<p><b>Name:</b> Group Policy allows reversible passwords</p> <p><b>Default scope:</b> All Group Policies</p>	<p>Group Policies containing reversible passwords are an attractive target as those passwords can be easily decrypted and used to elevate an adversary's privileges.</p> <p><b>Remediation:</b> Configure the "Store passwords using reversible encryption" setting located in "Computer Configuration - Policies - Windows Settings - Security Settings - Account Policies - Password Policy" section of the Group Policy to "disabled". There are a couple of use cases where this setting would be enabled: Challenge Handshake Authentication Protocol (CHAP) for remote access or Internet Authentication Services (IAS), Internet Information Services (IIS) Digest Authentication. Disabling this setting could break these applications. If this is needed for backwards compatibility the recommendation is to apply this to a single user or smallest subset of users vs the full domain.</p>	Group Policy objects in scope that have "Store passwords using reversible encryption" <b>enabled</b>
Domain "Replicating Directory Changes All" and "Replicating Directory Changes" delegation	<p><b>Name:</b> Non-Tier Zero accounts can steal password hashes (DCSync)</p> <p><b>Default scope:</b> All except Tier Zero accounts</p>	If non-Tier Zero accounts have the "Replicating Directory Changes All" and "Replicating Directory Changes" permissions, they can impersonate a domain controller and receive a replicated copy of the Active Directory database that will	Domain has "Replicating Changes All" and "Replicating Directory Changes" set to <b>Allow</b> for any accounts in scope

Vulnerability Template	Vulnerability	Risk	What to find
		<p>allow them to steal password hashes.</p> <p><b>Remediation:</b> These delegations should be removed unless there is a compelling reason for their existence.</p>	
Object read-only domain controller msDS- NeverRevealGroup status	<p><b>Name:</b> Protected group credentials exposed on read-only domain controllers</p> <p><b>Default scope:</b></p> <ul style="list-style-type: none"> <li>Administrators</li> <li>Account Operators</li> <li>Backup Operators</li> <li>Denied RODC Password Replication Group</li> <li>Server Operators</li> </ul>	<p>Read-only domain controllers (RODCs) should be configured so that Tier Zero user and group credentials are not replicated. If Tier Zero passwords are replicated, an adversary who gains access to the RODC can harvest the credentials and elevate their privileges.</p> <p><b>Remediation:</b> Ensure the built-in groups Administrators, Account Operators, Backup Operators, Denied RODC Password Replication Group, and Server Operators are set to "Deny" on the Password Replication Policy tab of the read-only domain controller in Active Directory Users and Computers.</p>	Objects in scope are <b>not listed</b> in the read-only domain controller "msDS- NeverRevealGroup" attribute
RODC password replication policy	<p><b>Name:</b> Tier Zero account token can be stolen from a read-only domain controller</p> <p><b>Default scope:</b> All groups except Allowed RODC Password Replication</p>	<p>Read-only domain controllers (RODCs) should be configured so that Tier Zero user and group credentials are not replicated. If Tier Zero passwords are replicated, an adversary who gains access to the RODC can harvest the credentials and elevate their privileges.</p> <p><b>Remediation:</b> Remove the account from the msDS-</p>	Objects in scope are listed in the read-only domain controller "msDS- RevealOnDemandGroup" attribute

Vulnerability Template	Vulnerability	Risk	What to find
		RevealOnDemandGroup attribute. Locate the account on the Properties - Password Replication Policy tab of read-only domain controller in Active Directory Users and Computers and either remove the account or change the setting to Deny.	
Account password last changed	<p><b>Name:</b> Managed and Group Managed Service accounts that have not cycled their password recently</p> <p><b>Default scope:</b> All Service Accounts</p>	<p>Managed Service Accounts (MSA) and Group Managed Service accounts (gMSA) that have not had their passwords cycled recently could indicate they've been compromised.</p> <p><b>Remediation:</b> The reason that prevented the managed service account from updating their password the default 30 days should be investigated. Such as verifying if the msDS-ManagedPasswordInterval attribute on the service account is set to a value greater than 30.</p>	<p>Accounts in scope that have not updated their password within last <b>30</b> days.</p> <p>NOTE: The number of days is editable.</p>
Computer account "ms-Msc-AdmPwd" attribute permissions	<p><b>Name:</b> Non-Tier Zero accounts with Microsoft Local Administrator Password (LAPS) access</p> <p><b>Default scope:</b> All except Tier Zero Users, Groups, and Computers</p>	<p>An incorrectly configured Microsoft Local Administrator Password (LAPS) can expose the local Administrator password (ms-Mcs-AdmPwd attribute) for an adversary to steal. Confidential attributes such as ms-Mcs-AdmPwd can only be viewed by accounts with "Full control" (GenericAll) or "All extended rights" (ExtendedRight) on a computer object, and unlike other attributes, is not accessible by Authenticated Users.</p> <p><b>Remediation:</b></p>	<p>Computer "ms-Mcs-AdmPwd" attribute has <b>GenericAll</b> or <b>ExtendedRight</b> set for any account in scope</p>

Vulnerability Template	Vulnerability	Risk	What to find
User permission on Resource-Based Constrained Delegation settings for KRBTGT	Non-Tier Zero user accounts with write permissions over Resource-Based Constrained Delegation on the KRBTGT account <b>Default scope:</b> All except Tier Zero users	Review accounts that can view the "ms-Mcs-AdmPwd" attribute of a computer account and determine if the access is required. If not required, remove the granted permission.  Non-Tier Zero user accounts that have the permission to write Resource-Based Constrained Delegation (RBCD) on the KRBTGT account can allow an adversary to impersonate any user and take control of the KRBTGT account, and from there, the entire domain. <b>Remediation:</b> To resolve vulnerability, review the KRBTGT object security to determine if non-Tier Zero user accounts should have Write permissions in the Resource-Based Constrained Delegation attribute. If not required, remove them.	Users in scope that have <b>Allow Write</b> permission on Resource-Based Constrained Delegation settings for KRBTGT account
Tier Zero computers permission granted on Resource-Based Constrained Delegation	<b>Name:</b> Tier Zero computer that has write permissions on Resource-Based Constrained Delegation granted to a non-Tier Zero account <b>Default scope:</b> All except Tier Zero objects	Non-Tier Zero accounts that have the permission to write Resource-Based Constrained Delegation (RBCD) on a Tier Zero computer such as a domain controller can allow an adversary to impersonate any user and take control of the DC. <b>Remediation:</b> To resolve vulnerability, review the Tier Zero computer security to determine if non-Tier Zero user accounts should have	Tier Zero computers that have accounts in scope with <b>Allow Write</b> permission on Resource-Based Constrained Delegation

Vulnerability Template	Vulnerability	Risk	What to find
		<p>Write permissions in the Resource-Based Constrained Delegation attribute. If not required, remove Write permissions on the attribute.</p>	
<p>gMSA root key access</p> <p><b>i</b> <b>NOTE:</b> For vulnerabilities that use this template, the hybrid agent service account must be a <a href="#">member of the Domain Admins or Enterprise Admins group</a>.</p>	<p><b>Name:</b> Non-Tier Zero accounts can access the gMSA root key</p> <p><b>Default scope:</b> All except Tier Zero objects</p>	<p>Non-Tier Zero accounts with access to the Group Key Distribution Services Master Root Keys could gain access to any gMSA account in the environment.</p> <p>The Hybrid Agent service account requires Domain Admin or Enterprise Admin permissions to read the security details on msKds-ProvRootKey objects. Vulnerability results with zero assessed objects indicates that either no msKds-ProvRootKey objects exist in the domain or the Hybrid Agent service account does not have permissions to read the msKds-ProvRootKey objects.</p> <p><b>Remediation:</b> Restrict access to the msKds-ProvRootKey objects in the domain to only Tier Zero users and groups. The default groups that have access to the objects are SYSTEM, Domain Admins, and Enterprise Admins.</p>	<p>Accounts in scope that have <b>Allow Read or Allow Write</b> permission for msKds-RootKeyData attribute on msKds-ProvRootKey objects</p>
<p>Write access on certificate templates</p>	<p><b>Name:</b></p> <p><b>Default scope:</b> All except Tier Zero users and groups and Foreign Security</p>	<p>Non-Tier Zero users with write access on certificate templates allow attackers to create illegitimate certificates for any user, which allows</p>	<p>Accounts in scope have <b>Allow Write</b> permissions on pKICertificateTemplate objects in the "Certificate Templates" container</p>

Vulnerability Template	Vulnerability	Risk	What to find
	Principal (S-1-5-9)	<p>them to elevate their privileges and compromise the domain.</p> <p>A template is misconfigured at the access control level if it has Access Control Entries (ACEs) that allow unintended, or otherwise non-Tier Zero, AD principals to edit sensitive security settings in the template.</p> <p><b>Remediation:</b> Remove non-Tier Zero users from having any write access to "Certificate Templates" container in Configuration - Services - Public Key Services or any pKICertificateTemplate object in that container.</p>	
AdminSDHolder inheritance status	<p><b>Name:</b> Inheritance is enabled on the AdminSDHolder container</p> <p><b>Default scope:</b> N/A</p>	<p>The AdminSDHolder object is rarely modified. If inheritance is enabled on the ACL of this object, it could be the result of an adversary propagating changes in the directory that make accessing additional Tier Zero accounts easier for them.</p> <p><b>Remediation:</b> On the AdminSDHolder object in the System container, open Security - Advanced, click "Disable inheritance", and select the option to "Remove all inherited permissions from this object".</p>	AdminSDHolder permission inheritance set to <b>enabled</b>
User access to gMSA password	<p><b>Name:</b> Non-Tier Zero users with access to gMSA password</p> <p><b>Default scope:</b></p>	<p>Non-Tier Zero users that are members of a group that is listed in a Group Managed Service Account's (gMSA) msDS-</p>	Users in scope that <b>are</b> able to retrieve the password for a Group Managed Service Account (gMSA)

Vulnerability Template	Vulnerability	Risk	What to find
	All except Tier Zero users	<p>groupMSAMembership attribute can gain access to the password of the account and move laterally to resources it manages.</p> <p><b>Remediation:</b> Unless there is a business reason, remove non-Tier Zero users from the group that is listed in the Group Managed Service Account's (gMSA) msDS-groupMSAMembership attribute.</p>	
Domain trust Kerberos AES encryption support status	<p><b>Name:</b> Domain trust without Kerberos AES encryption enabled</p> <p><b>Default scope:</b> All Trusted Domains</p>	<p>The setting "The other domain supports Kerberos AES Encryption" determines whether the trust supports AES encryption. Trusts that do not have the setting enabled will use RC4 encrypted Kerberos tickets which are considered significantly less secure than AES.</p> <p><b>Remediation:</b> Removing the previously allowed RC4_HMAC_MD5 encryption suite may have operational impacts and must be thoroughly tested for the environment before changing.</p> <p>In the Active Directory Domains and Trusts console, right-click the forest root domain, and select Properties. Select the Trusts tab, highlight the trust, and then click the Properties button. Then enable the setting "The other domain supports Kerberos AES Encryption".</p>	Domain trust in scope has Kerberos AES encryption support <b>disabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
KRBTGT account password last changed	<p><b>Name:</b> Kerberos KRBTGT account password has not changed recently</p> <p><b>Default scope:</b> N/A</p>	<p>The KRBTGT account is a domain default account that acts as a service account for the Key Distribution Center (KDC) service. During the Kerberos Authentication process, TGTs are issued to accounts requesting access to resources. These TGTs are encrypted by cryptographic key which is derived from the password of the KRBTGT account. In many Active Directory environments, the password for the KRBTGT account has not been changed since before moving to the 2008 domain functional level. This means that the password is not AES encrypted, which can expose the account to attack and break trusts with forests that require AES encryption.</p> <p><b>Remediation:</b> Microsoft does not have a specific recommendation regarding password reset frequency for the KRBTGT account other than it is that the password is reset regularly. The Security Technical Implementation Guide (STIG) recommends resetting the password every 180 days. It is also considered good practice to reset the KRBTGT password whenever a Tier Zero account leaves an organization since they may have the ability to use a ticket that was previously generated while they had access. The KRBTGT</p>	Kerberos KRBTGT account password has not been updated within the last <b>180</b> days

Vulnerability Template	Vulnerability	Risk	What to find
Group Policy "Allow Administrator account lockout" status	<p><b>Name:</b> Group Policy does not enforce built-in Administrator account lockout on all computers</p> <p><b>Default scope:</b> All computers</p>	<p>account keeps the two most recent passwords in password history. Therefore, the password should be reset twice to invalidate all tickets issued from the old KRBTGT password. When the tickets are invalidated, all machines and all applications will contact the domain controllers in the environment for new Kerberos tickets.</p> <p>In order to prevent brute force attacks, Microsoft implemented account lockouts for built-in Administrator accounts and added the ability to enforce and control the lockout behavior using the GPO setting "Allow Administrator account lockout". The lockout behavior only affects network logons, such as RDP attempts. Console logons are still allowed during the built-in Administrator account lockout period.</p> <p>Computers using Windows 11, version 22H2 or setup with October 11, 2022, Windows cumulative updates pre-installed may have the Local Security Policy "Allow Administrator account lockout" setting enabled by default but older Windows OS versions that had the October 11, 2022, Windows cumulative update installed after initial setup will have the "Allow Administrator account lockout" setting not configured.</p>	Computer objects in scope do not have an assigned group policy with "Allow Administrator account lockout" <b>Enabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
AZUREADSSOACC password last changed	<p>Microsoft Entra seamless single sign-on (AzureADSSOACC) account password has not changed recently</p> <p><b>Default scope:</b> N/A</p>	<p><b>Remediation:</b></p> <p>Configure the "Allow Administrator account lockout" setting located in "Computer Configuration - Policies - Windows Settings - Security Settings - Account Policies - Account Lockout Policy" section of the Group Policy to "Enabled".</p> <p>In addition, if not already configured, the Microsoft baseline recommendation is to set "Account lockout duration" to "10 minutes", "Account lockout threshold" to "10 invalid attempts", and "Reset account lockout counter after" to "10 minutes". This will ensure accounts would be locked out after 10 failed attempts within 10 minutes and the lockout would last for 10 minutes.</p> <p>The computer account AZUREADSSOACC is created in each Active Directory forest that is synchronized to Microsoft Entra ID using Microsoft Entra Connect. The computer account's Kerberos decryption key is shared securely with Microsoft Entra ID. It is highly recommended by Microsoft that the Kerberos decryption key of the AZUREADSSOACC computer account is updated at least every 30 days.</p> <p><b>Remediation:</b></p> <p>Using a Domain Administrator account that is</p>	<p>AzureADSSOACC account password has not been updated within last <b>30</b> days</p>

Vulnerability Template	Vulnerability	Risk	What to find
		not a member of the Protected Users group, update the Kerberos decryption key for the AZUREADSSO computer account with the Update-AzureADSSOForest command. Repeat the process for each Active Directory Forest. Ensure that you don't run the Update-AzureADSSOForest command more than once per forest. Otherwise, the feature stops working until the users' Kerberos tickets expire and are reissued by the on-premises Active Directory.	

## Discovery for Defense Evasion Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Active Directory Discovery for Defense Evasion.

**i** **NOTE:** Defense Evasion techniques are used by adversaries to avoid detection. Evasion techniques include hiding malicious code within trusted processes and folders, encrypting or obfuscating adversary code, or disabling security software.

Vulnerability Template	Vulnerability	Risk	What to find
Built-in Administrator account last used	<p><b>Name:</b> Built-in Administrator account that has been used</p> <p><b>Default scope:</b> N/A</p>	<p>The Built-in Administrator should never be used because it cannot be tied back to an individual. Any use of the account likely indicates it has been compromised.</p> <p><b>Remediation:</b> To resolve vulnerability, make sure that the Built-in Administrator account (if it has been renamed, the account whose SID is S-1-5-21-domain-500) has not been used within the last 30 days.</p>	<p>Built-in Administrator account was last used <b>less than 30</b> days ago</p> <p>NOTE: The number of days is editable.</p>
Members of protected groups adminCount attribute value	<p><b>Name:</b> User accounts in protected groups that are not protected by</p>	<p>Microsoft uses the adminCount attribute to indicate an object has had its ACL modified by the system to be more secure as it was a member of one of the administrative groups. Accounts that are members of the protected groups whose adminCount attribute is not</p>	<p>User objects in scope that are members of protected groups and have adminCount</p>

Vulnerability Template	Vulnerability	Risk	What to find
	<p>AdminSDHolder (SDProp)</p> <p><b>Default scope:</b> All users</p>	<p>set to 1 could be evidence of an adversary who has breached the directory and trying to remain undetected.</p> <p>Protected groups include:</p> <ul style="list-style-type: none"> <li>• Account Operators (S-1-5-32-548)</li> <li>• Administrators (S-1-5-32-544)</li> <li>• Backup Operators (S-1-5-32-551)</li> <li>• Cert Publishers (S-1-5-domain-517)</li> <li>• Domain Admins (S-1-5-domain-512)</li> <li>• Domain Controllers (S-1-5-domain-516)</li> <li>• Enterprise Admins (S-1-5-root_domain-519)</li> <li>• Read-only Domain Controllers (only since Windows Server 2008) (S-1-5-domain-521)</li> <li>• Replicator (S-1-5-32-552)</li> <li>• Schema Admins (S-1-5-root_domain-518)</li> <li>• Server Operators (S-1-5-32-549)</li> </ul> <p><b>Remediation:</b> Investigate accounts that are members of the protected groups whose adminCount attribute is not set to 1 to determine why the attribute is not set by Active Directory.</p>	<p>attribute set to <b>0</b> or not set.</p>
Account Primary Group ID permissions	<p><b>Name:</b> User accounts without readable Primary Group ID</p> <p><b>Default scope:</b> All users</p>	<p>Inability to read the Primary Group ID can indicate that read permissions have been removed by an adversary trying to cover their tracks as they elevate their permissions in an environment.</p> <p><b>Remediation:</b> To resolve vulnerability, review the User object and remove any Deny Read permissions which would prevent the Primary Group ID from being read.</p>	<p>Accounts in scope that have <b>Deny Read</b> set for the "Primary Group ID" attribute</p>
	<p><b>Name:</b> Computer accounts without readable Primary Group ID</p> <p><b>Default scope:</b> All computers</p>	<p>Inability to read the Primary Group ID can indicate that read permissions have been removed by an adversary trying to cover their tracks as they elevate their permissions in an environment.</p> <p><b>Remediation:</b> To resolve vulnerability, review the computer object and remove any Deny read permissions which would prevent the Primary Group ID attribute from being read.</p>	

Vulnerability Template	Vulnerability	Risk	What to find
Active Directory Operator group AdminSDHolder protection status	<p><b>Name:</b> Active Directory Operator groups that are not protected by AdminSDHolder</p> <p><b>Default scope:</b> N/A</p>	<p>The AdminSDHolder object maintains a template of permissions that are automatically applied to Tier Zero groups to ensure their security. A change to the AdminSDHolder behavior could indicate that an adversary has compromised the directory and is covering their tracks. The dwAdminSDExMask bit in the dsHeuristics attribute of CN=DirectorService,CN=Windows NT,CN=Services,CN=Configuration,DC=domain,DC=com, can be configured so that the following Active Directory Operator groups (and their nested members) are no longer protected:</p> <ul style="list-style-type: none"> <li>• Account Operators</li> <li>• Server Operators</li> <li>• Print Operators</li> <li>• Backup Operators.</li> </ul> <p><b>Remediation:</b> Set the 16th character (dwAdminSDExMask bit) of the dsHeuristics attribute to 0 to ensure that no Operator groups are excluded from AdminSDHolder protection. The dsHeuristics attribute is located on the Directory Service object in CN=Window NT,CN=Services, CN=Configuration,DC=domain,DC=com.</p>	The dsHeuristics attribute on the Directory Service object indicates <b>some Operator groups</b> are excluded from AdminSDHolder protection

## Discovery for Discovery Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Active Directory Discovery for Discovery.

**i** **NOTE:** Discovery techniques are used by adversaries to avoid detection. Evasion techniques include hiding malicious code within trusted processes and folders, encrypting or obfuscating adversary code, or disabling security software.

Vulnerability Template	Vulnerability	Risk	What to find
Account password last changed	<p><b>Name:</b> Tier Zero user accounts whose passwords have not</p>	<p>Administrator accounts with passwords that are not cycled regularly are more susceptible to brute force password cracking attempts. If a password manager or multi-factor authentication is not used, passwords should be updated a minimum of every 90 days.</p> <p><b>Remediation:</b></p>	Accounts in scope that have not updated their password within last <b>180</b> days

Vulnerability Template	Vulnerability	Risk	What to find
	changed recently <b>Default Scope:</b> Tier Zero users	To resolve vulnerability, update the administrator password and enforce a password policy to ensure the administrator account password is updated regularly.	

## Discovery for Initial Access Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Active Directory Discovery for Initial Access.

**i** | **NOTE:** Initial Access techniques are used by adversaries to obtain a foothold within a network, such as targeted spear-phishing, exploiting vulnerabilities or configuration weaknesses in public-facing systems.

Vulnerability Template	Vulnerability	Risk	What to find
Built-in Guest account status	<b>Name:</b> Built-in Guest account is enabled <b>Default scope:</b> N/A	The built-in Guest account enables access to Active Directory without requiring a password and should be disabled. <b>Remediation:</b> To resolve vulnerability, disable the built-in Guest account (if it has been renamed, the account whose SID is S-1-5-domain-501).	Built-in Guest accounts that are <b>enabled</b>
Anonymous access to Active Directory status	<b>Name:</b> Anonymous access to Active Directory is enabled <b>Default scope:</b> N/A	Anonymous access allows accounts to perform reconnaissance against Active Directory by binding to Active Directory over RPC (including over Name Service Provider Interface (NSPI)) without authenticating. Anonymous access to Active Directory is enabled using the fLDAPBlockAnonOps bit in the dsHeuristics attribute of CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=domain,DC=com. <b>Remediation:</b> Set the 7th character (fLDAPBlockAnonOps bit) of the dsHeuristics attribute to 0 to ensure that anonymous access is blocked. The dsHeuristics attribute is located on the Directory Service object in CN=WindowNT,CN=Services,CN=Configuration, DC=domain,DC=com.	The dsHeuristics attribute on the Directory Service object indicates Anonymous access to Active Directory is <b>enabled</b>
Active Directory user and group synchronization status	Active Directory Tier Zero object synchronized to	Tier Zero users or groups that are synchronized to Entra ID will have corresponding cloud objects. This can pose a security risk since organizations can	Active Directory users and groups in

Vulnerability Template	Vulnerability	Risk	What to find
	<p>Entra ID</p> <p><b>Default scope:</b> Tier Zero users and groups</p> <p>NOTE: If no Entra ID collection is available, an Inconclusive message is returned.</p>	<p>have password write-back enabled, which would leave Active Directory Tier Zero object under the influence of Entra ID users. While Entra ID is considered more secure than Active Directory, synchronizing Tier Zero accounts complicates knowing which accounts can control Tier Zero objects within the domain.</p> <p><b>Remediation:</b> If applicable to your organization, consider excluding Tier Zero accounts from synchronizing to Entra ID.</p>	scope that <b>are</b> synchronized to Entra ID

## Discovery for Lateral Movement Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Active Directory Discovery for Lateral Movement.

**i** **NOTE:** Lateral Movement techniques allow adversaries to move from one system to another within a network.

Vulnerability Template	Vulnerability	Risk	What to find
Account Trusted for Delegation attribute status	<p><b>Name:</b> User accounts with unconstrained delegation</p> <p><b>Default scope:</b> All users</p>	<p>The Kerberos TGT ticket can be captured when unconstrained delegation is enabled and then used to elevate the adversary's privileges to any service the TGT ticket has access to.</p> <p><b>Remediation:</b> To resolve vulnerability, remove the TRUSTED_FOR_DELEGATION flag in userAccountControl attribute. This can be performed in the account's Delegation tab - Account options. Make sure "Trust this user for delegation to any service (Kerberos only)" is not selected. If a Kerberos delegation is required, use one that is constrained.</p>	Accounts in scope that have Trusted for Delegation <b>enabled</b>
	<p><b>Name:</b> Computer accounts with unconstrained delegation</p> <p><b>Default scope:</b> All computers</p>	<p>The Kerberos TGT ticket can be captured when unconstrained delegation is enabled and then used to elevate the adversary's privileges to any service the TGT ticket has access to.</p> <p><b>Remediation:</b></p>	Accounts in scope that have Trusted for Delegation <b>enabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
	except domain controllers	Remove unconstrained delegation on the computer object from the computer's Properties - Delegation tab by ensuring "Trust this computer for delegation to any service (Kerberos only)" is not selected. If required, constrained delegation can be used by selecting the "Trust this computer for delegation to specified services only" option.	
Users Password Not Required attribute status	<p><b>Name:</b> User accounts do not require a password</p> <p><b>Default scope:</b> All users</p>	<p>An adversary can easily compromise a user account that does not require a password and find an attack path from that account to escalate their privileges.</p> <p><b>Remediation:</b> To resolve vulnerability, in the account's Attribute Editor tab, select userAccountControl and remove the PASSWD_NOTREQD value.</p>	User accounts in scope that have "Password not required" <b>enabled</b>
Domain Add computers to domain value	<p><b>Name:</b> All domain users can create computer accounts</p> <p><b>Default scope:</b> N/A</p>	<p>Without hardening, all domain users have the ability to create computer accounts in the domain. Improperly configured computer accounts are exposed to Kerberos authentication attacks. Only administrators should be able to add new computer accounts.</p> <p><b>Remediation:</b> In Active Directory Users and Computers Attribute Editor tab for the domain object, change the value of the ms-DS-MachineAccountQuota attribute (which is 10 by default) to a value of 0. This will prevent non-administrative users from being able to register new computer accounts within the domain.</p>	<p>Domain has the "ms-DS-MachineAccountQuota" attribute set to <b>more than 0</b></p> <p>NOTE: The operator and quota attribute value are editable.</p>
Account "Use any authentication protocol" status	<p><b>Name:</b> Accounts that allow Kerberos protocol transition delegation</p> <p><b>Default scope:</b> All users and computers</p>	<p>A service configured to allow Kerberos protocol transition will allow a delegated service to use any available authentication protocol. This can result in reduced authentication security and increase the chance of services being compromised by an adversary.</p> <p><b>Remediation:</b> In the account Properties -Delegation tab,</p>	Accounts in scope which have "Use any authentication protocol" <b>enabled</b> in delegation

Vulnerability Template	Vulnerability	Risk	What to find
		ensure configured delegation is not set to "Use any authentication protocol."	
Domain Unexpire Password permission delegation	<p><b>Name:</b> Non-Tier Zero accounts with Unexpire password permission delegation</p> <p><b>Default scope:</b> All except Tier Zero users and groups</p>	<p>If the "Unexpire password" permission is delegated an adversary could use it to restore the password of a Tier Zero principal.</p> <p>This vulnerability will not generate a Finding in Identity Defense.</p> <p><b>Remediation:</b> Except for the Domain Admins group, these delegations should be removed unless there is a compelling reason for their existence.</p>	Domain has "Unexpire password" set to <b>Allow</b> for any accounts in scope
Domain Migrate SID history permission delegation	<p><b>Name:</b> Non-Tier Zero accounts with Migrate SID history permission delegation</p> <p><b>Default scope:</b> All except Tier Zero users and groups</p>	<p>If the "Migrate SID history" permission is delegated an adversary can use it to elevate their privileges by adding a Tier Zero account to their SIDHistory attribute and obscuring the exploit.</p> <p><b>Remediation:</b> Except for the Domain Admins group, these delegations should be removed unless there is a compelling reason for their existence.</p>	Domain has "Migrate SID history" set to <b>Allow</b> for any accounts in scope
Domain Reanimate tombstones permission delegation	<p><b>Name:</b> Non-Tier Zero accounts with Reanimate tombstones permission delegation</p> <p><b>Default scope:</b> All except Tier Zero users and groups</p>	<p>If the "Reanimate tombstones" control access right is delegated an adversary could use it to restore and take control of a Tier Zero object.</p> <p><b>Remediation:</b> Except for the Domain Admins group, these delegations should be removed unless there is a compelling reason for their existence.</p>	Domain has "Reanimate tombstones" set to <b>Allow</b> for any accounts in scope
Group Policy "Add workstations to domain" setting Authenticated User status	<p><b>Name:</b> Tier Zero Group Policy allows Authenticated</p>	Without hardening, any authenticated user has permissions to create up to 10 computer accounts in the domain. Improperly configured computer accounts	Group Policy objects in scope <b>with</b> Authenticated Users configured in "Add workstations to domain" setting

Vulnerability Template	Vulnerability	Risk	What to find
	<p>Users to add computers to the domain</p> <p><b>Default scope:</b> All Tier Zero Group Policies</p>	<p>are exposed to Kerberos authentication attacks. Only administrators or other authorized users should have the ability to add new computer accounts.</p> <p><b>Remediation:</b> There are two methods to address this vulnerability.</p> <p>The first method is, in the Active Directory Users and Computers Attribute Editor tab for the domain object, change the value of the ms-DS-MachineAccountQuota attribute (which is 10 by default) to a value of 0. This will prevent non-administrative users from being able to register new computer accounts within the domain.</p> <p>The second method is to edit the "Add workstations to domain" setting located in "Computer Configuration - Policies - Windows Settings - Security Settings - Local Policies - User Rights Assignment" section of the Group Policy and remove "Authenticated Users".</p>	

## Discovery for Persistence Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Active Directory Discovery for Persistence.

**i** **NOTE:** Persistence techniques are used by adversaries to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

Vulnerability Template	Vulnerability	Risk	What to find
Foreign Security Principals Tier Zero group membership status	<p><b>Name:</b> Foreign Security Principals are members of a Tier Zero group</p> <p><b>Default scope:</b> All Foreign Security Principals</p>	<p>A Foreign Security Principal (FSP) is an object created by the system to represent a security principal in a trusted external forest. They can also represent special identities, such as Authenticated Users, Anonymous Logon, and Enterprise Domain Controllers. The FSP for a special identity is created when the special identity is added to a group.</p> <p>Foreign security principals can be added to Tier Zero groups in the local</p>	Foreign Security Principals in scope that <b>are</b> members of a Tier Zero group

Vulnerability Template	Vulnerability	Risk	What to find
	<p>Non-Tier Zero Group policy contains a scheduled task</p> <p><b>Default scope:</b> All non-Tier Zero Group Policies</p>	<p>domain but because they do not have the adminCount attribute, their origin can be difficult to audit. Thus adversaries can abuse this relationship to proceed without being detected.</p> <p><b>Remediation:</b> Investigate Foreign Security Principals that are members of the protected groups and remove the membership if appropriate.</p>	<p>Group Policy objects in scope <b>with</b> Scheduled Task configured</p>
<p>Group Policy contains Scheduled Task status</p>	<p>Tier Zero Group Policy contains a scheduled task</p> <p><b>Default scope:</b> All Tier Zero Group Policies</p>	<p>While there are legitimate uses for defining a scheduled task in a group policy, adversaries may abuse task scheduling registered in a group policy to facilitate initial or recurring execution of malicious code.</p> <p><b>Remediation:</b> In Group Policy Management, review the settings of the defined scheduled task to confirm it is valid and configured correctly. Setting to pay special attention to are Author (if applicable), user account running the task, and the process configured in Run field or Actions tab.</p> <p>While there are legitimate uses for defining a scheduled task in a group policy, adversaries may use task scheduling registered in a group policy to facilitate initial or recurring execution of malicious code. Scheduled tasks defined in Tier Zero group policies should be strictly monitored.</p> <p><b>Remediation:</b> In Group Policy Management, review the settings of the defined scheduled task to confirm it is valid and configured correctly. Setting to pay special attention to are Author (if applicable), user account running the task, and the process configured in Run field or Actions tab.</p>	<p>Group Policy objects in scope <b>with</b> Scheduled Task configured</p>

# Discovery for Privilege Escalation Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Active Directory Discovery for Privilege Escalation.

**i** **NOTE:** Privilege Escalation techniques are used by adversaries to gain higher-level privileges on a system, such as local administrator or root.

Vulnerability Template	Vulnerability	Risk	What to find
Active Directory workload identities Tier Zero status	<p><b>Name:</b> User or computer Active Directory workload identities that are Tier Zero</p> <p><b>Default scope:</b> N/A</p>	<p><b>Risk:</b> Tier Zero objects are the most critical assets within an organization's Active Directory while service accounts should adhere to a principle of least privilege. Over-privileged service accounts are considered security risks, since their compromise can allow attackers to gain unauthorized access to critical systems, sensitive data, and network resources.</p> <p><b>Remediation:</b> Review service accounts that are identified as Tier Zero objects and determine if lesser permissions can be granted to the account or if a non-Tier Zero object can be used in its place.</p>	User and computer Active Directory workload identities that are <b>Tier Zero objects</b>
Account Primary Group ID	<p><b>Name:</b> User accounts with non-default Primary Group IDs</p> <p><b>Default scope:</b> All users</p>	<p><b>Risk:</b> User accounts whose Primary Group IDs have been modified may have elevated privileges which are difficult to see and therefore easier to exploit within detection.</p> <p><b>Remediation:</b> To resolve vulnerability, in the account's Attribute Editor tab, select primaryGroupID and change the value to either 513 (Domain Users) or 514 (Domain Guest).</p>	Accounts in scope that have a "Primary Group" that is not <b>Domain Users</b> or <b>Domain Guests</b>
	<p><b>Name:</b> Computer accounts with non-default Primary Group IDs</p> <p><b>Default scope:</b> All computers</p>	<p><b>Risk:</b> Computer accounts whose Primary Group IDs have been modified may have elevated privileges which are difficult to see and therefore easier to exploit within detection.</p> <p><b>Remediation:</b></p> <ul style="list-style-type: none"> <li>The Primary Group ID should be reset to its default value. The default primary group for computer accounts is: <ul style="list-style-type: none"> <li>"Domain Computers" (515)</li> <li>for domain controller accounts, "Domain Controllers" (516)</li> <li>for read-only domain controllers, "Read-only Domain Controllers" (521).</li> </ul> </li> </ul>	Accounts in scope that have a "Primary Group" that is not <b>Domain Computers</b> or <b>Domain Controllers</b> or <b>Read-Only Domain Controllers</b>

Vulnerability Template	Vulnerability	Risk	What to find
Users Service Principal Name status	<p><b>Name:</b> Tier Zero user accounts with Service Principal Names</p> <p><b>Default scope:</b> Tier Zero users</p>	<p>Tier Zero user accounts with Service Principal Names (SPNs) defined are exposed to Kerberos-based authentication attacks, enabling an adversary to escalate their privileges within the directory.</p> <p><b>Remediation:</b> To resolve vulnerability, remove the Service Principal Name from the user object, if possible. If the Service Principal Name cannot be removed, enforce a very strong password on the user object which contains 32 characters with upper case, lower case, numeral, and special characters.</p>	User accounts in scope that have "Service Principal Name" <b>not empty</b>
Number of Tier Zero user accounts	<p><b>Name:</b> Abnormally large number of Tier Zero user accounts in the domain</p> <p><b>Default scope:</b> N/A</p>	<p>The number of Tier Zero accounts in a domain should be limited and closely monitored. An abnormally high number of Tier Zero accounts could indicate loose permissioning or group nesting which should be addressed. Tier Zero user accounts are being evaluated for this vulnerability.</p> <p><b>Remediation:</b> To resolve vulnerability, identify accounts that should not have Tier Zero user credentials and remove those credentials. Resolve any group nesting issues.</p>	Total number of Tier Zero user accounts within a domain is <b>more than 20</b>
Account SID History status	<p><b>Name:</b> Tier Zero user accounts with SID History populated</p> <p><b>Default scope:</b> Tier Zero users</p>	<p>If a user account's sidHistory attribute is populated, then the account has all the privileges that belong to the SID History as well. Tier Zero user accounts with SID History are particularly concerning as they may have more privilege than is visible and likely indicates an adversary has compromised the account and established a backdoor for persistence.</p> <p><b>Remediation:</b> To resolve vulnerability, remove the references in SID History if the user no longer requires the permissions assigned to the security groups listed. If the permissions are required, add the permission or group membership directly to the user object.</p>	Accounts in scope that have SID History <b>not empty</b>
	<p><b>Name:</b> Tier Zero groups with SID History populated</p> <p><b>Default scope:</b> Tier Zero groups</p>	<p>If a group's sidHistory attribute is populated, the group members have the privileges that belong to the SID History as well. Tier Zero groups with SID History are particularly concerning as they may have more privilege than is visible and likely indicates an adversary has compromised the account and established a backdoor for persistence.</p> <p><b>Remediation:</b></p>	

Vulnerability Template	Vulnerability	Risk	What to find
		To resolve vulnerability, remove the references in sidHistory if the group no longer requires the permissions assigned to the security groups listed. If the permissions are required, add the permission or group membership directly to the group object.	
Account SID History local SID status	<p><b>Name:</b> User accounts with SID from local domain in their SID History</p> <p><b>Default scope:</b> All users</p>	<p>If a user account's sidHistory attribute is populated, the account has all the privileges that belong to the SID History as well. While user accounts that were previously migrated may have a SID History from an external domain, the presence of a SID from the same domain is an indication an adversary has compromised the account and granted themselves more privilege than is immediately visible.</p> <p><b>Remediation:</b> To resolve vulnerability, immediately remove the local SID from the compromised user's sidHistory attribute and investigate who modified the attribute and when.</p>	Accounts in scope that <b>have</b> SID from local domain in their SID History
	<p><b>Name:</b> Groups with SID from local domain in their SID History</p> <p><b>Default scope:</b> All groups</p>	<p>If a group account's sidHistory attribute is populated, the group members have all the privileges that belong to the SID History as well. While group accounts that were previously migrated may have a SID History from an external domain, the presence of a SID History from the same domain is an indication an adversary has compromised the account and granted themselves more privilege than is immediately visible.</p> <p><b>Remediation:</b> To resolve vulnerability, immediately remove the local SID from the compromised group's sidHistory attribute and investigate who modified the attribute and when.</p>	
User account status	<p><b>Name:</b> Tier Zero user account is disabled</p> <p><b>Default scope:</b> Tier Zero users</p>	<p>The number of Tier Zero accounts in a domain should be limited and closely monitored. A Tier Zero account that is disabled but still contains privileges through Tier Zero group membership can be compromised by an adversary and used to elevate privileges.</p> <p><b>Remediation:</b> Remove Tier Zero group membership from user accounts that are disabled.</p>	Users in scope that are <b>disabled</b>
Group Members Count	<p><b>Name:</b></p>	Default Active Directory groups have elevated	Groups in scope

Vulnerability Template	Vulnerability	Risk	What to find
	<p>Default Active Directory groups which should not be in use contain members</p> <p><b>Default scope:</b></p> <ul style="list-style-type: none"> <li>Account Operators</li> <li>Backup Operators</li> <li>Cryptographic Operators</li> <li>Hyper-V Administrators</li> <li>Network Configuration Operators</li> <li>Print Operators</li> <li>Remote Desktop Users</li> <li>Replicator</li> <li>Server Operators</li> </ul>	<p>privileges and indirect control over vital aspects of Active Directory. These groups should typically have no members, so the presence of any memberships is a possible sign of an adversary using the group to elevate their privileges.</p> <p><b>Remediation:</b></p> <p>Remove the members within default Active Directory groups:</p> <ul style="list-style-type: none"> <li>• Account Operators (S-1-5-32-548)</li> <li>• Backup Operators (S-1-5-32-551)</li> <li>• Cryptographic Operators (S-1-5-32-569)</li> <li>• Hyper-V Administrators* (S-1-5-32-578)</li> <li>• Network Configuration Operators (S-1-5-32-556)</li> <li>• Print Operators (S-1-5-32-550)</li> <li>• Remote Desktop Users (S-1-5-32-555)</li> <li>• Replicator (S-1-5-32-552)</li> <li>• Server Operators (S-1-5-32-549)</li> </ul> <p>* NOTE: The Hyper-V Administrators group may have members If a Hyper-V environment is used.</p>	<p>that have more than <b>0</b> members</p> <p>NOTE: The operator and number of days are editable.</p>
Schema Admins Group Member Count	<p><b>Name:</b></p> <p>Schema Admins group contains members</p> <p><b>Default scope:</b></p> <p>N/A</p>	<p>Schema Admins group has elevated privileges and indirect control over vital aspects of Active Directory. This group should typically have no members, so the presence of any memberships is a possible sign of an adversary using the group to elevate their privileges.</p> <p><b>Remediation:</b></p> <p>Remove the members within Schema Admins.</p>	<p>Schema Admins group has <b>more than 0</b> members</p> <p>NOTE: The operator and number of days are editable.</p>
Non-members of protected groups	<p><b>Name:</b></p>	<p>Microsoft uses the adminCount attribute to indicate</p>	<p>User objects in scope that are not</p>

Vulnerability Template	Vulnerability	Risk	What to find
adminCount attribute value	<p>Ordinary user accounts with hidden privileges (SDProp)</p> <p><b>Default scope:</b> All users</p>	<p>an object has had its ACL modified by the system to be more secure as it was a member of one of the administrative groups. An adversary who has breached the directory may try to remain undetected by removing accounts they leveraged to escalate their privileges, and the admincount attribute is evidence of that cover-up. Protected groups include:</p> <ul style="list-style-type: none"> <li>Account Operators (S-1-5-32-548)</li> <li>Administrators (S-1-5-32-544)</li> <li>Backup Operators (S-1-5-32-551)</li> <li>Cert Publishers (S-1-5-21-&lt;domain&gt;-517)</li> <li>Domain Admins (S-1-5-21-&lt;domain&gt;-512 )</li> <li>Domain Controllers (S-1-5-21-&lt;domain&gt;-516 )</li> <li>Enterprise Admins (S-1-5-21-&lt;root_domain&gt;-519)</li> <li>Read-only Domain Controllers (only since Windows Server 2008) (S-1-5-21-&lt;domain&gt;-521)</li> <li>Replicator (S-1-5-32-552)</li> <li>Schema Admins (S-1-5-21-&lt;root_domain&gt;-518 )</li> <li>Server Operators (S-1-5-32-549)</li> </ul> <p><b>Remediation:</b> Investigate accounts that are not members of the protected groups whose adminCount attribute is set to 1 to determine if the user account was recently removed from a protected group and that action was expected. The adminCount attribute should then be manually set back to 0 in the Attribute Editor tab of the user object.</p>	members of protected groups and have adminCount attribute set to 1
Verify group membership of DnsAdmins group	<b>Name:</b> DnsAdmins	DNS is an appealing target for adversaries as it can be used to redirect domain queries or launch a	DnsAdmins group has more than <b>0</b> members

Vulnerability Template	Vulnerability	Risk	What to find
	group contains members <b>Default scope:</b> All users	denial of service. Members of the DnsAdmins group which are not highly Tier Zero Active Directory administrators are suspicious and increase the attack surface. <b>Remediation:</b> Review the members of the DnsAdmins group, determine if any members are not highly Tier Zero Active Directory administrators, and remove them if appropriate.	
Anonymous Logon and Everyone groups are members of Pre-Windows 2000 Compatible Access group	<b>Name:</b> Anonymous Logon and Everyone groups are members of the Pre-Windows 2000 Compatible Access group <b>Default scope:</b> N/A	The default permissions on many AD objects are set to allow access to the Pre-Windows 2000 Compatible Access group. If wide-open groups such as Everyone (S-1-1-0) or Anonymous Logon (S-1-5-7) are members of the Pre-Windows 2000 Compatible Access group, it creates exposure for an adversary to escalate their privileges. <b>Remediation:</b> Remove wide open groups Everyone (S-1-1-0) and Anonymous Logon (S-1-5-7) from the Pre-Windows 2000 Compatible Access group (S-1-5-32-554).	Pre-Windows 2000 Compatible Access group <b>contains</b> Anonymous Logon and Everyone groups
Tier Zero user account ownership	<b>Name:</b> Tier Zero users owned by non-Tier Zero accounts <b>Default scope:</b> N/A	The owner of an object can take control over the object and have all of its permissions. A non-Tier Zero user having ownership over a Tier Zero account can be evidence of tampering and represents an abusable attack path for an adversary. <b>Remediation:</b> Remove the non-Tier Zero user ownership on the Tier Zero user account and investigate who modified the owner and when.	Tier Zero user accounts that are owned by a <b>non-Tier Zero account</b>
Tier Zero computer account ownership	<b>Name:</b> Tier Zero computer is owned by a non-Tier Zero account <b>Default scope:</b> N/A	<b>Remediation:</b> Update the owner of the Domain Controller to the Domain Admins group or update other Tier Zero computers to Tier Zero owners.	Tier Zero computer accounts that are owned by a <b>non-Tier Zero account</b>

Vulnerability Template	Vulnerability	Risk	What to find
Account password last changed	<p><b>Name:</b> Tier Zero computer accounts that have not cycled their password recently</p> <p><b>Default scope:</b> Tier Zero computers</p>	<p>Tier Zero computers such as domain controllers will change their computer account password periodically (30 days by default). Domain controllers that have older password could be offline and susceptible to having password hashes stolen or used to introduce nefarious changes to the directory.</p> <p><b>Remediation:</b> The reason that prevents servers from changing their password should be investigated. Verify if the computer is offline. If online, check the values of the following registry entries:</p> <ul style="list-style-type: none"> <li>• HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange must be 0 or not exist</li> <li>• HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge should be 30</li> </ul> <p>If these values are incorrect, they should be reset to the default values and ensure that they are not set by a GPO.</p>	<p>Accounts in scope that have not updated their password within last <b>30 days</b>.</p> <p>NOTE: The number of days is editable.</p>
Group Policy "Recovery console: Allow automatic administrative logon" setting	<p><b>Name:</b> Tier Zero Group Policy allows Recovery mode to be not password-protected</p> <p><b>Default scope:</b> Tier Zero Group Policies</p>	<p>An unprotected Recovery Mode allows an adversary with physical access to a domain controller the ability to gain access to the Active Directory database.</p> <p><b>Remediation:</b> Configure the "Recovery console: Allow automatic administrative logon" setting located in "Computer Configuration - Policies - Windows Settings - Security Settings - Local Policies - Security Options" section of the Group Policy to "disabled"</p>	<p>Group Policy objects in scope "Recovery console: Allow automatic administrative logon" is <b>enabled</b></p>
Tier Zero computer Group Policy "Allow log on" settings	<p><b>Name:</b> Non-Tier Zero accounts are able to log onto Tier Zero computers</p>	<p>If a non-Tier Zero user is able to log onto a Tier Zero computer, such as a Domain Controller, locally or by remote session, they can execute code or obtain a copy of all password hashes.</p> <p><b>Remediation:</b> Prevent non-Tier Zero users from logging into Tier</p>	<p>Accounts in scope added to <b>Allow log on locally</b> or <b>Allow log on through Remote Desktop Services</b> in Tier Zero Group Policy</p>

Vulnerability Template	Vulnerability	Risk	What to find
	<b>Default scope:</b> All except Tier Zero users, groups and computers	Zero computers by removing the "Allow log on locally" and "Allow log on through Remote Desktop Services" rights for any non-Tier Zero group. These settings are located in Computer configuration - Policies - Windows Settings - Security Settings - Local Policies - User Rights Assignment.	
Non-Tier Zero account with write or extended permission on Tier Zero objects	<b>Name:</b> Non-Tier Zero account with write or extended permission on Tier Zero object	Tier Zero objects are the most critical assets within an organization's Active Directory. If an adversary can control any account that has elevated access on a Tier Zero object, they can control that object. No resources outside of Tier Zero should have control over anything inside Tier Zero. <b>Remediation:</b> Review non-Tier Zero accounts that have access to Tier Zero objects and determine if the access should be removed or if the non-Tier Zero account should be added to the Tier Zero object list.	Non-Tier Zero account with write or extended permission on <b>Tier Zero objects</b>
Non-Tier Zero computer "Deny log on" for Domain Admin status	<b>Name:</b> Group Policy does not prevent Domain Admins from logging onto non-Tier Zero computer <b>Default scope:</b> All except Tier Zero computers	When a Tier Zero account logs into a non-Tier Zero computer, their password hash remains in memory and can be harvested by an adversary. If Group Policies do not prevent Domain Admin logons to lower tiers, privileged credentials could be exposed. <b>Remediation:</b> Restrict logons to all non-Tier Zero computers for Domain Admins by configuring the "Deny log on locally" and "Deny logon through Remote Desktop Services" in the Group Policy. These settings are located in Computer Configuration - Policies - Windows Settings - Security Settings - Local Policies - User Rights Assignment.	Computer objects in scope that do not have assigned group policies with the Domain Admins group added to the <b>Deny log on locally</b> and <b>Deny log on through Remote Desktop Services</b> settings
DNS zone dynamic updates status	<b>Name:</b> DNS zone configuration allows anonymous record updates <b>Default scope:</b> N/A	Dynamic DNS records are created by DNS clients or systems on behalf of DNS clients (Example: DHCP servers). On Microsoft DNS servers, there are three possible configurations for dynamic updates: "None", "Nonsecure and secure", "Secure only". The "Nonsecure and secure" setting allows dynamic updates to be accepted without checking if the source of updates is trusted or not. DNS zones configured to allow anonymous record updates can be exploited by adversaries to receive incoming queries and harvest credentials. <b>Remediation:</b>	DNS zone dynamic updates set to <b>Nonsecure</b> and <b>secure</b>

Vulnerability Template	Vulnerability	Risk	What to find
	<p><b>i</b> <b>NOTE:</b> For vulnerabilities that use this template, the hybrid agent service account must be a member of the <b>Domain Admins</b> group.</p>	<p>If enabling dynamic updates is required for an organization, it is highly recommended to use “Secure only” dynamic updates option which ensures dynamic updates are accepted only from trusted sources. This option is available only if your primary DNS zone is hosted on a domain controller and is an AD-integrated DNS zone.</p>	
Computer Resource-Based Constrained Delegation status	<p><b>Name:</b> Tier Zero computer can be compromised through Resource-Based Constrained Delegation</p> <p><b>Default scope:</b> Tier Zero computers</p>	<p>If Kerberos Resource-Based Constrained Delegation (RBCD) is enabled on a Tier Zero computer such as a domain controller, an adversary can leverage this to elevate from a system under their control to a Tier Zero computer and take effective control over the entire domain.</p> <p><b>Remediation:</b> To resolve vulnerability, in the impacted computer’s Delegation tab, select “Do not trust this computer for delegation”.</p> <p>The following PowerShell command can be used to verify the account that has Resource-Based Constrained Delegation against the impacted computer account (Note: The “Identity” portion of the command will need to be updated to reflect the display name of the computer account being checked):</p> <pre>Get-ADComputer -Identity &lt;computer&gt; -Properties PrincipalsAllowedToDelegateToAccount</pre>	Computer accounts in scope that <b>have</b> Resource-Based Constrained Delegation configured
	<p><b>Name:</b> Non-Tier Zero computer can be compromised through Resource-Based Constrained Delegation</p> <p><b>Default</b></p>	<p>If Kerberos Resource-Based Constrained Delegation (RBCD) is enabled on a computer, an adversary can leverage this to elevate from a system under their control to another system it has delegation.</p> <p><b>Remediation:</b> To resolve vulnerability, in the impacted computer’s Delegation tab, select “Do not trust this computer for delegation”.</p> <p>The following PowerShell command can be used to verify the account that has Resource-Based</p>	

Vulnerability Template	Vulnerability	Risk	What to find
	<p><b>scope:</b> All except Tier Zero computers</p>	<p>Constrained Delegation against the impacted computer account (Note: The "Identity &lt;computer&gt;" portion of the command will need to be updated to reflect the display name of the computer account being checked):</p> <p>Get-ADComputer -Identity &lt;computer&gt; -Properties PrincipalsAllowedToDelegateToAccount</p>	
Domain Write Group Policy Object link delegation	<p><b>Name:</b> Non-Tier Zero accounts can link GPOs to the domain</p> <p><b>Default scope:</b> All except Tier Zero users and groups</p>	<p>Group Policies are an effective attack path as they can be used to weaken directory-wide security or deploy payloads. If an adversary gains the ability to link a Group Policy Object (GPO) at the domain level they can effectively take over the entire domain.</p> <p><b>Remediation:</b> These delegations should be removed for any non-Tier Zero account unless there is a compelling reason for their existence.</p>	Domain has the "Write gPLink" set to <b>Allow</b> for any accounts in scope
Domain promote a computer to a domain controller delegation	<p><b>Name:</b> Non-Tier Zero accounts that can promote a computer to a domain controller</p> <p><b>Default scope:</b> All except Tier Zero users and groups</p>	<p>The "Add/remove replica in domain" permission on the domain coupled with the SERVER_TRUST_ACCOUNT attribute in userAccountControl can allow an adversary to promote any computer they reach to a domain controller. This would allow them to move laterally across the directory and take advantage of DC-based attacks to harvest credentials.</p> <p><b>Remediation:</b> The "Add/remove replica in domain" delegation should be removed from any non-Tier Zero account unless there is a compelling reason for its existence.</p>	Domain has "Add/remove replica in domain" set to <b>Allow</b> for any account in scope
Active Directory Site Write gPLink delegation	<p><b>Name:</b> Non-Tier Zero accounts can link Group Policy Objects to an Active Directory site</p> <p><b>Default scope:</b> All except Tier</p>	<p>Group Policies are an effective attack path as they can be used to weaken directory-wide security or deploy payloads. If an adversary gains the ability to link a Group Policy Object (GPO) to an Active Directory site, they can directly control all objects it contains.</p> <p><b>Remediation:</b> These delegations should be removed unless there is a compelling reason for their existence.</p>	Active Directory Site has "Write gPLink" set to <b>Allow</b> for any accounts in scope

Vulnerability Template	Vulnerability	Risk	What to find
	Zero users and groups		
Domain Controller OU Write gPLink delegation	<p><b>Name:</b> Non-Tier Zero accounts can link Group Policy Objects to Domain Controller OU</p> <p><b>Default scope:</b> All except Tier Zero users and groups</p>	<p>Group Policies are an effective attack path as they can be used to weaken directory-wide security or deploy payloads. If an adversary gains the ability to link a Group Policy Object (GPO) to the Domain Controller OU they can directly control the domain controllers.</p> <p><b>Remediation:</b> These delegations should be removed unless there is a compelling reason for their existence.</p>	Domain Controllers OU has "Write gPLink" set to <b>Allow</b> for any accounts in scope
Computer account group membership status	<p><b>Name:</b> Tier Zero groups that have computer accounts as members</p> <p><b>Default scope:</b> Tier Zero groups</p>	<p>If a computer account is a member of a Tier Zero group, an adversary who compromises the computer will also elevate their privileges to the Tier Zero group the computer belongs to.</p> <p>Vulnerable objects will not be returned when any computer is a member of Cert Publishers or when a DC or RODC is a member of Domain Controllers, Enterprise Domain Controllers, Read-only Domain Controllers, or Enterprise Read-only Domain Controllers.</p> <p><b>Remediation:</b> Review computer account Tier Zero group membership to determine if the computer should be a member of the Tier Zero group. If not required, remove the account from the group.</p>	Groups in scope that <b>have</b> computer accounts as members
KRBTGT account resource-based constrained delegation status	<p><b>Name:</b> KRBTGT accounts with Resource-Based Constrained Delegation</p> <p><b>Default</b></p>	<p>Any delegations against the KRBTGT accounts are highly suspicious. If an adversary gains control over the KRBTGT account, they can use this to take control over the entire directory.</p> <p><b>Remediation:</b> To resolve vulnerability, in the KRBTGT account's Account tab, check "Account is sensitive and cannot be delegated." The following PowerShell command</p>	KRBTGT accounts that <b>have</b> Resource-Based Constrained Delegation configured

Vulnerability Template	Vulnerability	Risk	What to find
	<p><b>scope:</b> N/A</p>	<p>can be used to verify the account that has Resource-Based Constrained Delegation against the KRBTGT account (Note: The “Identity KRBTGT” portion of the command will need to be updated to reflect the name of the KRBTGT account being checked): Get-ADuser -Identity KRBTGT -Properties PrincipalsAllowedToDelegateToAccount</p>	
Domain trust configured insecure status	<p><b>Name:</b> Domain trust configured insecurely</p> <p><b>Default scope:</b> Dependent on the domain(s) selected when an Assessment is created. If a selected domain does not have a trust relationship, it will not be assessed for the vulnerability.</p>	<p>Trusts that have insecure settings are exposed to Kerberos-based authentication vulnerabilities or reduced protection against imposter identities.</p> <ul style="list-style-type: none"> <li>A domain trust is considered insecure if it has the trustAttribute TRUST_ATTRIBUTE_CROSS_ORGANIZATION_ENABLE_TGT_DELEGATION (0x00000800) bit enabled.</li> <li>A domain trust is considered insecure if it has the trustAttribute TRUST_ATTRIBUTE_PIM_TRUST (0x00000400) bit set.</li> </ul> <p><b>Remediation:</b></p> <ul style="list-style-type: none"> <li>Evaluate if EnableTgtDelegation is required and, if not, disable it on your domain trust.</li> <li>Evaluate if EnablePIMTrust is required and, if not, disable it on your domain PAM trust.</li> </ul>	<p>Domain trust in scope has <b>EnableTgtDelegation or EnablePIMTrust</b> configured in the trustAttribute</p>
Active Directory group existence in domain	<p><b>Name:</b> Suspicious ESX Admins group detected in domain</p> <p><b>Default scope:</b> ESX Admins</p>	<p>Microsoft has identified vulnerability CVE-2024-37085 where ESXi hypervisors can be exploited by several ransomware operators to obtain full administrative permissions on domain-joined ESXi hypervisors. A threat actor can create a group named “ESX Admins” in the domain and add users to it, which will grant full administrative access on the ESXi hypervisor. “ESX Admins” group is not a built-in group in Active Directory and does not exist by default. ESXi hypervisors do not validate that the group exists when the server is joined to a domain but considers any members of a group with this name as having full administrative access, even if the group did not originally exist. The membership in the group is determined by group name and not by security identifier (SID).</p> <p><b>Remediation</b></p>	<p>Active Directory group in scope is <b>detected</b></p>

Vulnerability Template	Vulnerability	Risk	What to find
Account ability to specify a certificate subjectAltName (SAN) in a certificate request	<p><b>Name:</b> Non-Tier Zero account can use a misconfigured certificate template to impersonate any user</p> <p><b>Default scope:</b> All except Tier Zero users and groups</p>	<p>Ensure the latest security updates released by VMware are installed on all domain-joined ESXi hypervisors. If installing software updates is not possible, perform the following to reduce the risk:</p> <p>Validate the group "ESX Admins" exists in the domain and is hardened.</p> <p>Manually deny access by this group by changing settings in the ESXi hypervisor. If full admin access for the Active Directory ESX admins group is not desired, disable this behavior using the advanced host setting: 'Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd'.</p> <p>Change the admin group to a different group in the ESXi hypervisor.</p> <p>Certificate template settings determine the characteristics for the derived certificates and the parameters required for a certificate request. A certificate template is considered "misconfigured" if the combination of settings defined can expose an organization to an attacker. A certificate template that meets the following criteria will allow a non-Tier Zero attacker to request a certificate that can be used to authenticate to the domain as a Tier Zero user: Subject Name set to "Supply in the request", "CA certificate manager approval" is not required, "Authorized signatures" is not required, Extended Key Usage (EKU) facilitates authentication, non-Tier Zero account can enroll (or can grant themselves permission to enroll) in a certificate.</p> <p><b>Remediation:</b></p> <p>Configure the certificate template Subject Name setting to "Build from this Active Directory information" and set the Issuance Requirements to require "CA certificate manager approval". In addition, ensure non-Tier Zero accounts do not have Enroll or Full Control permissions granted on the certificate template. It is also recommended that the certificates issued by the certificate authority be reviewed to confirm if the identified non-Tier zero account requested a certificate using the misconfigured certificate template and what Subject Name is used in the request.</p>	Accounts in scope <b>can</b> request a certificate that allows the subjectAltName (SAN) to be specified
Account ability to request an overly	<b>Name:</b>	Certificate template settings determine the	Accounts in scope <b>can</b> request a

Vulnerability Template	Vulnerability	Risk	What to find
permissive certificate with privileged EKU	<p>Non-Tier Zero account can request an overly permissive certificate with privileged EKU (ESC2)</p> <p><b>Default scope:</b> All except Tier Zero users and groups</p>	<p>characteristics for the derived certificates and the parameters required for a certificate request. A certificate template is considered “overly permissive” if the combination of settings defined can expose an organization to an attacker. A certificate template that has either no Extended Key Usage (EKU) defined or has the EKU “Any Purpose” is considered privileged.</p> <p><b>Remediation:</b> Ensure non-Tier Zero accounts do not have Enroll or Full Control permissions granted on the certificate template. It is also recommended to enforce extra security such as like adding Manager approval and signing requirements, if possible.</p>	certificate that has either no EKU defined or has the “Any Purpose” EKU
Account ability to create Delegated Managed Service Account	<p>Non-Tier Zero account can create Delegated Managed Service Accounts (dMSA) in an OU or container</p>	<p>Delegated Managed Service Account (dMSA) is a new Active Directory account type introduced in Windows Server 2025 that allows migration from a traditional service account to a machine account with managed and fully randomized keys, while disabling original service account passwords.</p> <p>An organization only requires a single Domain Controller on Microsoft Windows Server 2025 (not the functional domain level) in order to create a dMSA. Known as a "BadSuccessor" attack, a malicious user with the ability to create objects within an Organizational Unit (OU) or container can create a new dMSA and automatically have the ability to edit its attributes.</p> <p>The dMSA can then be configured to "migrate" a privileged account by manually setting the msDS-ManagedAccountPrecededByLink and msDS-DelegatedMsaState attributes.</p> <p>This will result in the dMSA being treated as a legitimate successor and have Kerberos tickets issued with the full rights of the privileged account. Windows environments that do not have a Windows 2025 Domain Controller are still considered vulnerable if there are non-Tier Zero accounts with permissions to create child objects in an OU or container (CVE-2021-42291).</p> <p><b>Remediation</b> One method to mitigate the "BadSuccessor" attack is to ensure only Tier Zero accounts can create Delegated Managed Service Accounts within an Organizational Unit (OU) or container.</p>	Accounts in scope <b>allowed</b> to create Delegated Managed Service Accounts in an OU or container

Vulnerability Template	Vulnerability	Risk	What to find
		<p>Review non-Tier Zero accounts granted the ability to create all child objects (permission: CreateChild, rights guid: 00000000-0000-0000-0000-000000000000), create msDS-DelegatedManagedServiceAccount objects (permission: CreateChild, rights guid: 0feb936f-47b3-49f2-9386-1dedc2c23765), or full control (permission: GenericAll, rights guid: 00000000-0000-0000-0000-000000000000) on a OU and container.</p> <p>Unless required, remove the permissions granted to the non-Tier Zero accounts.</p>	
Account migrated to Delegated Managed Service Account status	Tier Zero object migrated to a Delegated Managed Service Account (dMSA)	<p>Delegated Managed Service Account (dMSA) is a new Active Directory account type introduced in Windows Server 2025 that allows migration from a traditional service account to a machine account with managed and fully randomized keys, while disabling original service account passwords. Once an object is superseded by a dMSA, the dMSA account assumes all the privileges of that object.</p> <p><b>Remediation</b></p> <p>Review the Tier Zero object that the Delegated Managed Service Account (dMSA) is configured to supersede and confirm if the migration was intentional.</p>	Accounts in scope that are <b>superseded</b> by a Delegated Managed Service account (dMSA)
Delegated Managed Service accounts (dMSAs) with a suspicious configuration	Delegated Managed Service Account (dMSA) with a suspicious configuration (BadSuccess or)	<p>Known as a "BadSuccessor" attack, a malicious user can "migrate" a privileged account by manually setting the msDS-ManagedAccountPrecededByLink and msDS-DelegatedMsaState attributes on the dMSA. This will result in the dMSA being treated as a legitimate successor and have Kerberos tickets issued with the full rights of the privileged account. Typically, accounts that are legitimately migrated to a dMSA will have the msDS-SupersededManagedAccountLink populated with the distinguished name of the dMSA. If the msDS-SupersededManagedAccountLink does not have this value, it is likely dMSA was configured to supersede the privileged account by a user with limited permissions.</p> <p><b>Remediation</b></p> <p>Confirm if the dMSA should be superseding the privileged account. If not, remove the distinguished</p>	Delegated Managed Service accounts (dMSAs) in scope with a suspicious configuration to <b>supersede</b> a Tier Zero object

Vulnerability Template	Vulnerability	Risk	What to find
------------------------	---------------	------	--------------

name of the privileged account from the msDS-ManagedAccountPrecededByLink attribute of the dMSA.

## Discovery for Reconnaissance Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Active Directory Discovery for Reconnaissance.

**i** | **NOTE:** Reconnaissance techniques are used by adversaries to gain a thorough understanding and complete mapping of your environment for later use.

Vulnerability Template	Vulnerability	Risk	What to find
Domain Functional level	<p><b>Name:</b> Domain with obsolete domain functional level</p> <p><b>Default scope:</b> N/A</p>	<p>Active Directory domains configured for a legacy functional level (Windows Server 2012 or earlier) lack the most recent security feature to secure the environment.</p> <p><b>Remediation:</b> Raise the functional level of a domain to upgrade the features that are available within the domain. The domain controller is required to run on the Windows Server version that is compatible with the functional level. Note: If you have multiple domain controllers, make sure the oldest Windows Server version used is compatible with the functional level.</p>	Domain functional level <b>Windows Server 2012</b> or earlier

## Pre-Defined Entra ID Discoveries

Identity Defense comes with the following pre-defined Discoveries for Entra ID vulnerabilities.

**i** | **NOTE:** "System" displays in the Created By field of the Discoveries list when a Discovery type is pre-defined.

Discovery Type	Description
<a href="#">Entra ID Credential Access</a>	Techniques deployed by adversaries on systems and networks to steal usernames and credentials for re-use.
<a href="#">Entra ID Discovery</a>	Techniques used by adversaries to obtain information about systems and networks that they are looking to exploit or use for their tactical advantage.
<a href="#">Entra ID Initial Access</a>	Techniques used by adversaries to obtain a foothold within a network, such as targeted spear-phishing, exploiting vulnerabilities or configuration weaknesses in public-facing systems.
<a href="#">Entra ID Persistence</a>	Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
<a href="#">Entra ID Privilege Escalation</a>	Techniques used by adversaries to gain higher-level privileges on a system, such as local administrator or root.

## Entra ID Vulnerabilities that Require a Premium License

The following Entra ID vulnerabilities require a Premium License. If the organization has a free license, Assessment results for these Discoveries will return as **Inconclusive**.

- Entra ID guest user accounts that are inactive
- Entra ID Privileged accounts that are not secured by multi-factor authentication (MFA)

## Discovery for Entra ID Credential Access Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Entra Discovery for Credential Access.

**i** | **NOTE:** Credential Access techniques are deployed by adversaries on systems and networks to steal usernames and credentials for re-use.

Vulnerability Template	Vulnerability	Risk	What to find
Entra ID tenant on-premises Password hash synchronization	<p><b>Name:</b> Password hash synchronization with on-premises Active Directory is not enabled</p> <p><b>Default scope:</b> N/A</p> <p>NOTE: If no Active Directory collection is available, an Inconclusive message is returned.</p>	<p>Microsoft Entra Connect synchronizes a hash of the user's passwords from on-premises Active Directory to Entra ID. Password hash sync enables users to sign in to a service by using the same password that is used to sign in to the on-premises Active Directory instance. Password hash sync allows Identity Protection to detect compromised credentials by comparing password hashes with passwords known to be compromised.</p> <p><b>Remediation:</b> In Microsoft Entra Connect, the Password Hash Synchronization setting can be enabled on the User Sign-in page.</p>	Entra ID tenants in scope that have on-premises Active Directory Password hash synchronization <b>disabled</b>
Entra ID user account multi-factor authentication status	<p><b>Name:</b> Entra ID Privileged accounts that are not secured by multi-factor authentication (MFA)</p> <p><b>Default scope:</b> All Privileged users</p>	<p>Accounts that are assigned administrative rights are targeted by attackers. Requiring multi-factor authentication (MFA) on those accounts is an easy way to reduce the risk of those accounts being compromised.</p> <p><b>Remediation:</b> Administrator accounts identified may be a member of a Privileged or non-Privileged administrator</p>	Entra ID user accounts in scope that have multi-factor authentication <b>not registered</b>

Vulnerability Template	Vulnerability	Risk	What to find
		<p>role. Investigate each administrator to determine why they are not using multi-factor authentication (MFA). If a large number of administrators are not using MFA, MFA may need to be enforced using Security Defaults or Conditional Access policies.</p>	
Entra ID tenant administrator SSPR status	<p><b>Name:</b> Administrators are not enabled for self service password recovery</p> <p><b>Default scope:</b> Entra ID tenant(s)</p>	<p>By default, administrator accounts are enabled for self-service password reset (SSPR), and a strong default two-gate password reset policy is enforced.</p> <p><b>Remediation:</b> SSPR for administrator accounts can be re-enabled using the Update-MgPolicyAuthorizationPolicy PowerShell cmdlet. The -AllowedToUseSspr:\$true \$false parameter enables SSPR for administrators. Policy changes to enable or disable SSPR for administrator accounts can take up to 60 minutes to take effect.</p>	Entra ID tenants in scope that have an administrator service password reset (SSPR) <b>disabled</b>
Entra ID Conditional Access policy "Exchange ActiveSync clients" and "Other clients" access control	<p><b>Name:</b> Entra ID Conditional Access policies do not block legacy authentication for all users</p> <p><b>Default scope:</b> All users</p>	<p>Applications using legacy methods to authenticate with Microsoft Entra ID and access organization data are not considered secure. Protocols such as POP3, IMAP4, and SMTP have been replaced by modern authentication, which uses Multifactor Authentication (MFA).</p> <p><b>Remediation:</b> Organizations with Microsoft Entra ID P1 or P2 licenses should use Conditional Access policies to block legacy authentication. Organizations with Microsoft Entra ID Free tier should enable Microsoft Entra Security Defaults to block legacy authentication.</p> <p>NOTE: Microsoft recommends excluding the following accounts</p>	Entra ID user accounts in scope that do not have the client apps "Exchange ActiveSync clients" and "Other clients" access control set to <b>block</b> in an assigned Conditional Access policy

Vulnerability Template	Vulnerability	Risk	What to find
------------------------	---------------	------	--------------

from Conditional Access policies:

- Emergency access or break-glass accounts (to prevent tenant-wide account lockout),
- Service accounts and service principals (non-interactive accounts normally used by back-end services which cannot programmatically complete MFA).

Entra ID Conditional Access policy sign-in risk

**Name:**  
Entra ID Conditional Access policies do not protect all users from risky sign-ins  
**Default scope:**  
All users

A risky sign-in represents the probability that an authentication request is not authorized by the identity owner. Based on the risk level high, medium and low, a policy can be configured to block access or force multifactor authentication. Microsoft recommends that multifactor authentication is forced on Medium or above risky sign-ins.

**Remediation:**

Requires a Microsoft Entra ID P2 license.  
Enable a Conditional Access policy for the tenant that has "Users" set to include "All users" and exclude emergency access or break-glass accounts.

- In "Target resources", "Cloud apps" set to include "All cloud apps".
- In "Access controls" "Grant", set "Grant access" to "Require multi-factor authentication".
- In "Session", set "Sign-in frequency" to "Every time".

Entra ID user accounts in scope that do not have sign-in risk levels set to **high, medium** in an assigned Conditional Access policy

Vulnerability Template	Vulnerability	Risk	What to find
Entra ID Conditional Access user risk policy	<p><b>Name:</b> Entra ID Conditional Access polices do not protect all users from high user risk</p> <p><b>Default scope:</b> All users</p>	<ul style="list-style-type: none"> <li>• In Conditions, select “Sign-in risk”, set “Configure” to Yes.</li> <li>• Under “Select the sign-in risk level this policy will apply to”, select “High” and “Medium” options.</li> </ul> <p>NOTE: Microsoft recommends excluding the following accounts from Conditional Access policies:</p> <ul style="list-style-type: none"> <li>• Emergency access or break-glass accounts (to prevent tenant-wide account lockout).</li> <li>• Service accounts and service principals (non-interactive accounts normally used by back-end services which cannot programmatically complete MFA).</li> </ul> <p>User risk indicates the likelihood a user's identity has been compromised and is calculated based on the user risk detections that are associated with a user's identity. Based on a risk-level of high, medium, low a policy can be configured to block access or require a secure password change using multifactor authentication. Microsoft's recommendation is to require a secure password change for users with high risk.</p> <p><b>Remediation:</b> Requires a Microsoft Entra ID P2 license. Enable a Conditional Access policy for the tenant that has “Users” set to include “All users” and exclude emergency access or break-glass accounts. In “Target resources”, “Cloud apps” set to include “All cloud</p>	Entra ID user accounts in scope that do not have user risk levels set to <b>high</b> in an assigned Conditional Access policy

Vulnerability Template	Vulnerability	Risk	What to find
------------------------	---------------	------	--------------

apps”.

In “Access controls” “Grant”, set “Grant access” to “Require multifactor authentication” and “Require password change”.

In "Session", set "Sign-in frequency" to “Every time”.

In Conditions, select “User risk”, set “Configure” to Yes.

Under “Configure user risk levels needed for policy to be enforced”, select the “High” option.

NOTE: Microsoft recommends excluding the following accounts from Conditional Access policies:

- Emergency access or break-glass accounts (to prevent tenant-wide account lockout),
- Service accounts and service principals (non-interactive accounts normally used by back-end services which cannot programmatically complete MFA).

Entra ID Conditional Access policy mfa status

**i** **NOTE:** For vulnerabilities that use this template, a [premium license](#) is required.

**Name:**  
Entra ID Conditional Access policies do not protect all privileged users with multi-factor authentication (MFA)

**Default scope:**  
Privileged users

Administrators have increased access to the environment. Due to the power accounts with privileged roles have, they should be treated with special care. One common method to improve the protection of privileged accounts is to require a stronger form of account verification for sign-in, like requiring multifactor authentication.

**Remediation:**  
Improve protection by requiring multi-factor authentication (MFA) for the listed directory roles. The conditional access policy is not required if a conditional access policy that requires MFA has been created for all users.

Entra ID user accounts in scope that do not have require multi-factor authentication **enabled** in an assigned Conditional Access policy

Vulnerability Template	Vulnerability	Risk	What to find
Entra ID Conditional Access token protection	<b>Name:</b> Entra ID Conditional	Token protection attempts to reduce attacks using token theft by	Entra ID user accounts in scope that do not have token protection

Enable a Conditional Access policy for the tenant that has “Users or workload identities” set to include the directory roles:

- Global Administrator
- Application Administrator
- Authentication Administrator
- Billing Administrator
- Cloud Application Administrator
- Conditional Access Administrator
- Exchange Administrator
- Helpdesk Administrator
- Password Administrator
- Privileged Authentication Administrator
- Privileged Role Administrator
- Security Administrator
- SharePoint Administrator
- User Administrator

“Target resources” set to "All cloud apps",

“Access controls” set to “Grant access, Require multi-factor authentication”

Organizations with Security Defaults enabled will enforce MFA for privileged roles without requiring a Conditional Access policy.

Vulnerability Template	Vulnerability	Risk	What to find
	<p>Access policies do not require token protection for sign-in sessions for users</p> <p><b>Default scope:</b> All users</p>	<p>ensuring a token is usable only from the intended device. When a token is stolen, by hijacking or replay, it can be used to impersonate the victim until the token expires or is revoked. Token theft is considered a relatively rare event but can inflict significant damage.</p> <p>Token protection creates a cryptographically secure tie between the token and the device (client secret) it is issued to. Without the client secret, the bound token is useless.</p> <p>When a user registers a Windows 10 or newer device in Microsoft Entra ID, their primary identity is bound to the device.</p> <p><b>Remediation:</b> Requires a Microsoft Entra ID P2 license.</p> <p>Token protection is only supported with some Windows devices and a limited set of applications. Review the requirements and known limitations to confirm if token protection is appropriate for users in the organization.</p> <p><a href="https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-token-protection">https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-token-protection</a></p> <p>The setting to require token protection is located in "Session", "Require token protection for sign-in sessions".</p>	<p>for sign-in sessions <b>enabled</b> in an assigned Conditional Access policy</p>

## Discovery for Entra ID Discovery Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Entra Discovery for Discovery.

**i** **NOTE:** Discovery techniques are used by adversaries to avoid detection. Evasion techniques include hiding malicious code within trusted processes and folders, encrypting or obfuscating adversary code, or disabling security software.

Vulnerability Template	Vulnerability	Risk	What to find
User password last changed	<p><b>Name:</b> Entra ID privileged role members whose passwords have not changed recently</p> <p><b>Default Scope:</b> All Users</p>	<p>While it is not necessary to require mandatory periodic password resets, organizations should be aware of the password age of users that are members of Microsoft Entra built-in privileged roles.</p> <p><b>Remediation:</b> Ensure that privileged role members have update their password to satisfy the organization's password policy.</p>	<p>Users that are members of privileged roles that have not updated their password within last <b>90</b> days</p> <p>NOTE: The number of days is editable.</p>

## Discovery for Entra ID Initial Access Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Entra Discovery for Initial Access.

**i** | **NOTE:** Initial Access techniques are used by adversaries to obtain a foothold within a network, such as targeted spear-phishing, exploiting vulnerabilities or configuration weaknesses in public-facing systems.

Vulnerability Template	Vulnerability	Risk	What to find
Entra ID service principal Microsoft Services Agreement status	<p><b>Name</b> Entra ID service principals that violate Microsoft Services Agreement</p> <p><b>Scope</b> Static object type: service principal</p>	<p>Registered applications can be disabled by Microsoft due to suspicious, abusive, or malicious activity or due to a violation of Microsoft Services Agreement. Service Principals generated from those registered applications are flagged as being malicious and disabled by Microsoft.</p> <p><b>Remediation</b> Service Principals marked as malicious should be deleted from the Entra ID tenant. Recent activity performed by those Service Principals should be reviewed in Audit.</p>	Entra ID service principals in scope that <b>violate</b> Microsoft Services Agreement
Entra ID tenant security defaults status	<p><b>Name:</b> Security defaults are enabled</p> <p><b>Default scope:</b> N/A</p>	<p>Enabling security defaults is recommended for organizations that are using the free tier of Microsoft Entra ID licensing and want to increase their security posture. Organizations with premium Entra ID licensing should use</p>	Entra ID tenants in scope that have security defaults <b>enabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
		<p>Conditional Access polices for more granular control to achieve a higher security posture.</p> <p><b>Remediation</b></p> <p>If the organization is using the free tier of Microsoft Entra ID licensing, continue using security defaults. If the organization is using Microsoft Entra ID P1 or P2 licenses, continue using security defaults while the deployment of Conditional Access policies is planned. When security defaults are disabled, organizations should immediately enable Conditional Access policies to protect the organization. These policies should include at least those policies in the secure foundations category of Conditional Access templates. Organizations with Microsoft Entra ID P2 licenses that include Microsoft Entra ID Protection can expand on this list to include user and sign in risk-based policies to further strengthen the posture.</p>	
<p>Entra ID Guest account last used</p> <p><b>i</b> <b>NOTE:</b> For vulnerabilities that use this template, a <a href="#">premium license</a> is required</p>	<p><b>Name:</b> Entra ID guest user accounts that are inactive</p> <p><b>Default scope:</b> All users</p>	<p>When external partners no longer access your tenant, the guest accounts may become stale and vulnerable to attack.</p> <p><b>Remediation:</b> Review inactive guest users, block them from signing in, and delete them from the directory.</p>	<p>Entra ID user accounts in scope that were last used <b>more than 90 days</b> ago</p> <p><b>NOTE:</b> The number of days is editable.</p>
<p>Entra ID Microsoft Authenticator number matching and additional contexts status</p>	<p><b>Name:</b> Entra ID Microsoft Authenticator policy does not require geographic location</p>	<p>Microsoft has added features for strong multifactor authentication (MFA to help reduce MFA fatigue attacks and accidental MFA</p>	<p>Entra ID user accounts in scope that do not have the Microsoft</p>

Vulnerability Template	Vulnerability	Risk	What to find
	<p>and application name contexts for all users</p> <p><b>Default scope:</b> All users</p>	<p>approvals.</p> <p><b>Remediation:</b> In Authentication methods, enforce the use of Microsoft Authenticator passwordless push notifications with show geographic location context and show application name context.</p>	<p>Authenticator policy assigned with geographic location and application name <b>enabled</b></p>
Entra ID user account last used	Enabled privileged Entra ID user accounts that are inactive	<p>Inactive privileged Entra ID accounts pose an elevated risk. These accounts have elevated roles and are less frequently monitored and used. Attackers may try to exploit these accounts to gain access to and potentially compromise the organization.</p> <p><b>Remediation</b> Review the inactive accounts to determine if they are required or if they should be disabled.</p>	<p>Entra ID user accounts in scope that were last used <b>more than 90</b> days ago</p>
Entra ID user account last used	Enabled non-privileged Entra ID user accounts that are inactive	<p>Inactive Entra ID accounts can be targeted by attackers to gain unauthorized access to the organization.</p> <p><b>Remediation</b> Review the inactive accounts to determine if they are required or if they should be disabled.</p>	<p>Entra ID user accounts in scope that were last used <b>more than 90</b> days ago</p>
Entra ID users synchronized from Active Directory status	<p>Synchronized Active Directory user is assigned an Entra ID privileged role</p> <p><b>Default scope:</b> All users</p> <p>NOTE: If no Active Directory collection is available, an Inconclusive message is returned.</p>	<p>Active Directory is considered less secure than Entra ID. By assigning an Entra ID Privileged role to a synchronized on-premises Active Directory user, attackers have a clear pathway to take over Entra ID if Active Directory is compromised.</p> <p><b>Remediation:</b> Microsoft recommends using</p>	<p>Entra ID users in scope that <b>are</b> synchronized Active Directory users</p>

Vulnerability Template	Vulnerability	Risk	What to find
Entra ID User consent for applications setting	<p><b>Name:</b> Entra ID users are allowed to consent for all applications</p> <p><b>Default scope:</b> All tenants selected at the time an Assessment is created</p>	<p>cloud-only accounts for Microsoft Entra ID privileged roles.</p> <p>Remove synchronized Active Directory user accounts from direct and indirect membership of privileged roles. Active Directory users that require privileged access to Entra ID should be provided with a separate cloud-only Entra ID account.</p> <p>Before an application can access an organization's data, a user must grant the application permissions. Different permissions allow different levels of access. By default, all users are allowed to consent to applications for permissions that don't require administrator consent. To reduce the risk of malicious applications being granted access to the organization's data by users, it is recommended that users can only consent to applications that have been published by a verified publisher.</p> <p><b>Remediation:</b> Sign in to the Microsoft Entra admin center as a Global Administrator. Browse to Identity   Applications   Enterprise applications   Consent and permissions   User consent settings. Under User consent for applications, select "Allow user consent for apps from verified publishers, for selected permissions". Alternatively, if appropriate, "Do not allow user consent" can be selected.</p>	Entra ID tenants in scope that have "User consent for applications" set to <b>allow user consent for apps</b>

Vulnerability Template	Vulnerability	Risk	What to find
Entra ID Conditional Access Continuous Access Evaluation strictly enforce location	<p><b>Name:</b> Entra ID Conditional Access policies do not protect all users with strictly enforce location for Continuous Access Evaluation</p> <p><b>Default scope:</b> All users</p>	<p>Strictly enforce location is an enforcement mode for Continuous Access Evaluation that is configured in Conditional Access policies. This mode provides protection by immediately stopping access if the IP address detected by the resource provider isn't allowed by Conditional Access policy. This option is the highest security setting for Continuous Access Evaluation.</p> <p><b>Remediation:</b> Implementing strictly enforce location for Continuous Access Evaluation requires that administrators understand the routing of authentication and access requests in their network environment. Policies like this one should be tested with a subset of users and applied cautiously. The setting to strictly enforce location for Continuous Access Evaluation is located in "Session", "Customize continuous access evaluation", "Strictly enforce location policies".</p>	<p>Entra ID user accounts in scope that do not have Continuous Access Evaluation strictly enforce location <b>enabled</b> in an assigned Conditional Access policy</p>
Entra ID Conditional Access policy mfa status	<p><b>Name:</b> Entra ID Conditional Access policies do not protect all non-privileged users with multi-factor authentication (MFA)</p> <p><b>Default scope:</b> All except Privileged users</p>	<p>Attackers frequently target end users. After attackers gain entry, additional access to privileged information can be requested for the exposed account. Attackers can also download other data such as the entire directory to do a phishing attack on the organization.</p> <p><b>Remediation:</b> Improve protection by requiring multi-factor authentication (MFA) for all users. Enable a Conditional Access policy for the tenant</p>	<p>Entra ID user accounts in scope that do not have require multi-factor authentication <b>enabled</b> in an assigned Conditional Access policy</p>

Vulnerability Template	Vulnerability	Risk	What to find
Entra ID tenant on-premises synchronization time	<p><b>Name:</b> Synchronization with on-premises Active Directory is delayed</p> <p><b>Scope:</b> All tenants selected at the time an Assessment is created</p> <p><b>NOTE:</b> If no Active Directory collection is available, an</p>	<p>that has:</p> <p>“Users” set to include “All users” and exclude emergency access or break-glass accounts.</p> <p>In “Target resources”, “Cloud apps” set to include “All cloud apps”.</p> <p>In “Access controls” “Grant”, set “Grant access” to “Require multifactor authentication”</p> <p>Organizations with Security Defaults enabled will enforce MFA for all users in some situations (based on factors such as location, device, role, and task) without requiring a Conditional Access policy.</p> <p><b>NOTE:</b> Microsoft recommends excluding the following accounts from Conditional Access policies:</p> <ul style="list-style-type: none"> <li>• Emergency access or break-glass accounts (to prevent tenant-wide account lockout)</li> <li>• Service accounts and service principals (non-interactive accounts normally used by back-end services which cannot programmatically complete MFA).</li> </ul>	<p>Entra ID tenants in scope that have not synchronized with on-premises Active Directory in <b>12</b> hours.</p>

Vulnerability Template	Vulnerability	Risk	What to find
	Inconclusive message is returned.		

## Discovery for Entra ID Persistence Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Entra Discovery for Persistence.

**i** **NOTE:** Persistence techniques are used by adversaries to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

Vulnerability Template	Vulnerability	Risk	What to find
Entra ID Conditional Access cloud application inclusion status	<p><b>Name:</b> Entra ID cloud applications that are not included in a conditional access policy</p> <p><b>Default scope:</b> All Applications</p>	<p>Conditional Access policies allow administrators to assign controls to specific applications. Administrators can choose from the list of applications or services that include built-in Microsoft applications and any Microsoft Entra integrated applications. Ensure at least one conditional access policy applies to each Cloud application in the organization.</p> <p><b>Remediation:</b> Enable a Conditional Access policy for the tenant that has "Target resources" set to include any cloud application that are not currently included in a Conditional Access policy.</p>	Entra ID Cloud applications in scope that are <b>not included</b> in a conditional access policy

## Discovery for Entra ID Privilege Escalation Vulnerabilities

The following table describes the vulnerabilities identified in the pre-defined Entra ID Discovery for Privilege Escalation.

**i** **NOTE:** Privilege Escalation techniques are used by adversaries to gain higher-level privileges on a system, such as local administrator or root.

Vulnerability Template	Vulnerability	Risk	What to find
Number of Global Administrators	<b>Name:</b>	Users who are assigned the Global	Total number of Global

Vulnerability Template	Vulnerability	Risk	What to find
	<p>More than recommended number of Global Administrators in the organization</p> <p><b>Default scope:</b> N/A</p>	<p>Administrator role can read and modify almost every administrative setting in your Microsoft Entra organization. Microsoft recommends that you assign the Global Administrator role to fewer than five people in your organization.</p> <p><b>Remediation:</b> Review the users assigned the Global Administrator role, determine the access required, and assign a more appropriate privileged role to the user.</p>	<p>Administrators in the organization is more than or equal to <b>5</b></p> <p>NOTE: The number of Global Administrators is editable.</p>
Entra ID Role with Guest members	<p><b>Name:</b> Guest accounts assigned to the Global Administrator role</p> <p><b>Default scope:</b> N/A</p>	<p>Cyber-attackers use credential theft attacks to target administrator accounts and other privileged access to try to gain access to sensitive data.</p> <p><b>Remediation:</b> Remove Guest accounts from the Global Administrator role. If the Guest account is the initial Microsoft account used when the Entra ID was first setup, replace the Microsoft account with an individual cloud-based or synchronized account.</p>	<p>Roles in scope that have more than <b>0</b> Guest accounts as members</p> <p>NOTE: The number of Guest accounts is editable.</p>
Number of privileged role assignments	<p><b>Name:</b> More than recommended number of privileged role assignments</p> <p><b>Default Scope:</b> N/A</p>	<p>Some roles include privileged permissions, such as the ability to update credentials. Since these roles can potentially lead to elevation of privilege, the use of these privileged role assignments should be limited to fewer than 10 in the organization.</p> <p><b>Remediation:</b> Review the privileged role assignments and reduce the number of assignments by removing access to principals that do not require it. If all principals require the access, use role-assignable groups to manage the access to privileged roles.</p>	<p>Total number of privileged role assignments in the organization is more than or equal to <b>10</b></p> <p>NOTE: The number of privileged role assignments is editable.</p>
Entra ID Conditional Access	<p><b>Name:</b> Entra ID</p>	<p>Continuous access evaluation is auto enabled as part of the organization's</p>	<p>Entra ID user accounts in scope that are assigned a Conditional Access policy with Continuous</p>

Vulnerability Template	Vulnerability	Risk	What to find
Continuous Access Evaluation disabled status	Conditional Access policy configured to disable Continuous Access Evaluation for users <b>Default scope:</b> All users	Conditional Access policies. The key benefits of continuous access evaluation are: <ul style="list-style-type: none"> <li>• user termination or password change/reset</li> <li>• user session revocation is enforced in near real time, network location change</li> <li>• Conditional Access location policies are enforced in near real time, and token export to a machine outside of a trusted network can be prevented with Conditional Access location policies.</li> </ul> <b>Remediation:</b> Any Conditional Access policy that has disabled continuous access evaluation should be reviewed to ensure there is a legitimate reason it was created. The setting to disable Continuous Access Evaluation is located in "Session", "Customize continuous access evaluation", "Disable".	Access Evaluation set to <b>disabled</b>

## Creating a Discovery

You can create custom Discoveries based on pre-defined vulnerability templates.

**i** **NOTE:** All of the available vulnerability templates are used in pre-defined Discoveries. You can refer to the Pre-defined Discoveries and Vulnerabilities for [Active Directory](#) and [Entra ID](#) sections for guidance when creating a new Discovery.

### To create a Discovery:

1. From the [Discoveries list](#), click **Create**.
2. Select a **Workload** (Active Directory or Entra ID).
3. Enter a **Discovery Type**.
4. Click **Select Vulnerabilities** to display a list of available vulnerability templates for the workload.
5. Select each vulnerability template you want to add to the Discovery, then click **Select**.

6. **For each vulnerability added to the Discovery:**

- a. Enter a **Vulnerability Name**.
- b. For **Risk**, enter the reason why the vulnerability is considered a risk. For **Remediation**, enter the recommendation for resolving the vulnerability.

**i** **TIP:** You can refer to Pre-defined Discoveries and Vulnerabilities for [Active Directory](#) and [Entra ID](#) for examples of Risk and Remediation text.

7. If the vulnerability includes a Scope, specify the objects that you want the Assessment to evaluate. Use the information in the following table for guidance.

**i** **NOTES:**

- If the Tier Zero or Privileged objects checkbox is selected, all applicable Tier Zero or Privileged objects, both those collected from the provider (Identity Defense or BloodHound Enterprise) and any that were manually-created, will be included in/excluded from the scope (depending on which option you select).
- If a vulnerability pertains to a specific object or set of objects, the Scope section will be hidden. For example, if the vulnerability pertains to users, only Tier Zero users will be included. If the vulnerability pertains to a specific AD group, such as Built-In administrators, only that group will be included.

Scope selection	Description
All {objects}	All objects in the workload that are the applicable object type, including both Tier Zero/Privileged and non-Tier Zero/Non-Privileged objects.
Select {objects}	Only the objects you specify based on your selection criteria will be included. When finished, click <b>Add Object</b> to add the object (s) to the Selected {Object}s list. If you want to exclude individual objects within your selection (for example, you selected an AD group but want to exclude individual members from the scope), click <b>Add Exceptions</b> and enter the object(s) as you would if you were adding objects.
All Except Selected {objects}	Only the objects you specify based on your selection criteria will be excluded from the scope. You can add multiple objects, separated by semicolons. When finished, click <b>Add Object</b> to add the object (s) to the Selected {Object}s list.

8. Click **Save**.

## Viewing, Editing, and Deleting a Discovery

From the [Discoveries list](#), you can view the details of a Discovery. You can also edit or delete a user-created Discovery. You can also change the scope of a pre-defined Discovery (if applicable) and, in a few cases, the What to find value. (Refer to the Pre-defined Discoveries and Vulnerabilities for [Active Directory](#) and [Entra ID](#) sections for specific Vulnerability templates.)

**i** **NOTE:** You cannot delete pre-defined Discoveries and the option will be disabled.

**To view a Discovery:**

- Click the Discovery Type link.

**To edit a Discovery:**

1. Either:
  - In the Discoveries list, select the Discovery that you want to edit.  
OR
  - Open the Discovery that you want to edit.
2. Click **Edit**.
3. Update the Discovery as needed.
4. Click **Save**.

**To delete a user-created Discovery:**

**i** | **NOTE:** Currently, you can only delete one Discovery at a time.

1. Either:
  - In the Discoveries list, select the Discovery that you want to delete.  
OR
  - Open the Discovery that you want to delete.
2. Click **Delete**.

You will be prompted to confirm the deletion.

# Hybrid Audit

Hybrid Audit in Quest Security Management Platform allows you to monitor and analyze activity across both your on-premises and cloud-based Microsoft environments from a single, unified interface. To accomplish this, Hybrid Audit agents are installed in your Active Directory domain to monitor and record activity. You can then search and view the recorded events through Audit.

Hybrid Audit requires the following components:

- A deployed Hybrid agent that has been configured as a broker that connects with your on-premises Active Directory domains. See [Working with Hybrid Audit Brokers](#) for more details.
- Installed Hybrid Audit agent on Domain Controllers and member servers in the appropriate Active Directory domain to record events for actions performed on those computers. See [Hybrid Audit Agent Deployment](#) for details on installing an agent.
- Enabled events within Identity Defense so they can then be searched and viewed with Security Management Platform's Audit functionality. Refer to [Working with Audited Events](#) for more details.

For more details on installing and using a Hybrid Audit agent with Identity Defense, see:

- [Overview of the Hybrid Audit Workflow](#)
- [Hybrid Audit Installation Notes](#)
- [Working with Protection Templates](#)

## Overview of the Hybrid Audit Workflow

To set up Hybrid Audit for Active Directory in your organization, follow these steps:

- **Step 1: Add a Domain**
  - Navigate to **Tenants | Active Directory Domains** and add a new domain.
- **Step 2: Add Hybrid Agent**
  - Go to **Tenants | Hybrid Agents** and add a hybrid agent.
- **Step 3: Install Hybrid Agent**
  - Install the hybrid agent in the same Active Directory forest as the domain created in Step 1.
- **Step 4: Configure Hybrid Agent**
  - Navigate to **Tenants | Hybrid Agents** and click **Edit configuration** on the newly installed agent.
  - Under **Actions**, click **Select Actions** and add **Manage Identity Defense Hybrid Audit**.
  - Under **Connected Domains**, click **Select Existing** and add the domain from Step 1.
  - Click **Save**.

- **Step 5: Verify Broker Connection**
  - Navigate to **Defend | Hybrid Audit | Brokers**.
  - Wait a few minutes for the Hybrid Audit Broker to display and confirm it is connected.
- **Step 6: Wait for Topology Discovery**
  - Navigate to **Defend | Hybrid Audit | Agent Deployment**.
  - Wait for the topology to auto-complete and populate the list of non-workstation computers.
- **Step 7: Install Hybrid Audit Agents**
  - In **Defend | Hybrid Audit | Agent Deployment**, deploy Hybrid Audit agents to all Domain Controllers and Global Catalog Servers to audit:
    - Active Directory
    - Group Policy events
    - Logon Activity events
  - Deploy Hybrid Audit agents to other computers to audit Logon Activity as needed.

**i** **NOTE:** Logon Activity Authentication Activity events require native Windows "Audit Logon events" audit policy enabled on servers. See following guide for details: [Change Auditor for Logon Activity Events](#).

- **Step 8: Review Audited Events**
  - Navigate to **Defend | Hybrid Audit | Audited Events**.
  - Review the list of events audited in the Active Directory forest.
- **Step 9: View Audited Event Details**
  - Navigate to **Audit | Searches**.
  - Search events using predefined Active Directory, Group Policy, and Logon Activity searches.
  - Use the **Hybrid Audit Event Name** in the **Change Auditor Event Class Name** filter to create custom searches to search specific events.

## Hybrid Audit Agent Deployment

The Hybrid Audit agent is a lightweight on-premises component that enables Hybrid Audit to monitor and collect Active Directory activity from within your local environment and securely send it to the cloud service for analysis and reporting. The agent is responsible for:

- Capturing audited Active Directory events: It monitors security-relevant AD events (such as logons, changes, and other directory activities) directly on on-premises systems, typically domain controllers.

- Bridging on-premises AD with the cloud service: The agent acts as the connection point between your on-premises environment and Hybrid Audit, securely forwarding collected audit data to the Hybrid Audit backend.
- Enabling visibility and investigation: By sending audit data to Hybrid Audit, the agent allows administrators to view, search, and analyze events in the UI (for example, on the Audited Events page), helping with security monitoring, compliance, and troubleshooting.
- Supporting Hybrid Audit features: Features such as custom audited events, event exclusions, and object-specific auditing depend on the agent being installed and running in the environment.

The Agent Deployment page displays all servers in the Active Directory forest that the Hybrid Audit agent is installed in and allows you to manage agent installations across your on-premises environment. From here, you can:

- View Hybrid Audit agent details.
- Filter the computer list to find specific entries.
- Install, upgrade, or uninstall agents on selected computers.
- Download the Hybrid Audit agent installer for manual installation on on-premises computers.
- Track installation progress.
- Monitor agent connection status to the Hybrid Audit Broker.
- Run a topology scan to update your environment data.
- Export the table view to a CSV file.

**i** **NOTE:** Hybrid Audit supports high availability.

Hybrid Audit agents will connect to the global catalog server to get the service connection points for all the Hybrid Audit Brokers in the forest. The Hybrid Audit agent will attempt to connect to the Broker based on same Site, then same Domain, then the Forest. If the Broker that the agent is connected to becomes unavailable, the agent can connect to the next Broker.

### **To open the Agent Deployment page:**

- Navigate to **Hybrid Audit** from the left-hand menu and select **Agent Deployment**.

**Table 1: Available Computer Details**

Column	Details
Principal Name	The computer display name.
Domain	The domain the computer belongs to.
Computer Type	The computer role, such as Global Catalog, Domain Controller, Read-only Domain Controller, or Member.
Agent Status	<ul style="list-style-type: none"> <li>• Not Installed – Agent has never been installed.</li> <li>• Deploying – Agent is currently being deployed.</li> <li>• Installed – Agent was installed but has never connected.</li> <li>• Connected – Agent is currently connected.</li> <li>• Disconnected – Agent was connected but is now offline.</li> <li>• Uninstalled – Agent has been removed.</li> </ul>

Agent Version	The version number of the installed agent. An Info tip on the column header displays the latest available agent version number.
Last Deployment Result	The outcome of the most recent deployment attempt.
Connected To	The broker to which the computer is connected.

**NOTE:** Click **Filter** to apply filters by column and value or click a column header to sort or filter directly.

### **To install or upgrade an agent:**

**NOTE:** You must use an account with local administrator rights on the target computer.

1. Select the computers you want to install or upgrade the agent on.
2. Click **Install/Upgrade**.
3. Choose one of the following:
  - Run installation as Hybrid Agent service account (default).
  - Enter and validate credentials (used only for this operation; not stored).

Once credentials are validated, the installation or upgrade process will begin.

If the Hybrid Audit agent fails to install, Hybrid Audit will not be able to collect or display audit data from that computer. More specifically:

- Without the agent, on-premises Active Directory events on that computer are not captured.
- On the Agent Deployment page, the computer will typically appear with a status such as Not Installed or disconnected.
- Hybrid Audit related features do not function for that system.
- Gaps in visibility and compliance.

If this happens, review the deployment result or details shown in the Agent Deployment page; re-run the installation after addressing the issue; or reinstall the agent manually on the affected computer.

### **To uninstall an agent:**

1. Select the computers you want to uninstall the agent from.
2. Click **Uninstall**.
3. Choose one of the following:
  - **Run installation as Hybrid Agent service account** (default).
  - Enter and validate credentials (used only for this operation; not stored).
4. Once credentials are validated, the uninstall process will begin.

### ***To download the Hybrid Audit agent installer:***

1. Navigate to **Hybrid Audit** from the left-hand menu and select **Agent Deployment**, and click **Download Agent**.
2. Click **Download**. This downloads the installer file.
3. Copy the installer to each on-premises computer where auditing is required (for example, domain controllers or other relevant servers).
4. Run the installer locally on each computer. The agent is installed by launching the installer directly on the computer.
5. Follow the installation prompts.
6. The setup wizard guides you through configuration so the agent can connect back to the Hybrid Audit service and begin auditing.

### ***To initiate a scan of your environment to update topology data:***

**i** **NOTE:** Run a topology scan after adding new servers or domains to ensure the Agent Deployment page reflects the latest environment.

1. Click **Run Topology Collection**.
2. Confirm the action to scan and update the list of available servers.

### ***To download the current table view as a CSV file:***

- Click **Export to CSV** to download the current table view for offline use or reporting.

## **Hybrid Audit Installation Notes**

The following section outlines how to manage Shields Up and Tier Zero Protection in environments with both Hybrid Audit and Change Auditor deployed.

- **Scenario: Hybrid Audit enabled in a single domain forest (for example, forest.com) where Change Auditor is currently installed.**
  - Only Change Auditor is installed in the organization.
  - Shields Up or Tier Zero Protection is enabled in Identity Defense.
  - Protection templates are sent to the Change Auditor installation with same domain ID as the Shields Up domain or the Tier Zero object.
  - A Hybrid Audit agent is assigned to forest.com that has **Manage Identity Defense Hybrid Audit** enabled to designate a Hybrid Audit Broker.
  - Identity Defense detects that Shields Up and Tier Zero objects with domain ID matching forest.com now have a Hybrid Audit Broker assigned.
  - Protection templates for forest.com are no longer sent to Change Auditor coordinators and previously “Protected” Tier Zero objects have their status changed to “Not protected”.
    - Change Auditor agents in forest.com will no longer receive new protection templates.
  - Enabling Shields Up and Tier Zero protection for Tier Zero objects with the domain ID for forest.com will now be sent to the Hybrid Audit Broker.
    - As Hybrid Audit agents are installed, they will get the protection templates from the Hybrid Audit Broker.
- **Scenario: Hybrid Audit enabled in multi-domain forest (for example, domain1.forest.com, domain2.forest.com) where Change Auditor is installed.**
  - Only Change Auditor is installed in the organization.
  - Shields Up or Tier Zero Protection is enabled in Identity Defense.
  - Protection templates sent to Change Auditor installation with same domain ID as the Shields Up domain or the Tier Zero object (domain1.forest.com or domain2.forest.com).
  - The Hybrid Audit agent assigned to domain1.forest.com has **Manage Identity Defense Hybrid Audit** enabled.
  - Identity Defense detects Shields Up domain or Tier Zero object with domain ID for domain1.forest.com now has a Hybrid Audit Broker.
  - Protection templates for domain1.forest.com are no longer sent to Change Auditor coordinators and previously “Protected” Tier Zero objects have a status of “Not protected”.
  - Enabling Shields Up or Tier Zero protection for Tier Zero objects with domain ID matching domain1.forest.com will now be sent to the Hybrid Audit Broker.
    - As Hybrid Audit agents from domain1.forest.com are installed, they will get the protection templates from the Hybrid Audit Broker.
  - Protection templates for domain2.forest.com continue to be sent to Change Auditor.
    - Any Hybrid Audit agents installed in domain2.forest.com will not get protection templates since Identity Defense sees them as being handled by Change Auditor.

# Working with Hybrid Audit Brokers

Hybrid Audit uses the hybrid agent to communicate with on-premises Active Directory domains. A Hybrid Audit Broker is a Hybrid Audit agent that has been assigned the **Manage Identity Defense Hybrid Audit** permission.

The Hybrid Audit Broker:

- Scans your Active Directory forest topology to identify where Hybrid Audit agents can be deployed.
- Acts as a communication hub, sending commands to the agent and forwarding collected audit events to be displayed in Identity Defense.

**i** | **IMPORTANT:** Each Active Directory forest where hybrid audit agents are deployed must have at least one hybrid audit broker installed.

For more information, see:

- [Overview of the Hybrid Audit Workflow](#)
- [Hybrid Audit Installation Notes](#)

## Enabling Hybrid Audit Brokers

**To configure the Hybrid Audit Broker:**

- From the Dashboard, under **Configuration Status**, select **Configure for Hybrid Agent: Hybrid Audit Broker**. For a first time installation, click **Configure** to view instructions on how to initialize a Hybrid Audit Broker by assigning the **Manage Identity Defense Hybrid Audit** action.

Alternatively, from the left navigation, select **Tenants | Hybrid Agents**, select **Edit Configuration** on the Hybrid Audit agent you would like to use as a Hybrid Audit Broker, and assign it the **Manage Identity Defense Hybrid Audit** action.

After initiating the process, allow a few minutes for the Hybrid Audit Broker to appear under **Defend | Hybrid Audit | Brokers**.

## Viewing Hybrid Audit Broker Details

The Brokers page gives a clear, centralized view of Hybrid Audit Broker activity and health across your forest. It helps administrators easily track performance, check connections, and follow event flow in real time.

**i** | **NOTE:** Broker and Forest Domain Behavior

- Hybrid Audit Brokers are listed according to the forest they belong to.
- A Hybrid Audit Broker from any domain within the forest will attempt to scan the topology of all domains in that forest.
- Hybrid Audit Brokers can connect to agents located in any domain within the forest.
- In forests with multiple domains, Hybrid Audit agents can be deployed across different domains and still connect to a single Hybrid Audit Broker.

**To view the Hybrid Audit Broker status:**

- Navigate to **Hybrid Audit** from the left-hand menu and select **Brokers**.

**Table 2: Available Broker Information**

Column	Description
Principle Name	The unique identifier of the Hybrid Audit Broker.
Domain	The Active Directory domain where the Hybrid Audit Broker resides.
Forest	The forest associated with the Hybrid Audit Broker.
Status	Indicates the Hybrid Audit Broker's current operational state.
Version	Displays the installed version of the Hybrid Audit Broker software.
Agent Port	The port used by agents to connect to the Hybrid Audit Broker.
Total Events Last 24 Hours	Shows the number of events processed by the Hybrid Audit Broker in the past 24 hours.
Connected Agents	Indicates how many agents are currently connected to the Hybrid Audit Broker. The counter is reset when the Hybrid Audit Broker restarted.

**To view Hybrid Audit Broker details:**

- Click a Hybrid Audit Broker link to open a window with additional information including Distinguished Name, Operating System, Last Event Received From Agents, Event Last Uploaded, and Broker Process Is Running As.

**To filter the display:**

- Click **Filter** to apply filters by column and value or click a column header to sort or filter directly.

**To download the current table view as a CSV file:**

- Click **Export to CSV** to download the current table view for offline use or reporting.

## Working with Audited Events

The Audited Events page displays all events that are currently monitored. From this page, you can create custom Active Directory events, enable or disable auditing for specific events, exclude users, computers, and service accounts from generating audit activity, and remove custom events that are no longer needed.

- Enabling an event begins tracking the specified changes within the Active Directory forest.
- Disabling an event stops tracking those changes.

**i NOTE:**

- Events that are disabled by default are typically noisy events that should only be enabled for specific investigations.
- Active Directory, Group Policy, and Logon Activity events recorded by the deployed Hybrid Audit agents are available to search in **Audit | Search**. Specific events can be searched by using the **Hybrid Audit Event Name** in the **Change Auditor Event Class Name** search filter.

### **To view event details:**

- Click an event link to open a window with additional information, including the event's Name, Description, Subsystem, current status, and excluded accounts.

### **To enable and disable the events:**

- Check the box to select the event and click the **Enable** or **Disable** button as required.

### **To filter the display:**

- Click **Filter** to apply filters by column and value or click a column header to sort or filter directly.

### **To remove accounts from the Excluded Accounts list:**

- Click the required event link. In the Event Details dialog, under **Accounts Excluded for the Event**, select the required account and click **Remove**. Removing an account or expression from the list will cause it to no longer be excluded.

See also:

- [Creating and Deleting Custom Active Directory Events](#)
- [Excluding Accounts from Events](#)

## Creating and Deleting Custom Active Directory Events

The Hybrid Audit | Audited Event page now lets you create custom audit events tailored to your organization's needs. Easily define new events by selecting an Active Directory object class, choosing an attribute, and assigning a severity level. Once saved, your custom event is immediately created and monitored—giving you greater visibility, flexibility, and precision in your auditing strategy.

### **To create a custom event:**

1. Select **Defend | Hybrid Audit | Audited Events** and click **Create Event**.
2. Select the required Active Directory class, object attribute, and assign the severity for the event.
3. Click **Save**.
4. Select **Create** to confirm that you want to begin auditing changes to the attribute of the Active Directory class specified in this event.

### **To delete custom events:**

**i** | **NOTE:** Deleting an Active Directory event will stop auditing changes to the attribute of the Active Directory class specified.

1. Select **Defend | Hybrid Audit | Audited Events**.
2. Select the event to remove, and click **Delete Event**.

3. Select **Delete Events** to confirm the removal.

## Excluding Accounts from Events

Event exclusion lets you prevent specific users, computers, or service accounts (MSA, gMSA, dMSA) from being audited. When an object is excluded, events associated with that object are no longer captured.

### To exclude custom events:

1. Select **Defend | Hybrid Audit | Audited Events**.
2. Select the checkbox next to the event you want to modify, then click **Exclude Account**.
3. Choose how to exclude the account. Select an object from the **Objects to Exclude** list, or enter a wildcard expression, then click **Exclude Object**.
4. Click **Save** to confirm your selection.

Objects or expressions added to the excluded accounts list will not be audited for the selected events.

## Working with Protection Templates

The Protection page shows the protection templates used to secure Active Directory and Group Policy objects. Protection templates are created per domain. Each domain in a forest has its own set of templates. For example, in a forest with two domains, you will see two separate sets of Tier Zero protection templates, one for each domain. For information on enabling protection, see [Protecting Tier Zero Objects](#).

### **i** NOTE:

- Protection templates are only created and applied to domains that meet both of the following conditions:
  - The domain is listed under **Tenants | Active Directory Domain**.
  - The domain has an assigned **Tenants | Hybrid Agent with Manage Identity Defense Hybrid Audit** enabled.
- To create or edit protection templates, you must have the **Can Manage Hybrid Audit Protection** permission.

The following built-in protection templates are included by default and cannot be removed:

- Identity Defense Tier Zero Computer Protection Template
- Identity Defense Tier Zero Domain Protection Template
- Identity Defense Tier Zero Group Policy Protection Template
- Identity Defense Tier Zero Group Protection Template
- Identity Defense Tier Zero User Protection Template

From the Protection page, you can create, manage, and remove protection templates.

- [Creating Custom User-defined Protection Templates](#)
- [Viewing Protection Template Details](#)
- [Editing Protection Templates](#)
- [Duplicating Protection Templates](#)
- [Enabling and Disabling Protection Templates](#)
- [Deleting Protection Templates](#)

## Creating Custom User-defined Protection Templates

You can manually create a protection template for an Active Directory object or a Group Policy Object (GPO) by selecting the appropriate template type and configuring the required protection settings.



### NOTE:

- Custom (user-created) protection templates can be deleted. System-created templates cannot be deleted.
- Creating custom protection templates may prevent Active Directory processes from accessing the protected object, which could lead to unintended behavior. For this reason, using a system protection template is recommended whenever possible.
- Only one All Group Policies in the forest protection template is allowed per forest.

### ***To create a template to protect Active Directory computers, groups, and users:***

1. Navigate to **Hybrid Audit** from the left-hand menu and select **Protection**.
2. Click **Create Template**.
3. Enter a name for the template.
4. Select **Active Directory Object** as the template type.
5. Enter and select the Active Directory object to protect.
6. Select the protection scope.
7. Select the operations to protect. By default, Create, Modify Attributes, and Delete are selected.
8. (Optional) To protect additional operations, click **Add Object** and select the required operations.
9. (Optional) From the list of protected objects, remove any objects that are not needed.
10. Click **Save and Continue**.
11. Select which attributes to protect (All Attributes, Only Selected Attributes, or All Except Selected Attributes). You can also choose to exclude specific attributes from protection.
12. Click **Save and Continue**.
13. If the **userAccountControl** attribute is selected, optionally choose which flags within the attribute to protect.
14. Click **Save and Continue**.

15. Specify override accounts that are permitted to access the protected objects by searching and selecting the account.
16. Click **Save and Continue**.

**To create a template to protect Group Policy Objects:**

1. Navigate to **Hybrid Audit** from the left-hand menu and select **Protection**.
2. Click **Create Template**.
3. Enter a name for the template.
4. Select **Group Policy** as the template type.
5. Choose one of the following protection options: **All Group Policies in the forest** or **Selected Group Policies in the forest**. (Optionally) Select **Do not enforce protection for GPOAdmin working copy group policies**. This automatically adds the **GPOAdmin service account** to override accounts to exempt from protection.
6. Select the operations to protect - Create, Delete, Link, Modify Attributes.
7. (Optional) To protect additional operations, click **Add Object** and select the required operations.
8. (Optional) From the list of protected policies, remove any objects that are not needed.
9. Click **Save and Continue**.
10. Specify override accounts that are permitted to access the protected policies by searching and selecting the account.
11. Click **Save and Continue**.

## Viewing Protection Template Details

**To view the enabled protection templates:**

- Navigate to **Hybrid Audit** from the left-hand menu and select **Protection**. From here you can view and filter protection templates.

**Table 3: Available Protection Information**

Column	Description
Created By	Protection templates, are either created by a user or the system.
Template Name	The name assigned to the protection template.
Status	Whether the template is enabled or disabled.
Domain	The domain associated with the template.
Type	Indicates whether the template applies to Active Directory or Group Policy.
Protected Object	The specific object being protected by the template.
Scope	The protection scope: <ul style="list-style-type: none"> <li>• This object only</li> <li>• This object and child objects only</li> </ul>

- This object and all child objects

**To filter the display:**

- Click **Filter** to apply filters by column and value or click a column header to sort or filter directly.

**To view template details:**

1. In the Protection table, locate the template you want to view.
2. Click the template name link.

A page opens and displays the name of the selected protection template, the name of the account that overrides protection, and whether the override applies to Active Directory or Group Policy.

## Enabling and Disabling Protection Templates

Protection templates define how protections are enforced in your environment. Enabling a template applies the defined protections, while disabling it stops enforcement.

**To enable protection templates:**

1. In the Protection table, locate the template you want to view.
2. Select the disabled Active Directory or Group Policy template.
3. Click **Enable**.

The protections defined in the template are immediately enforced in your environment.

**To disable protection templates:**

1. In the Protection table, locate the template you want to view.
2. Select the enabled Active Directory or Group Policy template.
3. Click **Disable**.

The protections defined in the template are no longer enforced.

# Editing Protection Templates

## **i** NOTE:

- Administrators can edit system templates to:
  - Remove Active Directory objects or Group Policy objects from protection
  - Manage override accounts
- Users can create and edit their custom templates.
- You cannot add new protected objects to system templates; you can add objects only to user templates.
- You cannot rename system templates; only user templates can be renamed.
- The template type cannot be changed after creation.
- Predefined override accounts are permanent and cannot be removed.

### ***To edit protection:***

1. In the Protection table, locate the template you want to view.
2. Select a single Active Directory or Group Policy template.
3. Click **Edit**.
4. Update the objects, scope, and operations to protect as needed. Review the resulting list of protected objects and remove any that are no longer required.
5. Click **Save and Continue** to optionally edit the override accounts.
6. Add or remove override accounts as required.
7. Click **Save and Finish** to apply the updates.

# Duplicating Protection Templates

You can create a copy of an existing protection template to customize it for your organization's needs. This allows you to modify protection settings without changing the original system or user-defined template.

**NOTE:**

- Creating or modifying custom protection templates may unintentionally block Active Directory processes from accessing protected objects. Whenever possible, it is recommended to use unmodified system templates.
- The ability to duplicate a template is enabled only when all of the following conditions are met:
  - Only one protection template is selected.
  - The selected template does not protect:
    - All Group Policies in the forest
    - DomainDNS
- Duplicated system templates become user-defined templates.
- Carefully review any changes before enabling a duplicated template to avoid unintended protection or access issues.
- Disabled templates do not enforce protection until explicitly enabled.
- Group Policy protection templates that protect "All Group Policies in the forest" cannot be duplicated.
- Active Directory protection template that protect "DomainDNS" cannot be duplicated.

**To duplicate a protection template:**

1. Navigate to **Hybrid Audit** from the left-hand menu and select **Protection**.
2. Select a single Active Directory or Group Policy template.
3. Click **Duplicate**.
4. Click **Create** to confirm.

The duplicated protection template will have the name "copy of <original\_protection\_template\_name>"

## Deleting Protection Templates

Deleting a protection template will stop the protection defined in the template from being enforced in your environment.

**NOTE:**

- The Delete option is available only when a User protection template is selected.
- Multiple User protection templates can be deleted at the same time.
- The Delete option is disabled when a System protection template is selected.

**To delete custom user-defined protection templates:**

1. In the Protection table, locate the template you want to view.
2. Select the disabled Active Directory or Group Policy template.
3. Click **Delete**.
4. Confirm the removal by clicking **Delete Template**.

# Identity Defense Settings

From the Identity Defense Settings page you can:

- [Configure a Forwarding Destination](#)
- [Manage Indicators](#)
- [Manage Data Collections](#)

## Configuring a Forwarding Destination

If your organization uses Microsoft Sentinel and/or Splunk (Cloud Platform or Enterprise) as a SIEM solution, you can configure Identity Defense to forward [Findings](#) to the applicable tool for further analysis. You can also configure email alerts for [Findings](#), as well as for the first completed assessment.

Once configured, the tile for the forwarding destination shows details of the configuration, as well as when the last Finding was sent. A forwarding destination can also be edited or removed.

**To access the Forwarding configuration page:**

1. From the Security Management Platform left navigation menu, choose **Defend | Settings**.
2. Make sure the **Forwarding** tab is selected.

**To configure Microsoft Sentinel as a forwarding destination:**

1. Click **Add Forwarding Destination**, select **Microsoft Sentinel**.
2. Enter the Sentinel **Workspace ID** and **Shared (Primary) Key**.  
Refer to the [Microsoft documentation](#) for instructions on Finding the Workspace ID and key.
3. Click **Send Test Event** to ensure that a connection can be made to Sentinel.  
A message will be returned indicating whether or not the test event was successfully sent. If the test event was not successful, ensure the Workspace ID and Shared Key were entered correctly.
4. Click **Save**.

**To configure Splunk (Cloud Platform or Enterprise) as a forwarding destination:**

1. Click **Add Forwarding Destination**, select **Splunk**.
2. Enter the **Splunk HTTP Event Collector URL** (e.g. <http or https>://<cloud or server address>:<port>) and **Token**.  
Refer to the [Splunk documentation](#) for instructions on Finding the HTTP Event Collector URL and Token.
3. Click **Send Test Event** to ensure that a connection can be made to Splunk.  
A message will be returned indicating whether or not the test event was successfully sent. If the test event was not successful, ensure the URL and Token were entered correctly.
4. Click **Save**.

**To configure Email as a forwarding destination:**

1. Click **Add Forwarding Destination**, select **Email**.
2. Add the **Forward To** email recipients that you want alerts sent to. If you are entering multiple email addresses, separate each with a semicolon.
3. Click **Save**.

## Managing Indicators

An indicator consists of a set of criteria that is used to evaluate collected data and generate Findings for:

- Tier Zero (including Privileged) object activity
- The following Hygiene, Detected TTP, and Detected Anomaly indicators:
  - Security Assessment vulnerabilities detected by Identity Defense
  - Critical Activity and unprotected Active Directory Tier Zero objects collected by Audit.

**i** | **NOTE:** Indicator-specific detail, with listings by severity and by the data source, can be found in the [Appendix](#).

If you no longer want a Finding to be generated for an indicator, you can [mute](#) it.

**i** | **EXCEPTION:** New Tier Zero object indicators cannot be muted.

**To access the All Indicators page:**

1. From the left navigation menu, choose **Defend | Settings**.
2. Select the **All Indicators** tab.

A list of all indicators displays, with the following information for each:

- Finding (Indicator name)
- one of the following **Severity** levels:



### Critical

Generally reserved for Hygiene and Detected Indicators that are changes to Tier Zero and Privileged object security, have significant potential impact to the Active Directory or Entra ID environment, and are not part of the default Active Directory or Entra ID configuration.

Generally reserved for:

- Hygiene and Detected Indicators that are of high concern but impact single objects.
- the discovery of new Tier Zero domain objects and Privileged tenant objects.
- changes to Tier Zero and Privileged objects that occur more often through normal business operations or are part of the default Active Directory or Entra ID configuration.



### High

Generally reserved for the discovery of:

- Tier Zero user, computer, group, and Group Policy objects.
- Privileged user, role, group, and service principal objects.



### Medium

- **Type** (Tier Zero (which includes Privileged), Hygiene, Detected TTP, Detected Anomaly)
- **Active Findings**
- **Inactive Findings**
- number of **Muted Objects**
- **Mute Status**



**NOTE:** If you click the **Filter** button, you can filter displayed results by one or more of the following criteria:

- Indicator
- Severity
- Type
- Mute Status

#### **To view Indicator Details:**

- Click the link for the indicator.

## Muting and Unmuting Indicators

When [Managing indicators](#) you can mute (or unmute) selected indicators to prevent (or allow) Findings. You can also unmute objects that were muted during [Findings investigation](#).

## **i** NOTES:

- New Tier Zero/Privileged [*Object*] Detected indicators cannot be muted and the Mute Indicator option will be disabled.
- If an indicator for a Security Assessment vulnerability is muted, that vulnerability will not be evaluated in future Assessments.
- If an indicator for Audit Critical Activity is muted, associated events will be hidden.

### **To mute (or unmute) indicators:**

Either:

- Select one or more indicators from the [All Indicators list](#) and click **Mute** (or **Unmute**).
- OR
- From [Indicator Details](#), click **Mute Indicator** (or **Unmute Indicator**).

### **To unmute objects within an indicator:**

1. From the [Indicator Details](#) Muted Objects for this Indicator section, select the object(s) you want to unmute.
2. Click **Unmute Object**.

# Managing Data Collections

From the Data Collections page, you can monitor data collections for workloads within your organization. You can also:

- [manually run a data collection](#)
- [disable data collections](#) that you no longer want to run.

### **To access the Data Collections page:**

1. From the left navigation menu, choose **Defend | Settings**.
2. Select the **Data Collections** tab.

The list of all scheduled data collections in the organization displays, with the following information:

- the **Workload** (Active Directory or Entra ID)
- the **Tenant Name**
  - i** **NOTE:** For Active Directory workloads, this will be the location of the domain controller.
- **Last Collection**, which may be:
  - the date and time of the last data collection
  - Never Collected (i.e., a data collection has not yet run for the workload or the first data collection attempt failed)

- **Duration** of the data collection
- **Last Result**, which may be:
  - Successful
  - Failed
  - -- (indicating that data was never collected)
- **Next Collection**, which may be:
  - the date and time the next data collection is scheduled to run
  - -- (indicating that data was never collected)
- **Collection Status**, which may be:
  - Ready (i.e., the next data collection has not started)
  - Running
  - Disabled
- **Remaining Collections** (i.e., the remaining number of data collections that are permitted to be manually run for the workload within a 24 hour period)
  - i** **NOTE:** The number of collections remaining is determined by the last successful collection duration and the number of successful manually run collections completed in the last 24 hour period. The maximum number of Remaining Collections possible is 24.

# Appendix - Available Audit Search Columns and Filters

This appendix details all the columns, filters, and pre-defined values that are available to help you locate the information you need to secure your environment.

- [Available search filters and columns](#)
- [Available meta filters](#)

## Available search filters and columns

Filter	Value to enter/ available pre-defined values to select
Access Control Policy	<ul style="list-style-type: none"><li>• Enter an associated value</li></ul>
Action	Select from the following pre-defined values: <ul style="list-style-type: none"><li>• Add Attribute</li><li>• Add Object</li><li>• Delete Attribute</li><li>• Delete Object</li><li>• Modify Attribute</li><li>• Move Object</li><li>• Other Actions</li><li>• Rename Object</li></ul>
Activity	<ul style="list-style-type: none"><li>• Enter an associated value</li></ul>
Activity Category	<ul style="list-style-type: none"><li>• Active Directory Federation Services - Server Farm</li><li>• Active Directory Federation Services - Claims Provider Trusts</li><li>• Active Directory Federation Services - Authentication Methods</li><li>• Active Directory Federation Services - Relying Party Trusts</li><li>• Active Directory Federation Services - Endpoints</li><li>• AD Query</li><li>• Alert Plan</li><li>• Alert Rule</li></ul>

**Filter****Value to enter/ available pre-defined values to select**

---

- Anonymous Cloud Activity
- Anonymous Web Site Activity
- Audit Configuration
- Authentication Activity
- Authentication Services Monitoring
- Microsoft Entra
- Microsoft Entra - Administrative Units
- Microsoft Entra- Application
- Microsoft Entra - B2B
- Microsoft Entra - Directory
- Microsoft Entra - Group
- Microsoft Entra - Policy
- Microsoft Entra- Resource
- Microsoft Entra - Risk Event
- Microsoft Entra- Role
- Microsoft Entra - Sign-in
- Microsoft Entra - User
- Category
- Change Auditor Internal Auditing
- Computer Monitoring
- Configuration Monitoring
- Connection Object
- Custom AD Object Monitoring
- Custom ADAM Object Monitoring
- Custom Computer Monitoring
- Custom File System Monitoring
- Custom Group Monitoring
- Custom Registry Monitoring
- Custom User Monitoring
- Defender

**Filter****Value to enter/ available pre-defined values to select**

---

- Detected Anomaly
- Detected Anomaly Item
- Detected TTP
- Detected TTP Item
- DNS Service
- DNS Zone
- Domain Configuration
- Domain Controller Authentication
- Dynamic Access Control
- EMC
- Exchange ActiveSync Monitoring
- Exchange Administrative Group
- Exchange Distribution List
- Exchange Mailbox Monitoring
- Exchange Organization
- Exchange Permission Tracking
- Exchange Security Group
- Exchange User
- Fault Tolerance
- File System Access Denied
- File System Configuration Change
- File System Content Change
- File System Content Access
- File System Security Change
- FluidFS
- Forest Configuration
- FRS Service
- Full Text Event
- Group Policy Item
- Group Policy Object

**Filter****Value to enter/ available pre-defined values to select**

---

- Group Monitoring
- Hygiene
- Hygiene Item
- IP Security
- Link Configuration
- Local Group Monitoring
- Local User Monitoring
- Logon Session
- NetApp
- NETLOGON Service
- None
- Notification Template
- NTDS Service
- Microsoft 365 Exchange Online Administration
- Microsoft 365 SharePoint Online
- Microsoft 365 OneDrive for Business
- Microsoft 365 Exchange Online Mailbox
- OU
- Replication Transport
- Schema Configuration
- Search
- Security Change Detail
- Session Event
- Service Monitoring
- SharePoint Document
- SharePoint Document Library
- SharePoint Farm
- SharePoint Folder
- SharePoint List
- SharePoint List Item

**Filter****Value to enter/ available pre-defined values to select**

---

- SharePoint Permission
- SharePoint Security Group
- SharePoint Site
- SharePoint Site Collection
- Site Configuration
- Site Link Bridge Configuration
- Site Link Configuration
- Skype for Business Administration
- Skype for Business Configuration
- SQL Broker Event
- SQL CLR Event
- SQL Cursors Event
- SQL Data Level
- SQL Database Event
- SQL Deprecation Event
- SQL Errors and Warnings Event
- SQL Full Text Event
- Scan Event
- SQL Locks Event
- SQL Objects Event
- SQL OLEDB Event
- SQL Performance Event
- SQL Progress Report Event
- SQL Query Notifications Event
- SQL Scan Event
- SQL Security Audit Event
- SQL Server Event
- SQL Session Event
- SQL Stored Procedures Event
- SQL Transaction Event
- SQL TSQL Event

**Filter****Value to enter/ available pre-defined values to select**

---

- SQL User-Configurable Event
- Subnets
- System Events
- SYSVOL
- Threat Detection - Alert
- Threat Detection - Risky User
- TO
- TO Item
- Transactions Event
- User Cloud Activity
- User Web Site Activity
- VMware Account
- VMware Alarm
- VMware Authorization
- VMware Cluster
- VMware Custom Field
- VMware Datacenter
- VMware Datastore
- VMware DVPortgroup
- VMware Dvs
- VMware Generic
- VMware Host
- VMware License
- VMware Profile
- VMware Resource Pool
- VMware Scheduled Task
- VMware Session
- VMware Task
- VMware Template Upgrade

Filter	Value to enter/ available pre-defined values to select
	<ul style="list-style-type: none"> <li>VMware Upgrade</li> <li>VMware Virtual Machine</li> </ul>
Activity Id	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Activity Time	<ul style="list-style-type: none"> <li>Enter days or hours</li> </ul>
Actor Id	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Actor Name	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Actor Object Id	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Actor PUID	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Actor Service Principle Name	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Actor User Principal Name	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
AD Authorization Port	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
AD Kerberos	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
AD Security Change Applies To	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
AD Security Change Condition	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
AD Security Change Permission	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
AD Security Change Type	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
AD Simple Bind	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
AD SSL/TLS	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Additional Details	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Additional Info	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Add-on Guid	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Add-on Name	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Add-on Type	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>Bot</li> <li>Connector</li> <li>Tab</li> <li>App</li> </ul>
Affected Items	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Agent Domain Fully Qualified Domain Name	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>
Agent Forest Name	<ul style="list-style-type: none"> <li>Enter an associated value</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
Agent Fully Qualified Domain Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Agent Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Agent OS Version	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Agent Site Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Alert Recipient	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Alert Recipients	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Alert Rule Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Alert Rule Type	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Shared Alert Rule</li> <li>• Private Alert Rule</li> </ul>
Application Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Application Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Attribute Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Atypical Location	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Audit Item	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Audit Source	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Authentication Method	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Authentication Protocol	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Kerberos</li> <li>• NTLM</li> <li>• Unknown</li> </ul>
Authentication Protocol Version	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• V1</li> <li>• V2</li> </ul>
Auto Update From Federation Metadata	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Microsoft Entra Activity Operation Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
Microsoft Entra Activity Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Microsoft Entra Category	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Microsoft Entra Result Description	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Browser Authentication URL	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Category Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Category Type	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Shared Category</li> <li>• Private Category</li> </ul>
Channel Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Channel Guid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Channel Type	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Private</li> <li>• Standard</li> </ul>
Change Auditor Event Class ID	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Change Auditor Event Class Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Change Auditor Facility ID	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Change Auditor Facility Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
City	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Claims Provider Trust Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Client Info String	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Client IP Address	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Client Machine Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Client Process Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Client Version	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Cmdlet Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Comment	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Correlated Activity	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Coordinator Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
Correlation Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Country	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Creator	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Cross-Mailbox Operations	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Custom Event	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Destination File Extension	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Destination FileName	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Destination Folder	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Destination MailboxId	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Destination MailboxId Owner Master Account Sid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Destination MailboxId Owner Sid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Destination MailboxId Owner UPN	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Destination relative URL	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Detection Timing	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• Near Realtime</li> <li>• Not Defined</li> <li>• Offline</li> <li>• Realtime</li> </ul>
Device Information	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Distribution Group Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Domain Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Enabled	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Error Code	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Event Data	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Event Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Event Source	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Event Source Application	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Event Version	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
External Access	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Failure Reason	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Attribute	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Category	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Logon Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Object Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Security Change Applies To	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Security Change Condition	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Security Change Permission	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Security Change Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Shadow Copy	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System Share Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
File System SID	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
First Discovered	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Folder	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Folder Path	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Has file system security change condition	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Has no from value	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Identifiers	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Indicator	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Initiator User Mail	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Initiator User Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
Initiator User SID	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Installation Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Installation Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Internal Correlation Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Is Initial Scan	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Is Linked Group Policy Change	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• False</li> <li>• True</li> </ul>
Item type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Kerberos Ticket Lifetime (Hours)	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Latest Activity Time	<ul style="list-style-type: none"> <li>• Enter the required time frame</li> </ul>
Latest Event Time Detected	<ul style="list-style-type: none"> <li>• Enter the required time frame</li> </ul>
Logon Begin Type	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Additional logon</li> <li>• Concurrent user disconnected</li> <li>• Existing logon</li> <li>• Lock</li> <li>• Logoff</li> <li>• Logon</li> <li>• None</li> <li>• Remote logoff</li> <li>• Remote logon</li> <li>• Screensaver turned off</li> <li>• Screensaver turned on</li> <li>• Shutdown</li> <li>• Unlock</li> </ul>
Logon Duration	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Logon End	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Logon End Type	Select from the following pre-defined values:

Filter	Value to enter/ available pre-defined values to select
	<ul style="list-style-type: none"> <li>• Additional logon</li> <li>• Concurrent user disconnected</li> <li>• Existing logon</li> <li>• Lock</li> <li>• Logoff</li> <li>• Logon</li> <li>• None</li> <li>• Remote logoff</li> <li>• Remote logon</li> <li>• Screensaver turned off</li> <li>• Screensaver turned on</li> <li>• Shutdown</li> <li>• Unlock</li> </ul>
Logon Session End	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Logon Session Start	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Logon Start	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Logon Type (Exchange Online)	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• Admin</li> <li>• Best Access</li> <li>• Delegated</li> <li>• Delegated Admin</li> <li>• Owner</li> <li>• System Service</li> <li>• Transport</li> <li>• Unknown</li> </ul>
Logon Type (Windows)	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Remote Interactive</li> <li>• Domain Authentication</li> <li>• User Session</li> <li>• Interactive</li> <li>• Network</li> <li>• All</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
Logon User Display Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Logon User Sid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Machine Domain Info	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Machine Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Mailbox Guid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Mailbox Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Mailbox Owner Master Account Sid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Mailbox Owner Sid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Mailbox Owner UPN	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Malware Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Max Behavior Level	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
MFA Authentication Detail	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
MFA Authentication Method	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
MFA Required	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
MFA Result	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Modified Object	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Modified Properties	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Monitor Federation Metadata	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Notification Template Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Notification Template Type	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Shared Notification Template</li> <li>• Private Notification Template</li> </ul>
NTLM Impersonation Level	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Default</li> <li>• Anonymous</li> <li>• Identify</li> </ul>

Filter	Value to enter/ available pre-defined values to select
	<ul style="list-style-type: none"> <li>• Impersonate</li> <li>• Delegate</li> </ul>
NTLM Key Length	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Object Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Microsoft365 Organization Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Organization Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Origin AD Site Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Origin IP Address	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Origin IPv4 Address	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Origin IPv6 Address	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Origin Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Originating Server	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Parameters	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Parent Event Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Policy Setting	<ul style="list-style-type: none"> <li>• Access Credential Manager as a trusted caller</li> <li>• Access This Computer From The Network</li> <li>• Account Lockout Duration</li> <li>• Account Lockout Threshold</li> <li>• Account Logon: Audit Credential Validation</li> <li>• Account Logon: Audit Kerberos Authentication Service</li> <li>• Account Logon: Audit Kerberos Service Ticket Operations</li> <li>• Account Logon: Audit Other Account Logon Events</li> <li>• Account Management: Audit Application Group Management</li> <li>• Account Management: Audit Computer Account Management</li> <li>• Account Management: Audit Distribution Group Management</li> <li>• Account Management: Audit Other Account Management Events</li> </ul>

**Filter****Value to enter/ available pre-defined values to select**

---

- Account Management: Audit Security Group Management
- Account Management: Audit User Account Management
- Accounts: Administrator Account Status
- Accounts: Guest Account Status
- Accounts: Limit Local Account Use Of Blank Passwords To Console Logon Only
- Accounts: Rename Administrator Account
- Accounts: Rename Guest Account
- Act As Part Of The Operating System
- Add Workstations To Domain
- Adjust Memory Quotas For A Process
- Allow Log On Locally
- Allow Log On Through Terminal Services
- Application Data Folder options
- Application Data Folder target path
- Audit Account Logon Events
- Audit Account Management
- Audit Directory Service Access
- Audit Logon Events
- Audit Object Access
- Audit Policy Change
- Audit Privilege Use
- Audit Process Tracking
- Audit System Events
- Audit: Audit The Access Of Global System Objects
- Audit: Audit The Use Of Backup And Restore Privilege

**Filter****Value to enter/ available pre-defined values to select**

---

- Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings
- Audit: Shut Down System Immediately If Unable To Log Security Audits
- Authenticode Settings Enable Trusted Publisher Lockdown option
- Autoenrollment Settings
- Automatic Browser Configuration Auto-config URL
- Automatic Browser Configuration Automatic Configuration option
- Automatic Browser Configuration Automatic Configuration Time
- Automatic Browser Configuration Automatic detection option
- Automatic Browser Configuration Auto-proxy URL
- Automatic Certificate Request Settings
- Back Up Files And Directories
- Basic User Hash Rule
- Basic User Zone Rule
- BitLocker Drive Encryption
- Browser Title
- Bypass Traverse Checking
- Central Access Policy
- Change The System Time
- Change the time zone
- Computer Configuration Administrative Template
- Computer Preference Setting
- Connection Settings Delete Existing Option
- Connection Settings Import Option
- Contacts Folder target path
- Content Ratings option

**Filter****Value to enter/ available pre-defined values to select**

---

- Create A Pagefile
- Create A Token Object
- Create Global Objects
- Create Permanent Shared Objects
- Create symbolic links
- Custom Large Static Logo
- Custom Small Animated Logo
- Custom Small Static Logo
- Debug Programs
- Default Security Level
- Delete Existing Channels option
- Delete Existing Favorites option
- Deny Access To This Computer From The Network
- Deny Log On As A Batch Job
- Deny Log On As A Service
- Deny Log On Locally
- Deny Log On Through Terminal Services / Remote Desktop Services
- Designated File Types
- Desktop Folder options
- Desktop Folder target path
- Detailed Tracking: Audit DPAPI Activity
- Detailed Tracking: Audit Process Creation
- Detailed Tracking: Audit Process Termination
- Detailed Tracking: Audit RPC Events
- Devices: Allow Undock Without Having To Logon
- Devices: Allowed To Format And Eject Removable Media
- Devices: Prevent Users From Installing Printer Drivers

- 
- Devices: Restrict CD-ROM Access To Locally Logged-On User Only
  - Devices: Restrict Floppy Access To Locally Logged-On User Only
  - Devices: Unsigned Driver Installation Behavior
  - Disallowed Certificate Rule
  - Disallowed Hash Rule
  - Disallowed Path Rule
  - Disallowed Zone Rule
  - Domain Controller: Allow Server Operators To Schedule
  - Domain Controller: LDAP Server Signing Requirements
  - Domain Controller: Refuse Machine Account Password C
  - Domain Member: Digitally Encrypt Or Sign Secure Channel Data (Always)
  - Domain Member: Digitally Encrypt Secure Channel Data (When Possible)
  - Domain Member: Digitally Sign Secure Channel Data (When Possible)
  - Domain Member: Disable Machine Account Password Changes
  - Domain Member: Maximum Machine Account Password Age
  - Domain Member: Require Strong (Windows 2000 Or Later) Session Key
  - Downloads Folder options
  - Downloads Folder target path
  - DS Access: Audit Detailed Directory Service Replication
  - DS Access: Audit Directory Service Access
  - DS Access: Audit Directory Service Changes
  - DS Access: Audit Directory Service Replication

**Filter****Value to enter/ available pre-defined values to select**

---

- Enable Computer And User Accounts To Be Trusted For Delegation
- Encrypting File System
- Enforce Password History
- Enforce User Logon Restrictions
- Enforcement Files
- "Enforcement Users
- Enterprise Trust
- "Favorites List
- Favorites options
- Favorites target path
- File or Folder
- Force Shutdown From A Remote System
- Generate Security Audits
- Global Object Access Auditing: File system
- Global Object Access Auditing: Registry
- Group Policy Container Access
- Group policy disable computer configuration flag
- Group policy disable user configuration flag
- Group policy WMI Filter
- Impersonate A Client After Authentication
- Important URLs Home Page URL
- Important URLs Online Support URL
- Important URLs Search Bar URL
- Increase a process working set
- Increase Scheduling Priority
- Interactive Logon: Display user information when the session is locked
- Interactive Logon: Do Not Display Last User Name
- Interactive Logon: Do Not Require CTRL+ALT+DEL

**Filter****Value to enter/ available pre-defined values to select**

---

- Interactive Logon: Message Text For Users Attempting To Log On
- Interactive Logon: Message Title For Users Attempting To Log On
- Interactive Logon: Number Of Previous Logons To Cache (In Case Domain Controller Is Not Available)
- Interactive Logon: Prompt User To Change Password Before Expiration
- Interactive Logon: Require Domain Controller Authentication To Unlock Workstation
- Interactive Logon: Require Smart Card
- Interactive Logon: Smart Card Removal Behavior
- Intermediate Certificate Authorities
- IP Security Policy
- Links Folder options
- Links Folder target path
- Links List
- Load And Unload Device Drivers
- Lock Pages In Memory
- Log On As A Batch Job
- Log On As A Service
- Logon/Logoff: Audit Account Lockout
- Logon/Logoff: Audit IPsec Extended Mode
- Logon/Logoff: Audit Logon
- Logon/Logoff: Audit Network Policy Server
- Logon/Logoff: Audit Other Logon/Logoff Events
- Logon/Logoff: Audit Special Logon
- Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax
- Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax
- Manage Auditing And Security Log

**Filter****Value to enter/ available pre-defined values to select**

---

- Maximum Application Log Size
- Maximum Lifetime For Service Ticket
- Maximum Lifetime for User Ticket
- Maximum Lifetime For User Ticket Renewal
- Maximum Password Age
- Maximum Security Log Size
- Maximum System Log Size
- Maximum Tolerance for Computer Clock Synchronization
- Microsoft Network Client: Digitally Sign Communications (Always)
- Microsoft Network Client: Digitally Sign Communications (If Server Agrees)
- Microsoft Network Client: Send Unencrypted Password To Connect To Third-Party SMB Servers
- Microsoft Network Server: Amount Of Idle Time Required Before Suspending Session
- Microsoft Network Server: Digitally Sign Communication (Always)
- Microsoft Network Server: Digitally Sign Communications (If Client Agrees)
- Microsoft Network Server: Disconnect Clients When Logon Hours Expire
- Microsoft network server: Server SPN target name validation level
- Minimum Password Age
- Minimum Password Length
- Modify Firmware Environment
- Music Folder options
- Music Folder target path
- My Documents Folder options
- My Documents Folder Redirection: My Pictures Options

**Filter****Value to enter/ available pre-defined values to select**

---

- My Documents Folder target path
- NAP Client Health Registration Settings: CSP
- NAP Client Health Registration Settings: CSP Key Length
- NAP Client Health Registration Settings: Hash Algorithm
- NAP Client Health Registration Settings: Require server verification
- NAP Client Health Registration Settings: Trusted server group
- NAP Client Health Registration Settings: Trusted server URL
- NAP Enforcement Clients: DHCP Quarentine Enforcement Client
- NAP Enforcement Clients: IPsec Relying Party
- AP Enforcement Clients: RD Gateway Quarentine Enforcement Client
- NAP Enforcement Clients: Remote access enforcement client for Windows XP and Windows Vista
- NAP Enforcement Clients: Wireless EAPOL enforcement client for Windows XP
- NAP User Interface Settings: Description changed
- NAP User Interface Settings: Image File changed
- NAP User Interface Settings: Image File Name changed
- NAP User Interface Settings: Title changed
- Network Access: Allow Anonymous SID/Name Translation
- Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts
- Network Access: Do Not Allow Anonymous Enumeration Of SAM Accounts And Shares

- 
- Network Access: Do Not Allow Storage Of Credentials Or .NET Passports For Network Authentication
  - Network Access: Let Everyone Permissions Apply To Anonymous Users
  - Network Access: Named Pipes That Can Be Accessed Anonymously
  - Network Access: Remotely Accessible Registry Paths
  - Network Access: Remotely Accessible Registry Paths And Sub-Paths
  - Network Access: Restrict Anonymous Access To Named Pipes and Shares
  - Network Access: Shares That Can Be Accessed Anonymously
  - Network Access: Sharing And Security Model For Local Accounts
  - Network Security: Allow Local System to use computer identity for NTLM
  - Network security: Allow LocalSystem NULL session fallback
  - Network security: Allow PKU2U authentication requests to this computer to use online identities
  - Network security: Configure encryption types allowed for Kerberos
  - Network Security: Do Not Store LAN Manager Hash Value On Next Password Change
  - Network Security: Force Logoff When Logon Hours Expire
  - Network Security: LAN Manager Authentication Level
  - Network Security: LDAP Client Signing Requirements
  - Network Security: Minimum Session Security For NTLM SSP Based (Including Secure RPC) Clients
  - Network Security: Minimum Session Security For NTLM SSP Based (Including Secure RPC) Servers

- 
- Network security: Restrict NTLM: NTLM authentication in this domain
  - Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
  - Network security: Restrict NTLM: Add server exceptions in this domain
  - Network security: Restrict NTLM: Audit Incoming NTLM Traffic
  - Network security: Restrict NTLM: Audit NTLM authentication in this domain
  - Network security: Restrict NTLM: Incoming NTLM traffic
  - Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers
  - NLM: Location type
  - NLM: Location type permissions
  - NLM: Network icon permissions
  - NLM: Network name
  - NLM: Network name permissions
  - Object Access: Audit Application Generated
  - Object Access: Audit Certification Services
  - Object Access: Audit File Share
  - Object Access: Audit File System
  - Object Access: Audit Filtering Platform Connection
  - Object Access: Audit Filtering Platform Packet Drop
  - Object Access: Audit Handle Manipulation
  - Object Access: Audit Kernel Object
  - Object Access: Audit Other Object Access Events
  - Object Access: Audit Registry
  - Object Access: Audit SAM
  - Object Access: Detailed File Share
  - Password Must Meet Complexity Requirements

**Filter****Value to enter/ available pre-defined values to select**

---

- Perform Volume Maintenance Tasks
- Pictures Folder options
- Pictures Folder target path
- Place Favorites At Top Of List option
- Policy Change: Audit Authentication Policy Change
- Policy Change: Audit Authorization Policy Change
- Policy Change: Audit Filtering Platform Policy Change
- Policy Change: Audit MPSSVC Rule-Level Policy Change
- Policy Change: Audit Other Policy Change Events
- Policy Change: Audit Policy Change
- Prevent Local Guests Group From Accessing Application Log
- Prevent Local Guests Group From Accessing Security Log
- Prevent Local Guests Group From Accessing System Log
- Privilege Use: Audit Non Sensitive Privilege Use
- Privilege Use: Audit Other Privilege Use Events
- Privilege Use: Audit Sensitive Privilege Use
- Profile System Performance
- Program Settings option
- Proxy Settings Exceptions
- Proxy Settings FTP Proxy
- Proxy Settings Gopher Proxy
- Proxy Settings HTTP Proxy
- Proxy Settings Secure Proxy
- Proxy Settings Socks Proxy
- QoS Policy: Application Name
- QoS Policy: DSCP Value

**Filter****Value to enter/ available pre-defined values to select**

---

- QoS Policy: Local IP
- QoS Policy: Local IP Prefix Length
- QoS Policy: Local Port
- QoS Policy: Protocol
- QoS Policy: Remote IP
- QoS Policy: Remote IP Prefix Length
- QoS Policy: Remote Port
- QoS Policy: Throttle Rate
- QoS Policy: URL
- QoS Policy: URL Recursive
- QoS Policy: Version
- Recovery Console: Allow Automatic Administrative Logon
- Recovery Console: Allow Floppy Copy And Access To All Drives And All Folders
- Registry key
- Remove Computer From Docking Station
- Replace A Process Level Token
- Reset Account Lockout Counter After Change
- Restore Files And Directories
- Restricted Group
- Restricted Group Member
- Restricted Group Membership
- Retain Application Log
- Retain Security Log
- Retain System Log
- Retention Method For Application Log
- Retention Method For Security Log
- Retention Method For System Log
- Saved Games Folder target path

**Filter****Value to enter/ available pre-defined values to select**

---

- Script setting
- Searches Folder options
- Searches Folder target path
- Secure System Partition (For RISC Platforms Only)
- Security Zones and Privacy option
- Shut Down The Computer When The Security Audit Log Is Full
- Shut Down The System
- Shutdown: Allow System To Be Shut Down Without Having To Log On
- Shutdown: Clear Virtual Memory Pagefile
- Software Installation Policy
- Start Menu Folder options
- Start Menu Folder target path
- Starter GPO
- Starter GPO Computer setting
- Starter GPO User setting
- Store Passwords Using Reversible Encryption
- Synchronize Directory Service Data
- System Cryptography: Force Strong Key Protection For User Keys Stored On The Computer policy
- System Cryptography: Use FIPS Compliant Algorithms For Encryption, Hashing, and Signing policy
- System Objects: Default Owner For Objects Created By Members Of The Administrators Group policy
- System Objects: Require Case Insensitivity For Non-Windows Subsystems policy
- System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) policy
- System Services Policy Service
- System Services Policy Service Startup Mode

- 
- System Settings: Optional Subsystems
  - System Settings: Use Certificate Rules On Windows Executables For Software Restriction Policies
  - System: Audit IPsec Driver
  - System: Audit Other System Events
  - System: Audit Security State Change
  - System: Audit Security System Extension
  - System: Audit System Integrity
  - Take Ownership Of Files Or Other Objects
  - Toolbar background Bitmap
  - Toolbar Buttons
  - Trusted People
  - Trusted Publishers
  - Trusted Root Certification Authority
  - Unrestricted Certificate Rule
  - Unrestricted Hash Rule
  - Unrestricted Path Rule
  - Unrestricted Zone Rule
  - Unsigned Non-Driver Installation Behavior
  - User Account Control: Admin Approval Mode for the Built-in Administrator account
  - User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop
  - User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
  - User Account Control: Behavior of the elevation prompt for standard users
  - User Account Control: Detect application installations and prompt for elevation
  - User Account Control: Only elevate executables that are signed and validated

**Filter****Value to enter/ available pre-defined values to select**

---

- User Account Control: Only elevate UIAccess applications that are installed in secure locations
- User Account Control: Run all administrators in Admin Approval Mode
- User Account Control: Switch to the secure desktop when prompting for elevation
- User Account Control: Virtualize file and registry write failures to per-user locations
- User Administrative Template setting
- User Agent String
- User Credential Roaming
- User Credential Roaming Options
- User Group Policy Preference
- User Software Restriction Basic User Hash Rule
- User Software Restriction Basic User Path Rule
- User Software Restriction Basic User Zone Rule
- User Software Restriction Designated File Types
- User Software Restriction Disallowed Certificate Rule
- User Software Restriction Disallowed Hash Rule
- User Software Restriction Disallowed Path Rule
- User Software Restriction Disallowed Zone Rule
- User Software Restriction Enforcement Files
- User Software Restriction Enforcement Users
- User Software Restriction Policies Default Security Level
- User Software Restriction Trusted Publishers
- User Software Restriction Unrestricted Certificate Rule
- User Software Restriction Unrestricted Hash Rule
- User Software Restriction Unrestricted Path Rule
- User Software Restriction Unrestricted Zone Rule

Filter	Value to enter/ available pre-defined values to select
Policy Setting Category	<ul style="list-style-type: none"> <li>• Videos Folder options</li> <li>• Videos target path</li> <li>• Wireless Network Policy</li> <li>• Account Lockout Policy</li> <li>• Additional Rules</li> <li>• Administrative Templates: Policy definitions</li> <li>• Audit Policies</li> <li>• Audit Policy</li> <li>• Central Access Policy</li> <li>• Change Auditor Protection</li> <li>• Event Log</li> <li>• File System</li> <li>• Folder Redirection</li> <li>• GPO Status</li> <li>• Internet Explorer Maintenance</li> <li>• IP Security Policies on Active Directory</li> <li>• Kerberos Policy</li> <li>• NAP Client Configuration</li> <li>• Network List Manager Policies</li> <li>• Password Policy</li> <li>• Policy-Based QoS</li> <li>• Preferences</li> <li>• Public Key Policies</li> <li>• Registry</li> <li>• Restricted Groups</li> <li>• Scripts (Logon/Logoff)</li> <li>• Scripts (Startup/Shutdown)</li> <li>• Security Levels</li> <li>• Security Options</li> </ul>

Filter	Value to enter/ available pre-defined values to select
	<ul style="list-style-type: none"> <li>• Software Installation</li> <li>• Software Restriction Policies</li> <li>• Software Settings</li> <li>• Starter GPO</li> <li>• System Services</li> <li>• User Rights Assignment</li> <li>• Wireless Network Policies</li> <li>• WMI Filtering</li> </ul>
Policy Setting List Item	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Policy Setting Location	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Previous City	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Previous Country	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Previous IP	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Previous Sign-in Time	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Previous State	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Previous User Agent	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Property Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Property Before Value	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Property After Value	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Record Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Relying Party Resource	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Relying Party Trust Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Relying Party Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Request Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Result Status	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Risk Activity	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• Signin</li> <li>• User</li> </ul>
Risk Correlation Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

Filter	Value to enter/ available pre-defined values to select
Risk Detail	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• None</li> <li>• Admin Generated Temporary Password</li> <li>• User Performed Secured Password Change</li> <li>• User Performed Secured Password Reset</li> <li>• Admin Confirmed Signin Safe</li> <li>• Hidden</li> <li>• Admin Confirmed Signin Compromised</li> <li>• Admin Confirmed User Compromised</li> <li>• Admin Dismissed All Risk For User</li> <li>• Ai Confirmed Signin Safe</li> <li>• User Passed MFA Driven By Risk Based Policy</li> </ul>
Risk Detected Time	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Risk Event Details	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Risk Event Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Risk Event Status	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Active</li> <li>• Closed (MFA Auto-Closed)</li> <li>• Closed (Multiple Reasons)</li> <li>• Closed (marked as false positive)</li> <li>• Closed (resolved)</li> <li>• Closed (ignored)</li> <li>• Login Blocked</li> <li>• Remediated</li> </ul>
Risk Event Time	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Risk Event Type	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Anonymous IP Risk Event</li> <li>• Impossible Travel Risk Event</li> <li>• Leaked Credentials Risk Event</li> <li>• Malware Risk Event</li> <li>• Suspicious IP Risk Event</li> <li>• Unfamiliar Location Risk Event</li> </ul>

Filter	Value to enter/ available pre-defined values to select
Risk Level	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Hidden</li> <li>• High</li> <li>• Low</li> <li>• Medium</li> <li>• None</li> </ul>
Risk Source	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Risk State	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• At Risk</li> <li>• Confirmed Compromised</li> <li>• Confirmed Safe</li> <li>• Dismissed</li> <li>• None</li> <li>• Remediated</li> </ul>
Risk Type	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Unlikely Travel</li> <li>• Anonymized IP Address</li> <li>• Malicious IP Address</li> <li>• Unfamiliar Features</li> <li>• Malware Infected IP Address</li> <li>• Suspicious IP Address</li> <li>• Leaked Credentials</li> <li>• Investigations Threat Intelligence</li> <li>• Generic Admin Confirmed User Compromised</li> <li>• Mcas Impossible Travel</li> <li>• Mcas Suspicious Inbox Manipulation Rules</li> <li>• Investigations Threat Intelligence Signin Linked</li> <li>• Malicious IP Address Valid Credentials Blocked IP</li> </ul>
Schema Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Search Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Search Type	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Shared Search</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
	<ul style="list-style-type: none"> <li>• Private Search</li> </ul>
Send as User Mailbox Guid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Send as User SMTP	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Send on behalf of User Mailbox Guid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Send on behalf of User SMTP	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Server Farm Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Server Farm Node Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Server Farm Node Type	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• Primary computer</li> <li>• Secondary computer</li> </ul>
Service	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Active Directory Database</li> <li>• Active Directory Federation Services</li> <li>• Microsoft Entra</li> <li>• Exchange</li> <li>• Group Policy</li> <li>• Logon Activity</li> <li>• Security Management Platform Audit</li> <li>• Security Management Platform</li> <li>• OneDrive</li> <li>• SharePoint</li> <li>• Teams</li> </ul>
Severity	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• High</li> <li>• Low</li> <li>• Medium</li> </ul>
Sharing Target	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Sharing Target Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Sharing Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Site	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
Siter Url	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Source File Extension	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Source File Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Source Folders	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Source Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Source relative Url	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
State	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Status	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• Failed</li> <li>• Successful</li> </ul>
Status Reason (Change Auditor)	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• Failed</li> <li>• Protected</li> <li>• Succeeded</li> </ul>
Subject	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subject Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subject Object Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subject PUID	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subject Resource Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subject Service Principle Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subject Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subject User Principle Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subscription Expiry Date	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subscription Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Subscription Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Tab Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target AD Forest Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Additional Details	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Canonical Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
Target Computer Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Distinguished Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Domain Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target IP Address	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target is Domain Controller	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Target is Global Catalog	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Target is Exchange Server	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Target is Tier Zero	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
Target Managed By	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Object Class	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Object Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Organizational Unit CN	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Parent Object Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Policy Item	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Policy Section	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target PUID	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Resource Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target SAM Account Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Service Principle Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Site Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

<b>Filter</b>	<b>Value to enter/ available pre-defined values to select</b>
Target User Mail	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Target User Principle Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Team Guid	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Team Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Teams Property Name	<p>Select from the following pre-defined values:</p> <ul style="list-style-type: none"> <li>• Allow Box in Files tab</li> <li>• Accepted channel SMTP domains list</li> <li>• Allow DropBox in Files tab</li> <li>• Allow Egnyte in Files tab</li> <li>• Allow Guest access in Teams</li> <li>• Allow Google Drive in Files tab</li> <li>• Allow Resource Account Send Messages</li> <li>• Allow Share File in Files tab</li> <li>• Allow Skype for Business Interop</li> <li>• Allow TBot Proactive Messaging</li> <li>• Allow users to send emails to channels</li> <li>• Guests allow IP video</li> <li>• Guests screen sharing mode</li> <li>• Guests allow Meet Now</li> <li>• Guests allow editing of sent messages</li> <li>• Guests allow Deletion of sent messages</li> <li>• Guests allow chat</li> <li>• Guests allow Giphys in conversations</li> <li>• Guests Giphy content rating</li> <li>• Guests allow memes in conversations</li> <li>• Guests use Stickers in conversations</li> <li>• Guests allow immersive reader</li> <li>• Guests allow private calls</li> <li>• Meeting room device content pin</li> </ul>

Filter	Value to enter/ available pre-defined values to select
	<ul style="list-style-type: none"> <li>• Members can add additional tags</li> <li>• Resource Account Content Access</li> <li>• Show organization tab in chats</li> <li>• Suggested default tags</li> <li>• Suggested feeds appear in user's activity feed</li> <li>• Trending feeds appear in user's activity feed</li> <li>• Tagging permission mode</li> <li>• Team owners can override who can apply tags</li> <li>• Use Exchange address book policy</li> </ul>
Teams Role Type	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Member</li> <li>• Owner</li> <li>• Guest</li> </ul>
Tenant Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Tenant Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Tier Zero Source	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Tier Zero Status	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Certified</li> <li>• Not Tier Zero</li> <li>• Uncertified</li> </ul>
Time Detected	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Time Indexed	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Time Received	<ul style="list-style-type: none"> <li>• Enter days or hours</li> </ul>
Token Issuer	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• AD Federation Services</li> <li>• Microsoft Entra</li> </ul>
Url	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
Url Path	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User (Actor)	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

Filter	Value to enter/ available pre-defined values to select
User Agent	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User Display Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User DN	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User Down-level Logon Name	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User Id	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User is Administrator	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• False</li> <li>• True</li> <li>• Unknown</li> </ul>
User is Tier Zero	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>
User Key	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User Mail	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User Organizational Unit	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User Session Detail	Select from the following pre-defined values: <ul style="list-style-type: none"> <li>• Computer lock/unlock</li> <li>• Computer restart/shutdown</li> <li>• Incorrectly finished</li> <li>• Screensaver</li> <li>• Started before session monitoring service</li> <li>• Terminal services connection</li> <li>• User logon/logoff</li> <li>• User switch</li> </ul>
User Shared With	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User SID	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>
User Type	<ul style="list-style-type: none"> <li>• Enter an associated value</li> </ul>

## Available meta filters

Meta-field search filters group related properties into a single, easy-to-use filter, helping you quickly narrow down search results. For example, the Who meta-filter includes fields such as User (Actor), Actor Name, and Actor ID.

Filter	Property
Who	<ul style="list-style-type: none"> <li>• User (Actor)</li> <li>• User Display Name</li> <li>• User Down-level Logon Name</li> <li>• User SID</li> <li>• User DN</li> <li>• User Id</li> <li>• User Key</li> <li>• Actor Id</li> <li>• Actor Name</li> <li>• Actor Object Id</li> <li>• Actor User Principal Name</li> </ul>
What	<ul style="list-style-type: none"> <li>• Activity</li> <li>• Activity Category</li> <li>• Action</li> <li>• Additional Event Summary</li> <li>• Change Auditor Event Class Name</li> <li>• Indicator</li> <li>• User Session Detail</li> </ul>
Whom	<ul style="list-style-type: none"> <li>• Target</li> <li>• Target Canonical Name</li> <li>• Target Distinguished Name</li> <li>• Target SAM Account Name</li> <li>• Target User Principal Name</li> <li>• Target Object SID</li> <li>• Subject</li> <li>• Subject Name</li> <li>• Subject Object Id</li> <li>• Subject User Principal Name</li> </ul>
Origin	<ul style="list-style-type: none"> <li>• Target Computer Name</li> <li>• Target IP Address</li> <li>• Target Site Name</li> <li>• Origin Name</li> <li>• Origin AD Site Name</li> <li>• Origin IP Address</li> </ul>

Directory

- Origin IPv6 Address
- Target Domain Name
- Tenant Name
- Tenant Id

# Appendix - Identity Defense Indicator Details

This appendix provides details of all indicators in Identity Defense, listed both [by severity](#) and [by source](#).

**i** | **NOTE:** For the general criteria Identity Defense uses to determine severity levels, refer to the topic [Managing Indicators](#).

## Indicators by Severity

The following table lists all Identity Defense indicators, from most to least severe.

Indicator	Type	Severity	Source
Possible Golden Ticket Kerberos exploit	Detected Anomaly	Critical	Audit
Unsafe encryption used in Kerberos ticket (vulnerable to Kerberoasting)	Detected TTP	Critical	Audit
Groups with SID from local domain in their SID History	Hygiene	Critical	Assessments
User accounts with SID from local domain in their SID History	Hygiene	Critical	Assessments
Groups with well-known SIDs in their SID History	Hygiene	Critical	Assessments
User accounts with well-known SIDs in their SID History	Hygiene	Critical	Assessments
Potential sIDHistory injection detected	Detected Anomaly	Critical	Audit
File changes with suspicious file extensions	Detected Anomaly	Critical	Audit
Irregular domain controller registration	Detected Anomaly	Critical	Audit

Indicator	Type	Severity	Source
detected (DCShadow)			
Irregular Active Directory replication activity detected (DCSync)	Detected Anomaly	Critical	Audit
AD Database (NTDS.dit) file modification attempt detected	Detected Anomaly	Critical	Audit
Inheritance is enabled on the AdminSDHolder container	Hygiene	Critical	Assessments
Non-Tier Zero accounts that can promote a computer to a domain controller	Hygiene	Critical	Assessments
Non-Tier Zero accounts can steal password hashes (DCSync)	Hygiene	Critical	Assessments
Tier Zero users owned by non-Tier Zero accounts	Hygiene	Critical	Assessments
Tier Zero computer is owned by a non-Tier Zero account	Hygiene	Critical	Assessments
User accounts with non-default Primary Group IDs	Hygiene	Critical	Assessments
Computer accounts with non-default Primary Group IDs	Hygiene	Critical	Assessments
User accounts without readable Primary Group ID	Hygiene	Critical	Assessments
Computer accounts without readable Primary Group ID	Hygiene	Critical	Assessments
Delegated Managed Service Account (dMSA) with a suspicious configuration (BadSuccessor)	Hygiene	Critical	Assessments
Managed and Group Managed Service accounts that have not cycled their password recently	Hygiene	Critical	Assessments
Non-Tier Zero users with access to gMSA password	Hygiene	Critical	Assessments
Non-Tier Zero accounts can access the gMSA root key	Hygiene	Critical	Assessments
Non-Tier Zero accounts have access to write properties on certificate templates	Hygiene	Critical	Assessments
Non-Tier Zero user accounts with write permissions over Resource-Based Constrained Delegation on the KRBTGT account	Hygiene	Critical	Assessments
Active Directory Operator groups that are not protected by AdminSDHolder	Hygiene	Critical	Assessments
Ordinary user accounts with hidden	Hygiene	Critical	Assessments

Indicator	Type	Severity	Source
privileges (SDProp)			
User accounts in protected groups that are not protected by AdminSDHolder (SDProp)	Hygiene	Critical	Assessments
KRBTGT accounts with Resource-Based Constrained Delegation	Hygiene	Critical	Assessments
Built-in Administrator account that has been used	Hygiene	Critical	Assessments
Anonymous Logon and Everyone groups are members of the Pre-Windows 2000 Compatible Access group	Hygiene	Critical	Assessments
Built-in Guest account is enabled	Hygiene	Critical	Assessments
Schema Admins group contains members	Hygiene	Critical	Assessments
Default Active Directory groups which should not be in use contain members	Hygiene	Critical	Assessments
DnsAdmins group contains members	Hygiene	Critical	Assessments
Non Tier-Zero accounts with Reanimate tombstones permission delegation	Hygiene	Critical	Assessments
Non-Tier Zero accounts with Migrate SID history permission delegation	Hygiene	Critical	Assessments
Non Tier-Zero accounts with Unexpire password permission delegation	Hygiene	Critical	Assessments
Tier Zero Group Policy allows Recovery Mode to be not password-protected	Hygiene	Critical	Assessments
Tier Zero groups with SID History populated	Hygiene	Critical	Assessments
Tier Zero group policy object changes	Detected TTP	Critical	Audit
Domain level group policy linked changes detected	Detected TTP	Critical	Audit
Non-Tier Zero accounts can link GPOs to the domain	Hygiene	Critical	Assessments
Non-Tier Zero accounts can link Group Policy Objects to Domain Controller OU	Hygiene	Critical	Assessments
Non-Tier Zero accounts can link Group Policy Objects to an Active Directory site	Hygiene	Critical	Assessments
Security changes to Tier Zero group policy objects	Detected TTP	Critical	Audit
Tier Zero user accounts with Service Principal Names	Hygiene	Critical	Assessments

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
User ServicePrincipalName attribute changed (vulnerable to Kerberoasting)	Detected TTP	Critical	Audit
Non-Tier Zero user accounts with Service Principal Names	Hygiene	Critical	Assessments
Tier Zero group changes	Detected TTP	Critical	Audit
Unusual increase in failed AD changes	Detected Anomaly	Critical	Audit
Unusual increase in permission changes to AD objects	Detected Anomaly	Critical	Audit
Security changes to Tier Zero group objects	Detected TTP	Critical	Audit
Security changes to Tier Zero user objects	Detected TTP	Critical	Audit
Administrative privilege elevation detected (adminCount attribute)	Detected TTP	Critical	Audit
Non-Tier Zero accounts are able to log onto Tier Zero computers	Hygiene	Critical	Assessments
Tier Zero user logons to computers that are not Tier Zero	Detected TTP	Critical	Audit
Group Policy does not prevent Domain Admins from logging onto non-Tier Zero computer	Hygiene	Critical	Assessments
Unusual increase in failed AD Federation Services sign-ins	Detected Anomaly	Critical	Audit
Unusual increase in failed on-premises sign-ins	Detected Anomaly	Critical	Audit
Unusual increase in tenant sign-in failures	Detected Anomaly	Critical	Audit
Unusual increase in AD account lockouts	Detected Anomaly	Critical	Audit
Unusual increase in file renames	Detected Anomaly	Critical	Audit
Unusual increase in share access permission changes	Detected Anomaly	Critical	Audit
Unusual increase in file deletes	Detected Anomaly	Critical	Audit
Unusual increase in successful AD Federation Services sign-in	Detected Anomaly	Critical	Audit
Unusual increase in successful on-premises sign-ins	Detected Anomaly	Critical	Audit
Unusual increase in successful tenant sign-ins	Detected Anomaly	Critical	Audit
Unusual increase in successful tenant sign-ins	Detected Anomaly	Critical	Audit

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
Tier Zero domain and forest configuration changes	Detected TTP	Critical	Audit
Security changes to Tier Zero domain objects	Detected TTP	Critical	Audit
AD schema configuration changes	Detected TTP	Critical	Audit
Entra ID Conditional Access policy configured to disable Continuous Access Evaluation for users	Hygiene	Critical	Assessments
Entra ID service principals that violate Microsoft Services Agreement	Hygiene	Critical	Assessment
Entra ID Privileged risk events	Detected TTP	High	Audit
Replicating Directory Changes All domain permission granted	Detected TTP	High	Audit
New Tier Zero Domain detected	Tier Zero	High	Identity Defense
Non-Tier Zero account can use a misconfigured certificate template to impersonate any user	Hygiene	High	Assessments
Non-Tier Zero account can request an overly permissive certificate with privileged EKU (ESC2)	Hygiene	High	Assessments
Domain trust configured insecurely	Hygiene	High	Assessments
Domain trust without Kerberos AES encryption enabled	Hygiene	High	Assessments
Tier Zero computer accounts that have not cycled their password recently	Hygiene	High	Assessments
Tier Zero computers that have not recently authenticated to the domain	Hygiene	High	Assessments
Protected group credentials exposed on read-only domain controllers	Hygiene	High	Assessments
Tier Zero account token can be stolen from a read-only domain controller	Hygiene	High	Assessments
User accounts do not require a password	Hygiene	High	Assessments
Group Policy allows reversible passwords	Hygiene	High	Assessments
User accounts have a reversible password	Hygiene	High	Assessments
Computer accounts with reversible password	Hygiene	High	Assessments
Tier Zero account can be delegated	Hygiene	High	Assessments

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
User accounts with Kerberos pre-authentication disabled	Hygiene	High	Assessments
User accounts with unconstrained delegation	Hygiene	High	Assessments
Computer accounts with unconstrained delegation	Hygiene	High	Assessments
User accounts using DES encryption to log in	Hygiene	High	Assessments
Entra ID privileged role members whose passwords have not changed recently	Hygiene	Medium	Assessments
Tier Zero user accounts whose passwords have not changed recently	Hygiene	High	Assessments
User accounts with Service Principal Names using default encryption type	Hygiene	High	Assessments
Tier Zero user accounts configured for Password Never Expires	Hygiene	High	Assessments
Non-Tier Zero user accounts configured for Password Never Expires	Hygiene	High	Assessments
Non-default configuration of the Microsoft Local Administrator Password	Hygiene	High	Assessments
Non-Tier Zero accounts with Microsoft Local Administrator Password (LAPS) access	Detected TTP	High	Assessments
Group Policy scheduled task section modified	Detected TTP	High	Audit
Suspicious ESX Admins group detected in domain	Hygiene	High	Assessments
Suspicious group ESX Admins created or member added	Detected TTP	High	Audit
Suspicious changes to dMSA migration attributes (BadSuccessor)	Detected TTP	High	Audit
Tier Zero computer can be compromised through Resource-Based Constrained Delegation	Hygiene	High	Assessments
Tier Zero computer that has write permissions on Resource-Based Constrained Delegation granted to a non-Tier Zero account	Hygiene	High	Assessments
Non-Tier Zero computer can be compromised through Resource-Based Constrained Delegation	Hygiene	High	Assessments
Tier Zero object migrated to a Delegated Managed Service Account (dMSA)	Hygiene	High	Assessments

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
Accounts that allow Kerberos protocol transition delegation	Hygiene	High	Assessments
DNS zone configuration allows anonymous record updates	Hygiene	High	Assessments
Non-Tier Zero account with write or extended permission on Tier Zero object	Hygiene	High	Assessments
Security changes to Tier Zero computer objects	Detected TTP	High	Audit
Security changes that can prevent object enumeration detected	Detected TTP	High	Audit
Previously reported inactive Tier Zero users that may have become active	Detected TTP	High	Audit
Tier Zero user changes	Detected TTP	High	Audit
User or computer Active Directory workload identities that are Tier Zero	Hygiene	High	Assessments
Foreign Security Principals are members of a Tier Zero group	Hygiene	High	Assessments
Guest accounts assigned to the Global Administrator role	Hygiene	High	Assessments
Domain Controller is running SMBv1 protocol	Hygiene	High	Assessments
Non-Tier Zero account can create Delegated Managed Service Accounts (dMSA) in an OU or container	Hygiene	High	Assessments
All domain users can create computer accounts	Hygiene	High	Assessments
Protected Users group is not being used	Hygiene	High	Assessments
Abnormally large number of Tier Zero user accounts in the domain	Hygiene	High	Assessments
Enabled Tier Zero user accounts that are inactive	Hygiene	High	Assessments
Tier Zero groups that have computer accounts as members	Hygiene	High	Assessments
Anonymous access to Active Directory is enabled	Hygiene	High	Assessments
Tier Zero Group Policy contains a scheduled task	Hygiene	High	Assessments
Entra ID Conditional Access policies do not protect all users from high user risk	Hygiene	High	Assessments
Entra ID Conditional Access policies do not protect all users from risky sign-ins	Hygiene	High	Assessments

Indicator	Type	Severity	Source
Entra ID Privileged accounts that are not secured by multi-factor authentication (MFA)	Hygiene	High	Assessments
Entra ID Conditional Access policies do not protect all privileged users with multi-factor authentication (MFA)	Hygiene	High	Assessments
Entra ID Conditional Access policies do not protect all non-privileged users with multi-factor authentication (MFA)	Hygiene	High	Assessments
Entra ID Conditional Access policies do not block legacy authentication for all users	Hygiene	High	Assessments
Entra ID Privileged principal logons	Detected TTP	Medium	Audit
Synchronized Active Directory user is assigned an Entra ID privileged role	Hygiene	Medium	Assessments
Active Directory Tier Zero object synchronized to Entra ID	Hygiene	Medium	Assessments
Attempt to access protected Active Directory database detected	Detected TTP	Medium	Audit
Attempt to access protected Windows file or folder detected	Detected TTP	Medium	Audit
Attempt to edit protected group policy object detected	Detected TTP	Medium	Audit
Attempt to modify protected Active Directory object detected	Detected TTP	Medium	Audit
Entra ID Privileged service principal changes	Detected TTP	Medium	Audit
More than recommended number of Global Administrators in the organization	Hygiene	Medium	Assessments
More than recommended number of privileged role assignments	Hygiene	Medium	Assessments
Non-Tier Zero Group policy contains a scheduled task	Hygiene	Medium	Assessments
Microsoft Entra seamless single sign-on (AzureADSSOACC) account password has not changed recently	Hygiene	Medium	Assessments
Kerberos KRBTGT account password has not changed recently	Hygiene	Medium	Assessments
Entra ID users are allowed to consent for all applications	Hygiene	Medium	Assessments
Entra ID Privileged tenant level and directory activity	Detected TTP	Medium	Audit

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
Password hash synchronization with on-premises Active Directory is not enabled	Hygiene	Medium	Assessments
Administrators are not enabled for self service password recovery	Hygiene	Medium	Assessments
Entra ID Privileged role changes	Detected TTP	Medium	Audit
New Privileged Entra ID Role Detected	Tier Zero	Medium	Identity Defense
Security defaults are enabled	Hygiene	Medium	Assessments
Group Policy does not enforce built-in Administrator account lockout on all computers	Hygiene	Medium	Assessments
New Tier Zero GPO detected	Tier Zero	Medium	Identity Defense
Tier Zero Group Policy allows Authenticated Users to add computers to the domain	Hygiene	Medium	Assessments
New Privileged Entra ID Service Principal Detected	Tier Zero	Medium	Identity Defense
Entra ID Privileged group changes	Detected TTP	Medium	Audit
New Tier Zero Group detected	Tier Zero	Medium	Identity Defense
New Privileged Entra ID Group detected	Tier Zero	Medium	Identity Defense
New Tier Zero Computer detected	Tier Zero	Medium	Identity Defense
Entra ID Privileged user changes	Detected TTP	Medium	Audit
New Tier Zero User detected	Tier Zero	Medium	Identity Defense
Enabled privileged Entra ID user accounts that are inactive	Hygiene	Medium	Assessments
New Privileged Entra ID User Detected	Tier Zero	Medium	Identity Defense
Entra ID guest user accounts that are inactive	Hygiene	Medium	Assessments
Enabled non-privileged Entra ID user accounts that are inactive	Hygiene	Medium	Assessments
Entra ID Microsoft Authenticator policy does not require geographic location and application name contexts for all users	Hygiene	Medium	Assessments
Password hash synchronization with on-premises Active Directory is delayed	Hygiene	Medium	Assessments

Indicator	Type	Severity	Source
Synchronization with on-premises Active Directory is delayed	Hygiene	Medium	Assessments
Unprotected Tier Zero Domain	Tier Zero	Medium	Protection
Entra ID cloud applications that are not included in a conditional access policy	Hygiene	Medium	Assessments
Entra ID Conditional Access policies do not protect all users with strictly enforce location for Continuous Access Evaluation	Hygiene	Medium	Assessments
Entra ID Conditional Access policies do not require token protection for sign-in sessions for users	Hygiene	Medium	Assessments
Unprotected Tier Zero Group Policy	Tier Zero	Medium	Protection
Unprotected Tier Zero Group	Tier Zero	Medium	Protection
Unprotected Tier Zero Computer	Tier Zero	Medium	Protection
Unprotected Tier Zero User	Tier Zero	Medium	Protection
Printer Spooler service is enabled on a domain controller	Hygiene	Medium	Assessments
Tier Zero user account is disabled	Hygiene	Medium	Assessments
Domain with obsolete domain functional level	Hygiene	Medium	Assessments
NTLM version 1 authentications	Detected TTP	Medium	Audit

## Indicators by Source

Identity Defense Indicators originate from the following sources:

- [Indicators from Audit](#)
- [Indicators from Assessments](#)
- [Indicators from Identity Defense and Protection for Tier Zero Objects](#)

## Indicators from Audit

The following table contains an alphabetical list of all indicators that originate from Audit.

Indicator	Indicator Type	Severity
Active Directory Database (NTDS.dit) access attempt detected	Detected TTP	Critical

<b>Indicator</b>	<b>Indicator Type</b>	<b>Severity</b>
AD Database (NTDS.dit) file modification attempt detected	Detected TTP	Critical
AD schema configuration changes	Detected TTP	Critical
Administrative privilege elevation detected (adminCount attribute)	Detected TTP	Critical
Attempt to access protected Active Directory database detected	Detected TTP	Medium
Attempt to access protected Windows file or folder detected	Detected TTP	Medium
Attempt to edit protected group policy object detected	Detected TTP	Medium
Attempt to modify protected Active Directory object detected	Detected TTP	Medium
Domain level group policy linked changes detected	Detected TTP	Critical
Entra ID Privileged group changes	Detected TTP	Medium
Entra ID Privileged principal logons	Detected TTP	Medium
Entra ID Privileged risk events	Detected TTP	High
Entra ID Privileged role changes	Detected TTP	Medium
Entra ID Privileged service principal changes	Detected TTP	Medium
Entra ID Privileged tenant level and directory activity	Detected TTP	Medium
Entra ID Privileged user changes	Detected TTP	Medium
File changes with suspicious file extensions	Detected TTP	Critical
Group Policy scheduled task section modified	Detected TTP	High
Irregular Active Directory replication activity detected (DCSync)	Detected TTP	Critical
Irregular domain controller registration detected (DCShadow)	Detected TTP	Critical
NTLM version 1 authentications	Detected TTP	Medium
Possible Golden Ticket Kerberos exploit	Detected TTP	Critical
Potential SIDHistory injection detected	Detected TTP	Critical
Previously reported inactive Tier Zero users that may have become active	Detected TTP	High
Replicating Directory Changes All domain permission granted	Detected TTP	High
Security changes that can prevent object enumeration detected	Detected TTP	High
Security changes to Tier Zero computer objects	Detected TTP	High

Indicator	Indicator Type	Severity
Security changes to Tier Zero domain objects	Detected TTP	Critical
Security changes to Tier Zero group objects	Detected TTP	Critical
Security changes to Tier Zero group policy objects	Detected TTP	Critical
Security changes to Tier Zero user objects	Detected TTP	Critical
Suspicious changes to dMSA migration attributes (BadSuccessor)	Detected TTP	High
Suspicious group ESX Admins created or member added	Detected TTP	High
Tier Zero computer changes	Detected TTP	High
Tier Zero domain and forest configuration changes	Detected TTP	Critical
Tier Zero group changes	Detected TTP	Critical
Tier Zero group policy object changes	Detected TTP	Critical
Tier Zero user changes	Detected TTP	High
Tier Zero user logons to computers that are not Tier Zero	Detected TTP	Critical
Unsafe encryption used in Kerberos ticket (vulnerable to Kerberoasting)	Detected TTP	Critical
Unusual increase in AD account lockouts	Detected Anomaly	Critical
Unusual increase in failed AD changes	Detected Anomaly	Critical
Unusual increase in failed AD Federation Services sign-ins	Detected Anomaly	Critical
Unusual increase in failed on-premises sign-ins	Detected Anomaly	Critical
Unusual increase in file deletes	Detected Anomaly	Critical
Unusual increase in file renames	Detected Anomaly	Critical
Unusual increase in permission changes to AD objects	Detected Anomaly	Critical
Unusual increase in share access permission changes	Detected Anomaly	Critical
Unusual increase in successful AD Federation Services sign-in	Detected Anomaly	Critical
Unusual increase in successful on-premises sign-ins	Detected Anomaly	Critical
Unusual increase in successful tenant sign-ins	Detected Anomaly	Critical
Unusual increase in tenant sign-in failures	Detected Anomaly	Critical
User ServicePrincipalName attribute changed (vulnerable to Kerberoasting)	Detected TTP	Critical

## Indicators from Assessments

The following table contains an alphabetical list of all indicators that originate from Identity Defense Assessments,

Indicator	Type	Severity
Abnormally large number of Tier Zero user accounts in the domain	Hygiene	High
Accounts that allow Kerberos protocol transition delegation	Hygiene	High
Active Directory Tier Zero object synchronized to Entra ID	Hygiene	Medium
Active Directory Operator groups that are not protected by AdminSDHolder	Hygiene	Critical
Administrators are not enabled for self service password recovery	Hygiene	Medium
All domain users can create computer accounts	Hygiene	High
Anonymous Logon and Everyone groups are members of the Pre-Windows 2000 Compatible Access group	Hygiene	Critical
Anonymous access to Active Directory is enabled	Hygiene	High
Built-in Guest account is enabled	Hygiene	Critical
Built-in Administrator account that has been used	Hygiene	Critical
Computer accounts with non-default Primary Group IDs	Hygiene	Critical
Computer accounts with reversible password	Hygiene	High
Computer accounts with unconstrained delegation	Hygiene	High
Computer accounts without readable Primary Group ID	Hygiene	Critical
Default Active Directory groups which should not be in use contain members	Hygiene	Critical
Delegated Managed Service Account (dMSA) with a suspicious configuration (BadSuccessor)	Hygiene	Critical
DnsAdmins group contains members	Hygiene	Critical
DNS zone configuration allows anonymous record updates	Hygiene	High
Domain trust configured insecurely	Hygiene	High
Domain trust without Kerberos AES encryption enabled	Hygiene	High
Domain with obsolete domain functional level	Hygiene	Medium
Domain Controller is running SMBv1 protocol	Hygiene	High
Enabled privileged Entra ID user accounts that are inactive	Hygiene	Medium
Enabled non-privileged Entra ID user accounts that are inactive	Hygiene	Medium
Enabled Tier Zero user accounts that are inactive	Hygiene	High
Entra ID cloud applications that are not included in a conditional access policy	Hygiene	Medium
Entra ID Conditional Access policies do not block legacy authentication for all users	Hygiene	High
Entra ID Conditional Access policies do not protect all non-privileged users with multi-factor authentication (MFA)	Hygiene	High
Entra ID Conditional Access policies do not protect all privileged users with multi-factor authentication (MFA)	Hygiene	High

Indicator	Type	Severity
Entra ID Conditional Access policies do not protect all users from high user risk	Hygiene	High
Entra ID Conditional Access policies do not protect all users from risky sign-ins	Hygiene	High
Entra ID Conditional Access policies do not protect all users with strictly enforce location for Continuous Access Evaluation	Hygiene	High
Entra ID Conditional Access policies do not require token protection for sign-in sessions for users	Hygiene	Medium
Entra ID Conditional Access policy configured to disable Continuous Access Evaluation for users	Hygiene	Critical
Entra ID guest user accounts that are inactive	Hygiene	Medium
Entra ID Microsoft Authenticator policy does not require geographic location and application name contexts for all users	Hygiene	Medium
Entra ID Privileged accounts that are not secured by multi-factor authentication (MFA)	Hygiene	High
Entra ID privileged role members whose passwords have not changed recently	Hygiene	Medium
Entra ID service principals that violate Microsoft Services Agreement	Hygiene	Critical
Entra ID users are allowed to consent for all applications	Hygiene	Medium
Foreign Security Principals are members of a Tier Zero group	Hygiene	High
Group Policy does not enforce built-in Administrator account lockout on all computers	Hygiene	Medium
Group Policy does not prevent Domain Admins from logging onto non-Tier Zero computer	Hygiene	Critical
Group Policy allows reversible passwords	Hygiene	High
Groups with SID from local domain in their SID History	Hygiene	Critical
Groups with well-known SIDs in their SID History	Hygiene	Critical
Guest accounts assigned to the Global Administrator role	Hygiene	High
Inheritance is enabled on the AdminSDHolder container	Hygiene	Critical
Kerberos KRBTGT account password that has not changed recently	Hygiene	Medium
KRBTGT accounts with Resource-Based Constrained Delegation	Hygiene	Critical
Managed and Group Managed Service accounts that have not cycled their password recently	Hygiene	Critical
Microsoft Entra seamless single sign-on (AzureADSSOACC) account password has not changed recently	Hygiene	Medium
More than recommended number of Global Administrators in the organization	Hygiene	Medium

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>
More than recommended number of privileged role assignments	Hygiene	Medium
Non-default configuration of the Microsoft Local Administrator Password	Hygiene	High
Non-privileged accounts are able to log onto privileged computers	Hygiene	Critical
Non-Tier Zero accounts are able to log onto Tier Zero computers	Hygiene	Critical
Non-Tier Zero accounts can link GPOs to the domain	Hygiene	Critical
Non-Tier Zero accounts can link Group Policy Objects to an Active Directory site	Hygiene	Critical
Non-Tier Zero accounts can link Group Policy Objects to Domain Controller OU	Hygiene	Critical
Non-Tier Zero accounts have access to write properties on certificate templates	Hygiene	Critical
Non-Tier Zero accounts that can promote a computer to a domain controller	Hygiene	Critical
Non-Tier Zero account with write or extended permission on Tier Zero object	Hygiene	High
Non-Tier Zero computer can be compromised through Resource-Based Constrained Delegation	Hygiene	High
Non-Tier Zero user accounts configured for Password Never Expires	Hygiene	High
Non-Tier Zero user accounts with Service Principal Names	Hygiene	Critical
Non-Tier Zero user accounts with write permissions over Resource-Based Constrained Delegation on the KRBTGT account	Hygiene	Critical
Non-Tier Zero users with access to gMSA password	Hygiene	Critical
Non-Tier Zero account can request an overly permissive certificate with privileged EKU (ESC2)	Hygiene	High
Non-Tier Zero accounts can access the gMSA root key	Hygiene	Critical
Non-Tier Zero account can create Delegated Managed Service Accounts (dMSA) in an OU or container	Hygiene	High
Non-Tier Zero accounts can steal password hashes (DCSync)	Hygiene	Critical
Non-Tier Zero accounts with Microsoft Local Administrator Password (LAPS) access	Hygiene	High
Non-Tier Zero accounts with Reanimate tombstones permission delegation	Hygiene	Critical
Non-Tier Zero Group policy contains a scheduled task	Hygiene	Medium
Non-Tier Zero account can use a misconfigured certificate template to impersonate any user	Hygiene	High
Non Tier-Zero accounts with Unexpire password permission delegation	Hygiene	Critical
Non Tier-Zero accounts with Migrate SID history permission delegation	Hygiene	Critical
Ordinary user accounts with hidden privileges (SDProp)	Hygiene	Critical
Password hash synchronization with on-premises Active Directory is	Hygiene	Medium

Indicator	Type	Severity
delayed		
Password hash synchronization with on-premises Active Directory is not enabled	Hygiene	Medium
Printer Spooler service is enabled on a domain controller	Hygiene	Medium
Protected group credentials exposed on read-only domain controllers	Hygiene	High
Protected Users group is not being used	Hygiene	High
Schema Admins group contains members	Hygiene	Critical
Security defaults are enabled	Hygiene	Medium
Suspicious ESX Admins group detected in domain	Hygiene	High
Synchronization with on-premises Active Directory is delayed	Hygiene	Medium
Synchronized Active Directory user is assigned an Entra ID privileged role	Hygiene	Medium
Tier Zero account token can be stolen from a read-only domain controller	Hygiene	High
Tier Zero computer accounts that have not cycled their password recently	Hygiene	High
Tier Zero computer can be compromised through Resource-Based Constrained Delegation	Hygiene	High
Tier Zero computer is owned by a non-Tier Zero account	Hygiene	Critical
Tier Zero computer that has write permissions on Resource-Based Constrained Delegation granted to a non-Tier Zero account	Hygiene	High
Tier Zero computers that have not recently authenticated to the domain	Hygiene	High
Tier Zero Group Policy allows Recovery Mode to be not password-protected	Hygiene	Critical
Tier Zero groups that have computer accounts as members	Hygiene	High
Tier Zero groups with SID History populated	Hygiene	Critical
Tier Zero object migrated to a Delegated Managed Service Account (dMSA)	Hygiene	High
Tier Zero user account is disabled	Hygiene	Medium
Tier Zero user accounts configured for Password Never Expires	Hygiene	High
Tier Zero user accounts whose passwords have not changed recently	Hygiene	High
Tier Zero user accounts with Service Principal Names	Hygiene	Critical
Tier Zero user accounts with SID History populated	Hygiene	Critical
Tier Zero users owned by non-Tier Zero accounts	Hygiene	Critical
Tier Zero account can be delegated	Hygiene	High
Tier Zero Group Policy allows Authenticated Users to add computers to the domain	Hygiene	Medium
Tier Zero Group Policy contains a scheduled task	Hygiene	High
User accounts with Kerberos pre-authentication disabled	Hygiene	High

Indicator	Type	Severity
User accounts do not require a password	Hygiene	High
User accounts have a reversible password	Hygiene	High
User accounts in protected groups that are not protected by AdminSDHolder (SDProp)	Hygiene	Critical
User accounts using DES encryption to log in	Hygiene	High
User accounts with non-default Primary Group IDs	Hygiene	Critical
User accounts with Service Principal Names using default encryption type	Hygiene	High
User accounts with SID from local domain in their SID History	Hygiene	Critical
User accounts with unconstrained delegation	Hygiene	High
User accounts with well-known SIDs in their SID History	Hygiene	Critical
User accounts without readable Primary Group ID	Hygiene	Critical
User or computer Active Directory workload identities that are Tier Zero	Hygiene	High

## Indicators from Identity Defense and Protection for Tier Zero Objects

The following table contains an alphabetical list of all indicators that originate from Identity Defense and for protection for Tier Zero objects.

Indicator	Indicator Type	Severity	Source
New Privileged Entra ID Group Detected	Tier Zero	High	Identity Defense
New Privileged Entra ID Role Detected	Tier Zero	Medium	Identity Defense
New Privileged Entra ID Service Principal Detected	Tier Zero	Medium	Identity Defense
New Privileged Entra ID Tenant Detected	Tier Zero	Medium	Identity Defense
New Privileged Entra ID User Detected	Tier Zero	Medium	Identity Defense
New Tier Zero Domain detected	Tier Zero	High	Identity Defense
New Tier Zero GPO detected	Tier Zero	Medium	Identity Defense
New Tier Zero Group detected	Tier Zero	Medium	Identity Defense
New Tier Zero Computer detected	Tier Zero	Medium	Identity Defense
New Tier Zero User detected	Tier Zero	Medium	Identity Defense
Unprotected Tier Zero Domain	Tier Zero	Medium	Protection
Unprotected Active Directory Database	Tier Zero	Medium	Protection
Unprotected Tier Zero Computer	Tier Zero	Medium	Protection

Indicator	Indicator Type	Severity	Source
Unprotected Tier Zero Group	Tier Zero	Medium	Protection
Unprotected Tier Zero Group Policy	Tier Zero	Medium	Protection
Unprotected Tier Zero User	Tier Zero	Medium	Protection

# Appendix - Data Collection Details

To understand an environment's security posture, assessments and other calculations leveraging Active Directory and Microsoft Entra ID data require the collection of specific information. This data is crucial for identifying vulnerabilities, misconfigurations, and potential attack paths within Active Directory and Microsoft Entra ID.

To see a comprehensive list of the objects and their collected attributes and properties, see:

- [Active Directory Data Collection Details](#)
- [Microsoft Entra ID Data Collection Details](#)

## Active Directory Data Collection Details

Object	Attribute/Object	Notes
nTDSservice	canonicalName cn DistinguishedName dSHeuristics name objectGUID	
certificateTemplate	canonicalName cn distinguishedName name NTSecurityDescriptor objectGuid msPKI-Certificate-Name-Flag msPKI-Enrollment-Flag msPKI-Minimal-Key-Size msPKI-RA-Signature pKI-ExtendedKeyUsage	
certificationAuthority	canonicalName CN distinguishedName objectGuid name NTSecurityDescriptor	
Computer	canonicalName cn	* Collection of this data requires Administrator membership on the target

Object	Attribute/Object	Notes
	description	computers:
	displayName	
	distinguishedName	<ul style="list-style-type: none"> <li>IsSMB1Enabled</li> </ul>
	dnsHostName	True/False - Indicates if the target computer object has Server Message Block version 1 (SMBv1) enabled
	extensionAttribute (1-15)	
	GPLink	
	GPOptions	
	lastLogonTimeStamp	<ul style="list-style-type: none"> <li>IsSpoolerEnabled</li> </ul>
	msDS-AllowedToActOnBehalfOfOtherIdentity	True/False - Indicates if the target Domain Controller has the Print Spooler service is set to non-disabled state
	msDS-AllowedToDelegateTo	
	msDS-cloudExtensionAttribute (1-20)	
	msDS-NeverRevealGroup msDS-RevealOnDemandGroup	
	msDS-SupersededManagedAccountLink	
	msDS-SupersededServiceAccountState name	
	NTSecurityDescriptor	
	objectGuid	
	objectSid	
	operatingSystem	
	operatingSystemServicePack	
	operatingSystemVersion	
	primaryGroupid	
	pwdLastSet	
	samAccountName	
	servicePrincipalName	
	serverReferenceBL	
	userAccountControl	
	userPrincipalName	
	*IsSMB1Enabled	
	*IsSpoolerEnabled	
Container	canonicalName	
	cN	
	distinguishedName	
	name	
	nTSecurityDescriptor	
	objectGUID	

Object	Attribute/Object	Notes
	objectClass	
dnsZone	canonicalName cN distinguishedName name objectGuid *SetIsUnsecuredDynamicUpdateAllowed	* Collection of this data requires Administrator membership on the Domain Controller:  <ul style="list-style-type: none"> <li>SetIsUnsecuredDynamicUpdate Allowed</li> </ul> True/False - Indicates if the target DNS Zone is set to allow Nonsecure updates
Domain	canonicalName distinguishedName gPLink gPOptions ms-DS-MachineAccountQuota msDS-Behavior-Version name nTSecurityDescriptor objectGUID objectSID	
domainDNS	canonicalName cN maxPwdAge minPwdLength name objectGUID pwdHistoryLength pwdProperties	
controlAccessRight	canonicalName cN displayName distinguishedName name objectGUID rightsGUID validAccesses	
foreignSecurityPrincipal	canonicalName cN description distinguishedName memberOf msDS-PrincipalName	

Object	Attribute/Object	Notes
	name nTSecurityDescriptor objectGUID objectSID	
groupPolicyContainer	canonicalName cN displayName distinguishedName gPCFileSysPath name nTSecurityDescriptor objectGUID	
Group policy settings	allowAdministratorLockout clearTextPassword SeDenyInteractiveLogonRight SeDenyInteractiveLogonRight SeInteractiveLogonRight SeMachineAccountPrivilege SeRemoteInteractiveLogonRight securityLevel	
Group policy scheduled tasks	*Group Policy Scheduled Tasks	* Collects all scheduled tasks found specified in GPOs Computer + User configuration. Located under Preferences   Control Panel Settings   Scheduled Tasks
Group	canonicalName cN description displayName distinguishedName groupType iSCriticalSystemObject member memberOf name nTSecurityDescriptor objectGUID objectSID primaryGroupToken sAMAccountName sIDHistory	

Object	Attribute/Object	Notes
organizationalUnit	canonicalName distinguishedName name cN nTSecurityDescriptor objectGUID gPLink gPOptions	
ms-Kds-Prov-RootKey	canonicalName cN distinguishedName came nTSecurityDescriptor objectGUID	
Schema	allowedAttributes canonicalName cN distinguishedName IDAPDisplayName name objectClass objectGUID schemaIDGUID	
Secret	canonicalName cN distinguishedName name nTSecurityDescriptor objectGUID	
msDS-DelegatedManagedServiceAccount	canonicalName cN description displayName distinguishedName extensionAttribute (1-15) msDS-AllowedToDelegateTo msDS-cloudExtensionAttribute (1-20) msDS-DelegatedMSAState	

Object	Attribute/Object	Notes
	msDS-SupersededManagedAccountLink	
	msDS-SupersededServiceAccountState	
	msDS-GroupMSAMembership	
	msDS-ManagedAccountPrecededByLinkname	
	nTSecurityDescriptor	
	objectGUID	
	objectSID	
	pwdLastSet	
	sAMAccountName	
	servicePrincipalName	
	userAccountControl	
	userPrincipalName	
msDS-GroupManagedServiceAccount	canonicalName	
	cN	
	description	
	displayName	
	distinguishedName	
	extensionAttribute (1-15)	
	msDS-AllowedToDelegateTo	
	msDS-cloudExtensionAttribute (1-20)	
	msDS-DelegatedMSAState	
	msDS-SupersededManagedAccountLink	
	msDS-SupersededServiceAccountState	
	msDS-GroupMSAMembership	
	msDS-ManagedAccountPrecededByLinkname	
	nTSecurityDescriptor	
	objectGUID	
	objectSID	
	pwdLastSet	
	sAMAccountName	
	servicePrincipalName	
	userAccountControl	

Object	Attribute/Object	Notes
	userPrincipalName	
msDS-ManagedServiceAccount	canonicalName cN description displayName distinguishedName extensionAttribute (1-15) msDS-AllowedToDelegateTo msDS-cloudExtensionAttribute (1-20) msDS-DelegatedMSAState mSDS-SupersededManagedAccountLink mSDS-SupersededServiceAccountState mSDS-GroupMSAMembership mSDS-ManagedAccountPrecededByLink name nTSecurityDescriptor objectGUID objectSID pwdLastSet sAMAccountName servicePrincipalName userAccountControl userPrincipalName	
Site	canonicalName cN distinguishedName gpPLink gPOptions name nTSecurityDescriptor objectGUID	
siteServer	distinguishedName objectGuid serverReference	
trustedDomain	canonicalName	

Object	Attribute/Object	Notes
	cN distinguishedName name objectGUID msDS-SupportedEncryptionTypes trustAttributes trustDirection trustPartner trustType	
User	adminCount canonicalName cN description displayName distinguishedName extensionAttribute (1-15) lastLogonTimestamp manager msDS-AllowedToActOnBehalfOfOtherIdentity msDS-AllowedToDelegateTo msDS-cloudExtensionAttribute (1-20) msDS-SupersededManagedAccountLink msDS-SupersededServiceAccountState name nTSecurityDescriptor objectGUID objectSID physicalDeliveryOfficeName primaryGroupID pwdLastSet sAMAccountName servicePrincipalName sIDHistory userAccountControl userPrincipalName	

# Microsoft Entra ID Data Collection Details

Object	Attribute/Object
Application	AppId CreatedDateTime DeletedDateTime DisplayName Id IdentifierUri KeyCredentials Owners PasswordCredentials VerifiedPublisher
Authorization Policy	AllowedToUseSSPR DefaultUserRolePermissions DisplayName Id
Conditional Access Policy	ApplicationsIncludeApplications ConditionalAccessPolicyIncludeUser ConditionalAccessPolicyExcludeUser ConditionalAccessPolicyIncludeGroup ConditionalAccessPolicyExcludeGroup ConditionalAccessPolicyIncludeRole ConditionalAccessPolicyExcludeRole ConditionsClientAppTypes ConditionsSignInRiskLevels ConditionsUserRiskLevels CreatedDateTime DisplayName GrantControlsBuiltInControls GrantControlsOperator Id ModifiedDateTime SessionControlsContinuousAccessEvaluation SessionControlsSecureSignInSessionIsEnabled SessionControlsSignInFrequencyAuthenticationType SessionControlsSignInFrequencyFrequencyInterval SessionControlsSignInFrequencyIsEnabled State TemplateId

<b>Object</b>	<b>Attribute/Object</b>
Contact	DisplayName GivenName Id JobTitle Mail OnPremisesLastSyncDateTime OnPremisesSyncEnabled Surname
Device	AccountEnabled ApproximateLastSignInDateTime ComplianceExpirationDateTime CreatedDateTime DeletedDateTime DeviceCategory DeviceId DisplayName DomainName Id IsCompliant OnPremisesLastSyncDateTime OnPremisesSecurityIdentifier OnPremisesSyncEnabled OperatingSystem OperatingSystemVersion RegistrationDateTime TrustType
Directory Role	Description DirectoryRoleMember DisplayName Id IsBuiltIn IsEnabled IsPrivileged Members RoleTemplateId
Group	CreatedDateTime DeletedDateTime Description DisplayName ExpirationDateTime Members

Object	Attribute/Object
	Owners GroupTypes Id Mail MailEnabled OnPremisesDomainName OnPremisesLastSyncDateTime OnPremisesNetBiosName OnPremisesSamAccountName OnPremisesSecurityIdentifier OnPremisesSyncEnabled PreferredLanguage RenewedDateTime SecurityIdentifier Visibility
MS Authenticator Policy	ExcludeTarget FeatureSettings Id IncludeTarget State
Organization	BusinessPhones City Country CountryLetterCode CreatedDateTime DefaultUsageLocation DeletedDateTime DisplayName Id IsMultipleDataLocationsForServicesEnabled OnPremisesLastPasswordSyncDateTime OnPremisesLastSyncDateTime OnPremisesSyncEnabled PostalCode PreferredLanguage State Street TechnicalNotificationMails TenantType

<b>Object</b>	<b>Attribute/Object</b>
Security Defaults Policy	Description DisplayName Id IsEnabled
Service Principal	AccountEnabled AlternativeNames AppDescription AppDisplayName AppId ApplicationAuthenticationClientSignInActivity ApplicationAuthenticationResourceSignInActivity ApplicationTemplateId AppOwnerOrganizationId AppRoleAssignmentRequired CreatedDateTime DelegatedClientSignInActivity DelegatedResourceSignInActivity DeletedDateTime Description DisabledByMicrosoftStatus DisplayName Id KeyCredentials LastSignInActivity Owners PasswordCredentials ServicePrincipalType SignInAudience Tags
Service Principal Permissions	ConsentType PermissionDisplayName(AppRole displayName) PermissionType PermissionValue(AppRole value) ResourceDisplayName ServicePrincipalId
User	AccountEnabled BusinessPhones DisplayName ExternalUserState

Object	Attribute/Object
	GivenName Id JobTitle LastPasswordChangeDateTime LastSignInDateTime Mail OnPremisesDomainName OnPremisesLastSyncDateTime OnPremisesSamAccountName OnPremisesSecurityIdentifier OnPremisesSyncEnabled SecurityIdentifier SignInActivity Surname UserPrincipalName UserType
User Registration Details	Id IsAdmin IsMFARegistered MethodsRegistered UserDisplayName UserPrincipalName UserType

# Documentation Roadmap

The Security Management Platform Global Settings User Guide contains the documentation for tasks that apply to all Security Management Platform products. This includes:

- Signing up for Quest Security Management Platform
- Managing Organizations and Regions
- Tenant Management
- Configuration settings (Permissions and subscription information)
- Audit logs

Each management product, such as Identity Defense contains its own user guide and release notes that contain the following module -specific content:

- The Release Notes contain a release history and details new features, resolved issues, and known issues.
- The User Guide contains descriptions and procedures for the tasks you can perform with the management tool.

## Additional resources

- For sales or other inquiries, visit [www.quest.com/contact](http://www.quest.com/contact).
- To sign up for a trial or purchase a subscription, go to <https://www.quest.com/on-demand>.
- 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 [Quest On Demand community](#) provides a space for blog posts and a forum to discuss the Security Management Platform products.

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit [www.quest.com](http://www.quest.com) or follow Quest Software on [X \(formerly Twitter\)](#) and [LinkedIn](#).

## 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