

Quest® Security Guardian

# User Guide



© 2025 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 Security Guardian</b> .....	<b>5</b>
About On Demand .....	5
About Security Guardian .....	5
Access Control .....	6
Functional Overview .....	8
Configuring Additional Components .....	9
<b>Using the Dashboard</b> .....	<b>12</b>
<b>Tier Zero Objects</b> .....	<b>14</b>
How Tier Zero Objects are Identified .....	14
Tier Zero Objects List .....	15
Viewing Tier Zero Object Details .....	16
Adding Tier Zero Objects Manually .....	17
Removing Manually-Added Tier Zero Objects .....	18
Certifying Tier Zero Objects .....	18
Protecting Tier Zero Objects .....	19
Exporting the Tier Zero Objects List .....	20
<b>Privileged Objects</b> .....	<b>21</b>
Privileged Objects List .....	21
Viewing Privileged Object Details .....	22
Adding Privileged Objects Manually .....	23
Removing a Manually-added Privileged Object .....	24
Certifying Privileged Objects .....	24
Exporting the Privileged Objects List .....	25
<b>Assessments</b> .....	<b>26</b>
First Assessment Notification Email .....	26
Built-in Assessments .....	26
All Assessments List .....	27
Discoveries and Vulnerabilities .....	28
Discoveries List .....	28
Pre-Defined Active Directory Discoveries .....	28
Additional Permissions Required for Specific Vulnerabilities .....	29
Discovery for Credential Access Vulnerabilities .....	29
Discovery for Defense Evasion Vulnerabilities .....	45
Discovery for Discovery Vulnerabilities .....	47
Discovery for Initial Access Vulnerabilities .....	47

Discovery for Lateral Movement Vulnerabilities .....	48
Discovery for Persistence Vulnerabilities .....	52
Discovery for Privilege Escalation Vulnerabilities .....	53
Discovery for Reconnaissance Vulnerabilities .....	66
Pre-Defined Entra ID Discoveries .....	67
Entra ID Vulnerabilities that Require a Premium License .....	67
Discovery for Entra ID Credential Access Vulnerabilities .....	67
Discovery for Entra ID Discovery Vulnerabilities .....	74
Discovery for Entra ID Initial Access Vulnerabilities .....	74
Discovery for Entra ID Persistence Vulnerabilities .....	79
Discovery for Entra ID Privilege Escalation Vulnerabilities .....	80
Creating a Discovery .....	82
Viewing, Editing, and Deleting a Discovery .....	83
Creating an Assessment .....	84
Viewing, Editing, and Deleting an Assessment .....	85
Assessment Results .....	86
Viewing Detail for an Assessed Vulnerability .....	87
<b>Findings .....</b>	<b>90</b>
Investigating Findings .....	92
Investigating Tier Zero and Privileged Object Findings .....	92
Investigating Hygiene and Detected Indicators .....	93
Muting Findings for Hygiene and Detected Indicators .....	95
Dismissing Findings .....	96
Viewing Finding History .....	96
<b>Security Settings .....</b>	<b>98</b>
Configuring a Forwarding Destination .....	98
Managing Indicators .....	99
Muting and Unmuting Indicators .....	100
Managing Data Collections .....	101
<b>Appendix - Security Guardian Indicator Details .....</b>	<b>103</b>
Indicators by Severity .....	103
Indicators by Source .....	112
Indicators from On Demand Audit .....	112
Indicators from Security Guardian Assessments .....	114
Indicators from Security Guardian and Protection for Tier Zero Objects .....	118
<b>About us .....</b>	<b>120</b>
Technical support resources .....	120

---

# Introducing Quest Security Guardian

- [About On Demand](#)
- [About Security Guardian](#)
- [Access Control](#)
- [Functional Overview](#)
- [Configuring Additional Components](#)

## About On Demand

Quest On Demand 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.

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

Currently, the following modules are available:

- Audit
- License Management
- Migration
- Recovery
- Security

## About Security Guardian

Quest® Security Guardian is an integrated On Demand solution that helps you keep the Active Directory domain(s) and Entra ID tenant(s) 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 On Demand Audit.
- Have Findings forwarded to a SIEM tool and alerts sent to selected email recipients.

Refer to the [Functional Overview](#) for visual representations of Security Guardian functionality.

## Access Control

Quest On Demand uses the Role-based Access Control (RBAC) security policy that restricts information system access to authorized users. Your Quest On Demand 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 On Demand 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 On Demand 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.

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

On Demand comes configured with a number of default roles. The default role permissions settings cannot be changed, but you can create custom roles with specific permission settings to align with your company policies. You can assign multiple roles to each user in order to combine permission sets.

**i** **NOTE:** Every user must be assigned to at least one role. You cannot remove all roles from a user. For more information about the various roles that can be assigned to users, please see the On Demand Global Settings Current - User Guide.

The Security Administrator role gives users full access to Security Guardian, as well as the following permissions for On Demand global settings:

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

For more information on assigning roles, see [Users and Roles](#) in the On Demand Global Settings User Guide.

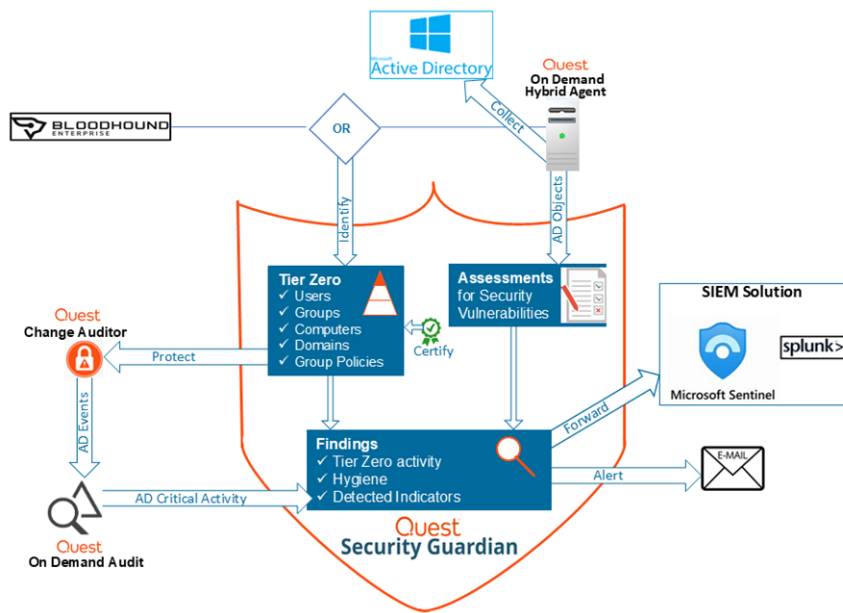


# Functional Overview

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

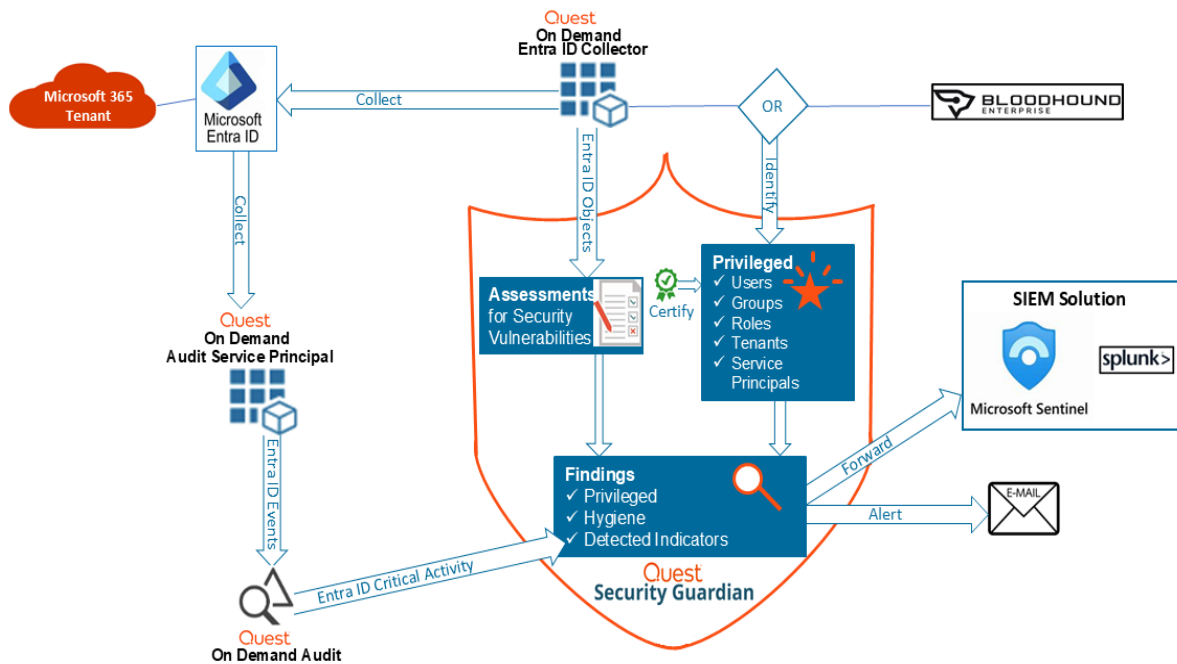
You can click on individual images within the diagram to link to the applicable topic in this guide.

## Functional Overview for Active Directory





## Functional Overview for Entra ID



# Configuring Additional Components

Additional components need to be configured to make Security Guardian fully functional.

### To configure additional components:

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

**NOTE:** Once an additional component is configured in On Demand, it's available to any other module that uses it.

Component	Purpose	Instructions
Hybrid Agent	Gives Security Guardian access to the Active Directory domain(s) that you want to keep secure.	<p><a href="#">On Demand Global Settings User Guide - Managing your on-premises domains</a></p> <p>When configuring the agent, ensure that:</p> <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
Entra ID Data Collector	A Service Principal that gives Security Guardian access to Entra ID objects in the tenant(s) that you want to keep secure.	<p><b>i</b> <b>NOTE:</b> 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 an additional permission to <a href="#">assess certain vulnerabilities</a>.</p> <p>On Demand Global Settings:</p> <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 On Demand Audit Entra ID Service Principal to collect Critical Activity, which contributes to Detected Indicator findings in Security Guardian.</p>
Quest Change Auditor (via On Demand Audit)	Sends Active Directory events to On Demand Audit for reporting in Security Guardian <a href="#">Findings</a> and allows you to <a href="#">protect</a> Tier Zero objects.	<p>Instructions are provided via a tool tip in the Security Guardian UI. You can also find instructions at <a href="#">On Demand Audit User Guide - Change Auditor Integration</a></p> <p><b>i</b> <b>NOTE:</b> A minimum of version 7.3 is required to send critical activity events to On Demand Audit, and a minimum of version 7.4 is required to <a href="#">protect</a> Tier Zero objects.</p>
SpecterOps BloodHound Enterprise (Optional)	Identifies Tier Zero assets in your organization's Active Directory domain(s) and Privileged assets in your Entra ID tenant(s), which you can monitor and <a href="#">assess</a> for security vulnerabilities in Security Guardian.	<a href="#">On Demand Audit User Guide - SpecterOps BloodHound Integration</a>

Component	Purpose	Instructions
	<p><b>i</b> <b>NOTE:</b> If BloodHound Enterprise is not configured, Security Guardian will be used as your organization's provider.</p>	
<p>SIEM solution:</p> <ul style="list-style-type: none"> <li>• Microsoft Sentinel</li> <li>• Splunk Cloud or Enterprise</li> </ul> <p>(Optional)</p>	<p>Allows Security Guardian Findings to be forwarded to a configured SIEM tool for further analysis</p> <p><b>i</b> <b>NOTE:</b> Regardless of whether your organization uses a SIEM solution, you can also have Finding alerts sent via email.</p>	<p><a href="#">Configuring a Forwarding Destination</a></p>

---

# Using the Dashboard

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


**To access the Security Guardian dashboard:**

From the On Demand left navigation menu, choose **Security | 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 Security Guardian (you can click **View All** for an object type to view the complete list for each workload )

 **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 Security Guardian 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.

---

# 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 AD and the assets within it.

Currently, Security Guardian supports the following Tier Zero object types:

- Domains
- Computers
- Groups
- Group Policies
- Users

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

You can also add Tier Zero objects to Security Guardian [manually](#).

## How Tier Zero Objects are Identified

Following are the criteria that the Security Guardian 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
- √ Distributed COM Users
- √ 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.

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 (Security Guardian 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 from within On Demand Audit. 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 On Demand left navigation menu, choose **Security | 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 (Security Guardian, 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** (Security Guardian, 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 (Security Guardian 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
- 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 (Security Guardian or BloodHound Enterprise) cannot be removed via On Demand.

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 Security Guardian 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 (Security Guardian 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 is integrated with On Demand, you can protect Tier Zero objects from unauthorized or accidental modifications or deletions from the Security Guardian 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 On Demand. However, Change Auditor can be used to unprotect objects. Once an object is unprotected, a new Finding will be raised in Security Guardian.
- 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
- Protected
- Pending Evaluation

**i** **NOTE:** A Pending Evaluation status indicates that either Change Auditor has not completed processing the protection request or that Change Auditor 7.4 or later is not integrated with On Demand.

#### **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

# 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.

Security Guardian supports the following Privileged types:

- Groups
- Roles
- Service Principals
- Tenants
- Users

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

## Privileged Objects List

The Privileged Objects list displays all of the Privileged objects that have been collected by the [Privileged objects provider](#) (Security Guardian 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 from within On Demand Audit. 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 On Demand left navigation menu, choose **Security | 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 (Security Guardian, 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** (Security Guardian, 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)
- **i** | **NOTE:** This field *may* be populated only if On Premises Synch 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 (Security Guardian 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 (Security Guardian 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 (Security Guardian or BloodHound Enterprise) cannot be removed via On Demand.

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 (Security Guardian 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 Security Guardian 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

---

# Assessments

Assessments are a set of Discoveries that are evaluated against collected data to identify vulnerabilities in your organization's Active Directory domain(s) and/or Entra ID tenant(s). 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 **Security | Assessments**.

## First Assessment Notification Email

If [email is configured](#) for Security Guardian, 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

Security Guardian 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 On Demand 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.

## 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:

- the **Assessment** name (with a link to [Assessment Details](#))
- the Active Directory domain or Entra ID tenant containing the assessed objects (with the option to [Link to Results](#))
- the **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](#))
- the **Status** of the Assessment:

### Configuration Required

**i** | **NOTE:** This status is used to indicate the absence of an Active Directory domain or Entra ID tenant in On Demand for the organization. This may be because:



- A domain or tenant has not yet been added to On Demand, which will prevent the built-in Assessment from running.
- The domain or tenant selected for the Assessment has since been removed from On Demand.
- 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**

- the date and time when data was **Last Collected**

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

# Discoveries and Vulnerabilities

Discoveries are evaluated by Assessments to identify vulnerabilities in your organization's Active Directory and/or Entra ID. Security Guardian 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

Quest Security Guardian comes with the following pre-defined Discoveries for Active Directory vulnerabilities.

 **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.

Discovery Type	Description
Privilege Escalation	Techniques used by adversaries to gain higher-level privileges on a system, such as local administrator or root.
Reconnaissance	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
Users DES encryption attribute status	<p><b>Name:</b> User accounts using DES encryption to log in</p> <p><b>Default scope:</b> All users</p>	<p>DES encryption is weak and easy for an adversary to crack. User accounts configured to use DES encryption for authentication 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>	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
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 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.</p>	Accounts in scope that have "Store password using reversible encryption" enabled
Users Kerberos preauthentication status	<p><b>Name:</b> User accounts with</p>	User accounts with Kerberos pre-authentication disabled can be compromised as part	User accounts in scope that have "Do not require Kerberos

Vulnerability Template	Vulnerability	Risk	What to find
	<p>Kerberos pre-authentication disabled</p> <p><b>Default scope:</b> All users</p>	<p>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>	<p>preauthentication" <b>enabled</b></p>
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>	<p>User accounts in scope that have "Service Principal Name" <b>not empty</b></p>
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> 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.</p>	<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</p>
Users Password Never Expires status	<p><b>Name:</b> Non-Tier Zero user accounts configured for</p>	<p>User accounts with passwords that are not cycled regularly are more</p>	<p>User accounts in scope that have "Password Never Expires" <b>enabled</b></p>

Vulnerability Template	Vulnerability	Risk	What to find
	Password Never Expires <b>Default scope:</b> All except Tier Zero users	susceptible to brute force password cracking attempts. Accounts that are configured to never require a password change should be remediated accordingly. <b>Remediation:</b> To resolve vulnerability, on the user properties Account tab, ensure the "Password never expires" option is unchecked.	
	<b>Name:</b> Tier Zero user accounts configured for Password Never Expires <b>Default scope:</b> Tier Zero users	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. <b>Remediation:</b> To resolve vulnerability, on the user Properties Account tab, make sure Password never expires is unchecked.	
Protected Users group membership status	<b>Name:</b> Protected Users group is not being used <b>Default scope:</b> Tier Zero users	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 credential theft. <b>Remediation:</b> 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	User accounts in scope that <b>are not</b> members of the "Protected Users" group



Vulnerability Template	Vulnerability	Risk	What to find
		<p>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> 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 that have not recently authenticated to the domain</p> <p><b>Default scope:</b> Tier Zero computers</p>	<p>Tier Zero computers such as domain controllers will 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</p>	<p>Accounts in scope that were last used <b>more than 30</b> days ago</p> <p>NOTE: The number of days is editable.</p>

Vulnerability Template	Vulnerability	Risk	What to find
		controllers that are out of sync with the domain over 30 days should be reinstalled or removed.	
Domain controller SMBv1 protocol status	<p><b>Name:</b> Domain Controller is running SMBv1 protocol</p> <p><b>Default scope:</b> N/A</p> <p><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>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>	Computers in scope that have the SMBv1 protocol enabled
Domain controller Print Spooler status	<p><b>Name:</b> Printer Spooler service is enabled on a domain controller</p> <p><b>Default scope:</b> N/A</p> <p><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 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 service on all domain controllers.</p>	Domain controller that has the Print Spooler service <b>enabled</b>
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</p>	Group Policy objects in scope that have "Store passwords using reversible encryption" <b>enabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
		<p>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</p> <p>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>	
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>	<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 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>	Domain has "Replicating Changes All" and "Replicating Directory Changes" set to <b>Allow</b> for any accounts in scope
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>	Read-only domain controllers (RODCs) should be configured so that Tier Zero user and group credentials are not replicated. If Tier Zero	Objects in scope are <b>not listed</b> in the read-only domain controller "msDS- NeverRevealGroup" attribute

Vulnerability Template	Vulnerability	Risk	What to find
	<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>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>	
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-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.</p>	Objects in scope are listed in the read-only domain controller "msDS-RevealOnDemandGroup" attribute
Account password last changed	<p><b>Name:</b> Managed and Group Managed Service accounts that have not</p>	<p>Managed Service Accounts (MSA) and Group Managed Service accounts (gMSA) that have not had their passwords cycled recently</p>	Accounts in scope that have not updated their password within last <b>30</b> days.

Vulnerability Template	Vulnerability	Risk	What to find
	<p>cycled their password recently</p> <p><b>Default scope:</b> All Service Accounts</p>	<p>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>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> 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.</p>	<p>Computer "ms-Mcs-AdmPwd" attribute has <b>GenericAll</b> or <b>ExtendedRight</b> set for any account in scope</p>
User permission on Resource-Based Constrained Delegation settings for KRBTGT	<p>Non-Tier Zero user accounts with write permissions over Resource-Based Constrained Delegation on the KRBTGT account</p>	<p>Non-Tier Zero user accounts that have the permission to write Resource-Based Constrained Delegation (RBCD) on the KRBTGT account can allow an</p>	<p>Users in scope that have <b>Allow Write</b> permission on Resource-Based Constrained Delegation settings for KRBTGT account</p>

Vulnerability Template	Vulnerability	Risk	What to find
	<p><b>Default scope:</b> All except Tier Zero users</p>	<p>adversary to impersonate any user and take control of the KRBTGT account, and from there, the entire domain.</p> <p><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.</p>	
Tier Zero computers permission granted on Resource-Based Constrained Delegation	<p><b>Name:</b> Tier Zero computer that has write permissions on Resource-Based Constrained Delegation granted to a non-Tier Zero account</p> <p><b>Default scope:</b> All except Tier Zero objects</p>	<p>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.</p> <p><b>Remediation:</b> To resolve vulnerability, review the Tier Zero computer security to determine if non-Tier Zero user accounts should have Write permissions in the Resource-Based Constrained Delegation attribute. If not required, remove Write permissions on the attribute.</p>	Tier Zero computers that have accounts in scope with <b>Allow Write</b> permission on Resource-Based Constrained Delegation
gMSA root key access	<p><b>Name:</b> Non-Tier Zero accounts can access the gMSA root key</p> <p><b>Default scope:</b></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</p>	Accounts in scope that have <b>Allow Read or Allow Write</b> permission for msKds-RootKeyData attribute on msKds-ProvRootKey objects

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> or <b>Enterprise Admins</b> group.</p>	<p>All except Tier Zero objects</p>	<p>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></p> <p>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>Write access on certificate templates</p>	<p><b>Name:</b></p> <p><b>Default scope:</b></p> <p>All except Tier Zero users and groups and Foreign Security Principal (S-1-5-9)</p>	<p>Non-Tier Zero users with write access on certificate templates allow attackers to create illegitimate certificates for any user, which allows 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></p> <p>Remove non-Tier Zero users from having any write access</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
		to "Certificate Templates" container in Configuration - Services - Public Key Services or any pKICertificateTemplate object in that container.	
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> All except Tier Zero users</p>	<p>Non-Tier Zero users that are members of a group that is listed in a Group Managed Service Account's (gMSA) msDS-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>	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
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. 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>
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>	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	Kerberos KRBTGT account password has not been updated within the last <b>180</b> days

Vulnerability Template	Vulnerability	Risk	What to find
		<p>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></p> <p>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 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>	
Group Policy "Allow Administrator account lockout" status	<b>Name:</b> Group Policy does not	In order to prevent brute force attacks, Microsoft	Computer objects in scope do not have an assigned group policy with "Allow

Vulnerability Template	Vulnerability	Risk	What to find
	<p>enforce built-in Administrator account lockout on all computers</p> <p><b>Default scope:</b> All computers</p>	<p>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> <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",</p>	<p>Administrator account lockout" <b>Enabled</b></p>

Vulnerability Template	Vulnerability	Risk	What to find
		"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.	
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>NOTE: If no Entra ID collection is available, an Inconclusive message is returned.</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 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</p>	AzureADSSOACC account password has not been updated within last <b>30</b> days

Vulnerability Template	Vulnerability	Risk	What to find
		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 less than <b>30 days</b> 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 AdminSDHolder (SDProp)</p> <p><b>Default scope:</b> All users</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 set to 1 could be evidence of an adversary who has breached the directory and trying to remain undetected. 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> </ul>	<p>User objects in scope that are members of protected groups and have adminCount attribute set to <b>0 or not set</b>.</p>

Vulnerability Template	Vulnerability	Risk	What to find
		<ul style="list-style-type: none"> <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>	
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>	Accounts in scope that have <b>Deny Read</b> set for the "Primary Group ID" attribute
	<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>	
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>	The dsHeuristics attribute on the Directory Service object indicates <b>some Operator groups</b> are excluded from AdminSDHolder protection

Vulnerability Template	Vulnerability	Risk	What to find
		<p><b>Remediation:</b></p> <p>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>	

## 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></p> <p>Tier Zero user accounts whose passwords have not changed recently</p> <p><b>Default Scope:</b></p> <p>Tier Zero users</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> <p>To resolve vulnerability, update the administrator password and enforce a password policy to ensure the administrator account password is updated regularly.</p>	Accounts in scope that have not updated their password within last <b>180</b> days

## 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	<p><b>Name:</b></p> <p>Built-in Guest account is enabled</p>	The built-in Guest account enables access to Active Directory without requiring a password and should be disabled.	Built-in Guest accounts that are <b>enabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
	<p><b>Default scope:</b> N/A</p>	<p><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).</p>	
Anonymous access to Active Directory status	<p><b>Name:</b> Anonymous access to Active Directory is enabled</p> <p><b>Default scope:</b> N/A</p>	<p>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.</p> <p><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.</p>	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	<p>Active Directory Tier Zero object synchronized to 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>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 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>	Active Directory users and groups in 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 except domain controllers</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> 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.</p>	Accounts in scope that have Trusted for Delegation <b>enabled</b>
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</p>	<p>Without hardening, all domain users have the ability to create computer accounts in the domain. Improperly configured computer accounts are exposed to</p>	Domain has the "ms-DS-MachineAccountQuota" attribute set to <b>more than 0</b> NOTE: The operator and

Vulnerability Template	Vulnerability	Risk	What to find
	accounts <b>Default scope:</b> N/A	Kerberos authentication attacks. Only administrators should be able to add new computer accounts. <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.	quota attribute value are editable.
Account "Use any authentication protocol" status	<b>Name:</b> Accounts that allow Kerberos protocol transition delegation <b>Default scope:</b> All users and computers	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. <b>Remediation:</b> In the account Properties -Delegation tab, ensure configured delegation is not set to "Use any authentication protocol."	Accounts in scope which have "Use any authentication protocol" <b>enabled</b> in delegation
Domain Unexpire Password permission delegation	<b>Name:</b> Non-Tier Zero accounts with Unexpire password permission delegation <b>Default scope:</b> All except Tier Zero users and groups	If the "Unexpire password" permission is delegated an adversary could use it to restore the password of a Tier Zero principal.  This vulnerability will not generate a Finding in Security Guardian. <b>Remediation:</b> Except for the Domain Admins group, these delegations should be removed unless there is a compelling reason for their existence.	Domain has "Unexpire password" set to <b>Allow</b> for any accounts in scope
Domain Migrate SID history permission delegation	<b>Name:</b> Non-Tier Zero accounts with Migrate SID history permission delegation	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. <b>Remediation:</b>	Domain has "Migrate SID history" set to <b>Allow</b> for any accounts in scope

Vulnerability Template	Vulnerability	Risk	What to find
	<p><b>Default scope:</b> All except Tier Zero users and groups</p>	<p>Except for the Domain Admins group, these delegations should be removed unless there is a compelling reason for their existence.</p>	
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>	<p>Domain has "Reanimate tombstones" set to <b>Allow</b> for any accounts in scope</p>
Group Policy "Add workstations to domain" setting Authenticated User status	<p><b>Name:</b> Tier Zero Group Policy allows Authenticated Users to add computers to the domain</p> <p><b>Default scope:</b> All Tier Zero Group Policies</p>	<p>Without hardening, any authenticated user has permissions to create up to 10 computer accounts in the domain. Improperly configured computer accounts 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>	<p>Group Policy objects in scope <b>with</b> Authenticated Users configured in "Add workstations to domain" setting</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 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>	Foreign Security Principals in scope that <b>are</b> members of a Tier Zero group
Group Policy contains Scheduled Task status	<p>Non-Tier Zero Group policy contains a scheduled task</p> <p><b>Default scope:</b> All non-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>	Group Policy objects in scope <b>with</b> Scheduled Task configured

Vulnerability Template	Vulnerability	Risk	What to find
	<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 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
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>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>	<p>Accounts in scope that have a "Primary Group" that is not <b>Domain Users</b> or <b>Domain Guests</b></p>
	<p><b>Name:</b> Computer accounts with non-default Primary</p>	<p>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>	<p>Accounts in scope that have a "Primary Group" that is not <b>Domain Computers</b> or <b>Domain Controllers</b> or <b>Read-Only</b></p>

Vulnerability Template	Vulnerability	Risk	What to find
	Group IDs <b>Default scope:</b> All computers	<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:</li> <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>	<b>Domain Controllers</b>
Users Service Principal Name status	<b>Name:</b> Tier Zero user accounts with Service Principal Names <b>Default scope:</b> Tier Zero users	<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	<b>Name:</b> Abnormally large number of Tier Zero user accounts in the domain <b>Default scope:</b> N/A	<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	<b>Name:</b> Tier Zero user accounts with SID History populated <b>Default scope:</b> Tier Zero users	<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</p>	Accounts in scope that have SID History <b>not empty</b>

Vulnerability Template	Vulnerability	Risk	What to find
		group membership directly to the user object.	
	<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> 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.</p>	
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	<b>Name:</b>	The number of Tier Zero accounts in a domain	Users in scope that are <b>disabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
	Tier Zero user account is disabled <b>Default scope:</b> Tier Zero users	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. <b>Remediation:</b> Remove Tier Zero group membership from user accounts that are disabled.	
Group Members Count	<b>Name:</b> Default Active Directory groups which should not be in use contain members <b>Default scope:</b> Account Operators Backup Operators Cryptographic Operators Hyper-V Administrators Network Configuration Operators Print Operators Remote Desktop Users Replicator Server Operators	Default Active Directory groups have elevated 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. <b>Remediation:</b> Remove the members within default Active Directory groups: <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>	Groups in scope that have more than 0 members NOTE: The operator and number of days are editable.



Vulnerability Template	Vulnerability	Risk	What to find
Schema Admins Group Member Count	<p><b>Name:</b> Schema Admins group contains members</p> <p><b>Default scope:</b> 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> 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 adminCount attribute value	<p><b>Name:</b> Ordinary user accounts with hidden privileges (SDProp)</p> <p><b>Default scope:</b> All users</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. 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>User objects in scope that are not members of protected groups and have adminCount attribute set to 1</p>

Vulnerability Template	Vulnerability	Risk	What to find
		<p><b>Remediation:</b></p> <p>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>	
Verify group membership of DnsAdmins group	<p><b>Name:</b> DnsAdmins group contains members</p> <p><b>Default scope:</b> All users</p>	<p>DNS is an appealing target for adversaries as it can be used to redirect domain queries or launch a denial of service. Members of the DnsAdmins group which are not highly Tier Zero Active Directory administrators are suspicious and increase the attack surface.</p> <p><b>Remediation:</b></p> <p>Review the members of the DnsAdmins group, determine if any members are not highly Tier Zero Active Directory administrators, and remove them if appropriate.</p>	DnsAdmins group has more than <b>0</b> members
Anonymous Logon and Everyone groups are members of Pre-Windows 2000 Compatible Access group	<p><b>Name:</b> Anonymous Logon and Everyone groups are members of the Pre-Windows 2000 Compatible Access group</p> <p><b>Default scope:</b> N/A</p>	<p>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.</p> <p><b>Remediation:</b></p> <p>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).</p>	Pre-Windows 2000 Compatible Access group <b>contains</b> Anonymous Logon and Everyone groups
Tier Zero user account ownership	<p><b>Name:</b> Tier Zero users owned by non-Tier Zero accounts</p> <p><b>Default scope:</b> N/A</p>	<p>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.</p> <p><b>Remediation:</b></p> <p>Remove the non-Tier Zero user ownership on the Tier Zero user account and investigate who modified the owner and when.</p>	Tier Zero user accounts that are owned by a <b>non-Tier Zero account</b>

Vulnerability Template	Vulnerability	Risk	What to find
Tier Zero computer account ownership	<p><b>Name:</b> Tier Zero computer is owned by a non-Tier Zero account</p> <p><b>Default scope:</b> N/A</p>	<p><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.</p>	Tier Zero computer accounts that are owned by a <b>non-Tier Zero account</b>
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>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>	Group Policy objects in scope "Recovery console: Allow automatic administrative logon" is <b>enabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
	<p><b>Default scope:</b></p> <p>Tier Zero Group Policies</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><b>Default scope:</b> All except Tier Zero users, groups and 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 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.</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
Non-Tier Zero Group Policy "Deny log on" for Domain Admin status	<p><b>Name:</b> Domain Admins can log into computers with non-Tier Zero Group Policy</p> <p><b>Default scope:</b> All except Tier Zero Group Policies</p>	<p>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, Tier Zero credentials could be exposed.</p> <p><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.</p>	Group Policies in scope that do not have Domain Admins group added to the <b>Deny log on locally</b> or <b>Deny log on through Remote Desktop Services</b> setting
DNS zone dynamic updates status	<p><b>Name:</b> DNS zone configuration allows anonymous record updates</p> <p><b>Default scope:</b> N/A</p>	<p>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</p>	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>queries and harvest credentials.</p> <p><b>Remediation:</b></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>	
<p>Computer Resource-Based Constrained Delegation status</p>	<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></p> <p>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>	<p>Computer accounts in scope that <b>have</b> Resource-Based Constrained Delegation configured</p>
	<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></p> <p>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</p>	

Vulnerability Template	Vulnerability	Risk	What to find
	<p><b>scope:</b> All except Tier Zero computers</p>	<p>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): 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</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></p>	Active Directory Site has "Write gPLink" set to <b>Allow</b> for any accounts in scope

Vulnerability Template	Vulnerability	Risk	What to find
	Objects to an Active Directory site <b>Default scope:</b> All except Tier Zero users and groups	These delegations should be removed unless there is a compelling reason for their existence.	
Domain Controller OU Write gPLink delegation	<b>Name:</b> Non-Tier Zero accounts can link Group Policy Objects to Domain Controller OU <b>Default scope:</b> All except Tier Zero users and groups	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. <b>Remediation:</b> These delegations should be removed unless there is a compelling reason for their existence.	Domain Controllers OU has "Write gPLink" set to <b>Allow</b> for any accounts in scope
Computer account group membership status	<b>Name:</b> Tier Zero groups that have computer accounts as members <b>Default scope:</b> Tier Zero groups	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. 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. <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.	Groups in scope that <b>have</b> computer accounts as members

Vulnerability Template	Vulnerability	Risk	What to find
KRBTGT account resource-based constrained delegation status	<p><b>Name:</b> KRBTGT accounts with Resource-Based Constrained Delegation</p> <p><b>Default scope:</b> N/A</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 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>	KRBTGT accounts that <b>have</b> Resource-Based Constrained Delegation configured
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>	Domain trust in scope has <b>EnableTgtDelegation</b> or <b>EnablePIMTrust</b> configured in the trustAttribute
Active Directory group existence in domain	<p><b>Name:</b> Suspicious ESX Admins group detected in</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</p>	Active Directory group in scope is <b>detected</b>



Vulnerability Template	Vulnerability	Risk	What to find
	<p>domain</p> <p><b>Default scope:</b> ESX Admins</p>	<p>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>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>	
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>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>	Accounts in scope <b>can</b> request a certificate that allows the subjectAltName (SAN) to be specified

Vulnerability Template	Vulnerability	Risk	What to find
		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.	
Account ability to request an overly permissive certificate with privileged EKU	<p><b>Name:</b> 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>Certificate template settings determine the 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>	Accounts in scope <b>can</b> request a certificate that has either no EKU defined or has the “Any Purpose” EKU

## 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></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</p>	Domain functional level <b>Windows Server 2012</b> or earlier

Vulnerability Template	Vulnerability	Risk	What to find
	N/A	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.	

## Pre-Defined Entra ID Discoveries

Quest Security Guardian 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 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 user accounts in scope that have multi-factor authentication <b>not registered</b>
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></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></p>	Entra ID tenants in scope that have an administrator service password reset (SSPR) <b>disabled</b>

Vulnerability Template	Vulnerability	Risk	What to find
	Entra ID tenant(s)	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.	
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 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>	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
Entra ID Conditional Access policy sign-in risk	<p><b>Name:</b> Entra ID Conditional Access polices do not protect all users from risky sign-ins</p> <p><b>Default scope:</b> All users</p>	<p>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.</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.</p> <ul style="list-style-type: none"> <li>• In “Target resources”, “Cloud apps” set to include “All cloud apps”.</li> <li>• In “Access controls” “Grant”, set “Grant access” to “Require multi-factor authentication”.</li> <li>• In “Session”, set “Sign-in frequency” to “Every time”.</li> <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> </ul>	Entra ID user accounts in scope that do not have sign-in risk levels set to <b>high, medium</b> in an assigned Conditional Access policy

Vulnerability Template	Vulnerability	Risk	What to find
		<ul style="list-style-type: none"> <li>Service accounts and service principals (non-interactive accounts normally used by back-end services which cannot programmatically complete MFA).</li> </ul>	
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>	<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.</p> <p>Enable a Conditional Access policy for the tenant that has "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" and "Require password change".</p> <p>In "Session", set "Sign-in frequency" to "Every time".</p> <p>In Conditions, select "User risk", set "Configure" to Yes.</p> <p>Under "Configure user risk levels needed for policy to be enforced", select the "High" option.</p> <p>NOTE: Microsoft recommends excluding the following accounts from Conditional Access policies:</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
<p>Entra ID Conditional Access policy mfa status</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 Conditional Access policies do not protect all privileged users with multi-factor authentication (MFA)</p> <p><b>Default scope:</b> Privileged users</p>	<p>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.</p> <p><b>Remediation:</b></p> <p>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.</p> <p>Enable a Conditional Access policy for the tenant that has “Users or workload identities” set to include the directory roles:</p> <ul style="list-style-type: none"> <li>• Global Administrator</li> <li>• Application Administrator</li> <li>• Authentication Administrator</li> <li>• Billing Administrator</li> <li>• Cloud Application Administrator</li> </ul>	<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
		<ul style="list-style-type: none"> <li>• Conditional Access Administrator</li> <li>• Exchange Administrator</li> <li>• Helpdesk Administrator</li> <li>• Password Administrator</li> <li>• Privileged Authentication Administrator</li> <li>• Privileged Role Administrator</li> <li>• Security Administrator</li> <li>• SharePoint Administrator</li> <li>• User Administrator</li> </ul> <p>“Target resources” set to "All cloud apps",</p> <p>“Access controls” set to “Grant access, Require multi-factor authentication”</p> <p>Organizations with Security Defaults enabled will enforce MFA for privileged roles without requiring a Conditional Access policy.</p>	

Entra ID Conditional Access token protection	<p><b>Name:</b> Entra ID Conditional Access policies do not require token protection for sign-in sessions for users</p> <p><b>Default scope:</b> All users</p>	<p>Token protection attempts to reduce attacks using token theft by 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>	Entra ID user accounts in scope that do not have token protection for sign-in sessions <b>enabled</b> in an assigned Conditional Access policy
--	--	---	--

Vulnerability Template	Vulnerability	Risk	What to find
		<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>	

## 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.



**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 tenant security defaults status	<b>Name:</b> Security defaults are enabled  <b>Default scope:</b> N/A	<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 Conditional Access policies 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>	Entra ID tenants in scope that have security defaults <b>enabled</b>
Entra ID Guest account last used	<b>Name:</b> Entra ID guest user accounts that are inactive  <b>Default scope:</b> All users	<p>When external partners no longer access your tenant, the guest accounts may become stale and vulnerable to attack.</p> <p><b>Remediation:</b></p>	Entra ID user accounts in scope that were last used more than <b>90</b> days ago

Vulnerability Template	Vulnerability	Risk	What to find
<p><b>i</b> <b>NOTE:</b> For vulnerabilities that use this template, a <a href="#">premium license</a> is required</p>		Review inactive guest users, block them from signing in, and delete them from the directory.	NOTE: The number of days is editable.
Entra ID Microsoft Authenticator number matching and additional contexts status	<p><b>Name:</b> Entra ID Microsoft Authenticator policy does not require geographic location and application name contexts for all users</p> <p><b>Default scope:</b> All users</p>	<p>Microsoft has added features for strong multifactor authentication (MFA to help reduce MFA fatigue attacks and accidental MFA 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>	Entra ID user accounts in scope that do not have the Microsoft Authenticator policy assigned with geographic location and application name <b>enabled</b>
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 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>	Entra ID users in scope that <b>are</b> synchronized Active Directory users

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>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>
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</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

Vulnerability Template	Vulnerability	Risk	What to find
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>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>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 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 multifactor authentication”</p>	Entra ID user accounts in scope that do not have require multi-factor authentication <b>enabled</b> in an assigned Conditional Access policy

Vulnerability Template	Vulnerability	Risk	What to find
		<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>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>	
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>NOTE: If no Active Directory collection is available, an Inconclusive message is returned.</p>	<p>Delays in synchronization with on-premises Active Directory can be due to misconfiguration or issues with the Microsoft Entra Connect server.</p> <p><b>Remediation:</b> Login to Microsoft Entra Connect Health and review any potential sync errors.</p>	Entra ID tenants in scope that have not synchronized with on-premises Active Directory in <b>12</b> hours.

## 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	<p><b>Name:</b> More than recommended number of Global Administrators in the organization</p> <p><b>Default scope:</b> N/A</p>	<p>Users who are assigned the Global 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>Total number of Global Administrators in the organization is more than or equal to <b>5</b></p> <p>NOTE: The number of Global Administrators is editable.</p>



Vulnerability Template	Vulnerability	Risk	What to find
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.</p> <p>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 Continuous Access Evaluation disabled status	<p><b>Name:</b> Entra ID Conditional Access policy configured to disable Continuous Access Evaluation for users</p> <p><b>Default scope:</b> All users</p>	<p>Continuous access evaluation is auto enabled as part of the organization's Conditional Access policies. The key benefits of continuous access evaluation are:</p> <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> </ul>	<p>Entra ID user accounts in scope that are assigned a Conditional Access policy with Continuous Access Evaluation set to <b>disabled</b></p>

- 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.

**Remediation:**

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".

## Creating a Discovery

You can create custom Discoveries based on pre-defined vulnerability templates.



**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.



**TIP:** You can refer to Pre-defined Discoveries and Vulnerabilities for [Active Directory](#) and [Entra ID](#) for examples of Risk and Remediation text.

- 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 (Security Guardian 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.

- 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:**

- Either:
  - In the Discoveries list, select the Discovery that you want to edit.  
OR
  - Open the Discovery that you want to edit.
- 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.

## 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**.

- 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>

- Click **Save**.

## Viewing, Editing, and Deleting an Assessment

From the [All Assessments list](#), you view the details of an Assessment. 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.

## Assessment Results

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

**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

**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.




The Results page for the Assessment is divided into sections:

The first section, **Summary of Assessment Vulnerabilities**, provides 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.

-  **With Vulnerable Objects (*n*)**
-  **Without Vulnerable Objects (*n*)**
-  **With Inconclusive Results (*n*)**

The second section, **Summary of Last 7 Days**, 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

The third section contains the list of evaluated vulnerabilities, which provides the following information:

- the **Discovery Type** in which the vulnerability is defined
- the **Vulnerability** name, which links to [vulnerability-specific detail](#), including any objects the vulnerability was detected in
- the date and time when the vulnerability was **Last Detected**
  -  **NOTE:** This field displays the signed-in user's local date and time.
- the number of **Vulnerable Objects** found
  -  **NOTE:** A  icon indicates that an error occurred while the vulnerability was being evaluated.
- the 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 Detail 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](#).

### 7 Day Assessment Trend

A graph depicts color-coded results over the past 7 days that the Assessment was run, as described below.

**i TIPS:**

- You can click individual states in State Filtering so that only the states you want to focus on are displayed in the graph. (The Compliant Objects state is always hidden by default.)
- Hover over the graph to display the number of vulnerable objects (if any) detected per day.
- Click on an area of the graph to display details about that Assessment run in the list below.



**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.

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.



***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.

---

# Findings

Findings allow you to view and investigate notable events in your organization's Active Directory and/or 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 Security Guardian Assessments.
- Detected TTP and Detected Anomaly Indicators collected by Security Guardian from On Demand Audit.

**i** **NOTE:** Hygiene (from Security Guardian Assessments) indicates that objects are susceptible to an adversary attack. Detected (from On Demand Audit) indicates that an action took place that could possibly be an adversary attack. Detected TTP (tactics, techniques and procedures) are search-based detected indicators whereas Detected Anomalies are indicators based on statistical analysis.


**To view Findings:**

From the left navigation menu, choose **Security | Findings**.

The Findings list displays the following information for each finding:

- **Finding**

- one of the following **Severity** levels:

 **NOTE:** Security Guardian calculates severity levels by a range of values (i.e., 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.



**High**

- 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.


Generally reserved for the discovery of:

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


- **Type** (Tier Zero, Hygiene, Detected TTP, or Detected Anomaly)

- **Workload** (Active Directory or Entra ID)

- The date and time **Last Detected**

 **NOTE:** 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](#), you can investigate Findings in more detail for indicators of:

- [Tier Zero](#) and [Privileged](#) objects that have been identified by the provider (Security Guardian or BloodHound Enterprise) or added manually by a user.
- [Hygiene and Detected Indicators](#) that have been found through Security Guardian Assessments and On Demand Audit Critical Activity.

Click on the Finding you want to investigate.

The Investigate Finding page consists of two sections.

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

You can navigate between sections either by clicking a section 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.

### 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 (Security Guardian 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 Security Guardian is the provider, this option will be hidden.</p>
View Recent Activity	<p>This link opens the <a href="#">Quick Search page</a> in On Demand Audit, which lists event data for the selected object.</p>
<b>Escalate this Finding</b>	
Copy	<p>This link allows you to copy the text of the Finding to the clipboard so that you can share it with others.</p>
Send email	<p>This link allows you to prepare and send an escalation email to recipients with whom you want to share the Finding.</p>

#### 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 Security Guardian Assessment is run

AND/OR

- critical activity anomalies are detected by On Demand 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:

- the **Severity** of the Finding
- the Finding **Type** (Hygiene, Detected TTP, Detected Anomaly)
- the **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 **i** icon to view the additional values.
- the number of **Affected Objects**
- **Last Updated** (that is, 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.

### 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)
  - 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
<b><i>For Selected Objects in the list</i></b>	
Object Name (for a single object)	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

Link	Description
	<p>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>
Mute Object button	See <a href="#">Muting Findings for Hygiene and Detected Indicators</a> .
View Activity button (for a single object)	This link opens the <a href="#">Quick Search page</a> in On Demand Audit, which lists event data for the object being investigated.
View Assessment button (for a single object)	<p><b>If the indicator was raised by a Security Guardian Assessment</b>, this link opens the Assessment Results <a href="#">Vulnerability Detail</a> page that includes the selected object.</p> <p><b>i</b>   <b>NOTE:</b> This button is enabled only when a single object is selected.</p>
View critical activity link	<b>If the indicator was raised by an On Demand Audit critical activity event</b> , this link opens <a href="#">Critical Activity event details</a> in On Demand Audit.
<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.

## 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.

### **i** 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.

**i** **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.

**i** **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 (Security Guardian or BloodHound Enterprise) or Manually added.
- when the Finding was created by Security Guardian.

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 On Demand Audit.
- when the Finding was created by Security Guardian.
- 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).

---

# Security Settings

From the Security Guardian 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 Security Guardian 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 On Demand left navigation menu, choose **Security | 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 Security Guardian
  - Critical Activity and unprotected Active Directory Tier Zero objects collected by On Demand 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 **Security | 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 On Demand 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 On Demand left navigation menu, choose **Security | 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 - Security Guardian Indicator Details

This appendix provides details of all indicators in Security Guardian, listed both [by severity](#) and [by source](#).

**i** **NOTE:** For the general criteria Security Guardian uses to determine severity levels, refer to the topic [Managing Indicators](#).

## Indicators by Severity

The following table lists all Security Guardian indicators, from most to least severe.

Indicator	Type	Severity	Source
Possible Golden Ticket Kerberos exploit	Detected Anomaly	Critical	On Demand Audit
Unsafe encryption used in Kerberos ticket (vulnerable to Kerberoasting)	Detected TTP	Critical	On Demand 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	On Demand Audit
File changes with suspicious file	Detected Anomaly	Critical	On Demand

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
extensions			Audit
Irregular domain controller registration detected (DCShadow)	Detected Anomaly	Critical	On Demand Audit
Irregular Active Directory replication activity detected (DCSync)	Detected Anomaly	Critical	On Demand Audit
AD Database (NTDS.dit) file modification attempt detected	Detected Anomaly	Critical	On Demand 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
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 privileges (SDProp)	Hygiene	Critical	Assessments



<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
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	On Demand Audit
Domain level group policy linked changes detected	Detected TTP	Critical	On Demand 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	On Demand Audit
Tier Zero user accounts with Service Principal Names	Hygiene	Critical	Assessments
User ServicePrincipalName attribute	Detected TTP	Critical	On Demand

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
changed (vulnerable to Kerberoasting)			Aud
Non-Tier Zero user accounts with Service Principal Names	Hygiene	Critical	Assessments
Tier Zero group changes	Detected TTP	Critical	On Demand Audit
Unusual increase in failed AD changes	Detected Anomaly	Critical	On Demand Audit
Unusual increase in permission changes to AD objects	Detected Anomaly	Critical	On Demand Audit
Security changes to Tier Zero group objects	Detected TTP	Critical	On Demand Audit
Security changes to Tier Zero user objects	Detected TTP	Critical	On Demand Audit
Administrative privilege elevation detected (adminCount attribute)	Detected TTP	Critical	On Demand 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	On Demand Audit
Domain Admins can log into computers with non-Tier Zero group policy	Hygiene	Critical	Assessments
Unusual increase in failed AD Federation Services sign-ins	Detected Anomaly	Critical	On Demand Audit
Unusual increase in failed on-premises sign-ins	Detected Anomaly	Critical	On Demand Audit
Unusual increase in tenant sign-in failures	Detected Anomaly	Critical	On Demand Audit
Unusual increase in AD account lockouts	Detected Anomaly	Critical	On Demand Audit
Unusual increase in file renames	Detected Anomaly	Critical	On Demand Audit
Unusual increase in share access permission changes	Detected Anomaly	Critical	On Demand Audit
Unusual increase in file deletes	Detected Anomaly	Critical	On Demand Audit
Unusual increase in successful AD Federation Services sign-in	Detected Anomaly	Critical	On Demand Audit
Unusual increase in successful on-premises sign-ins	Detected Anomaly	Critical	On Demand Audit
Unusual increase in successful tenant sign-ins	Detected Anomaly	Critical	On Demand Audit

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
Unusual increase in successful tenant sign-ins	Detected Anomaly	Critical	On Demand Audit
Tier Zero domain and forest configuration changes	Detected TTP	Critical	On Demand Audit
Security changes to Tier Zero domain objects	Detected TTP	Critical	On Demand Audit
AD schema configuration changes	Detected TTP	Critical	On Demand Audit
Entra ID Conditional Access policy configured to disable Continuous Access Evaluation for users	Hygiene	Critical	Assessments
Entra ID Privileged risk events	Detected TTP	High	On Demand Audit
Replicating Directory Changes All domain permission granted	Detected TTP	High	On Demand Audit
New Tier Zero Domain detected	Tier Zero	High	Security Guardian
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 ECU (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

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
Tier Zero account can be delegated	Hygiene	High	Assessments
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
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	On Demand Audit
Suspicious ESX Admins group detected in domain	Hygiene	High	Assessments
Suspicious group ESX Admins created or member added	Detected TTP	High	On Demand 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
Accounts that allow Kerberos protocol transition delegation	Hygiene	High	Assessments
DNS zone configuration allows anonymous record updates	Hygiene	High	Assessments

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>	<b>Source</b>
Security changes to Tier Zero computer objects	Detected TTP	High	On Demand Audit
Tier Zero user changes	Detected TTP	High	On Demand Audit
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
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
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	On Demand Audit
Synchronized Active Directory user is	Hygiene	Medium	Assessments

Indicator	Type	Severity	Source
assigned an Entra ID privileged role			
Active Directory Tier Zero object synchronized to Entra ID	Hygiene	Medium	Assessments
Attempt to access protected Active Directory database detected	Detected TTP	Medium	On Demand Audit
Attempt to access protected Windows file or folder detected	Detected TTP	Medium	On Demand Audit
Attempt to edit protected group policy object detected	Detected TTP	Medium	On Demand Audit
Attempt to modify protected Active Directory object detected	Detected TTP	Medium	On Demand Audit
Entra ID Privileged service principal changes	Detected TTP	Medium	On Demand 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	On Demand Audit
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	On Demand Audit
New Privileged Entra ID Role Detected	Tier Zero	Medium	Security Guardian
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	Security

Indicator	Type	Severity	Source
			Guardian
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	Security Guardian
Entra ID Privileged group changes	Detected TTP	Medium	On Demand Audit
New Tier Zero Group detected	Tier Zero	Medium	Security Guardian
New Privileged Entra ID Group detected	Tier Zero	Medium	Security Guardian
New Tier Zero Computer detected	Tier Zero	Medium	Security Guardian
Entra ID Privileged user changes	Detected TTP	Medium	On Demand Audit
New Tier Zero User detected	Tier Zero	Medium	Security Guardian
New Privileged Entra ID User Detected	Tier Zero	Medium	Security Guardian
Entra ID guest 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
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

Indicator	Type	Severity	Source
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	On Demand Audit

## Indicators by Source

Security Guardian Indicators originate from the following sources:

- [On Demand Audit](#)
- [Security Guardian Assessments](#)
- [Security Guardian Tier Zero detection or protection](#)

## Indicators from On Demand Audit

The following table contains an alphabetical list of all indicators that originate from On Demand Audit.

Indicator	Indicator Type	Severity
Active Directory Database (NTDS.dit) access attempt detected	Detected TTP	Critical
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



<b>Indicator</b>	<b>Indicator Type</b>	<b>Severity</b>
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
Replicating Directory Changes All domain permission granted	Detected TTP	High
Security changes to Tier Zero computer objects	Detected TTP	High
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 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

Indicator	Indicator Type	Severity
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 Security Guardian Assessments

The following table contains an alphabetical list of all indicators that originate from Security Guardian 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

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>
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
DnsAdmins group contains members	Hygiene	Critical
DNS zone configuration allows anonymous record updates	Hygiene	High
Domain Admins can log into computers with non-Tier Zero group policy	Hygiene	Critical
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 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
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 users are allowed to consent for all applications	Hygiene	Medium

<b>Indicator</b>	<b>Type</b>	<b>Severity</b>
Foreign Security Principals are members of a Tier Zero group	Hygiene	High
Group Policy allows reversible passwords	Hygiene	High
Group Policy does not enforce built-in Administrator account lockout on all computers	Hygiene	Medium
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
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 can steal password hashes (DCSync)	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 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

Indicator	Type	Severity
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 accounts with Microsoft Local Administrator Password (LAPS) access	Hygiene	High
Non-Tier Zero accounts with Reanimate tombstones permission delegation	Hygiene	Critical
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
Non-Tier Zero Group policy contains a scheduled task	Hygiene	Medium
Ordinary user accounts with hidden privileges (SDProp)	Hygiene	Critical
Password hash synchronization with on-premises Active Directory is delayed	Hygiene	Medium
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 Authenticated Users to add computers to the domain	Hygiene	Medium
Tier Zero Group Policy allows Recovery Mode to be not password-protected	Hygiene	Critical

Indicator	Type	Severity
Tier Zero Group Policy contains a scheduled task	Hygiene	High
Tier Zero groups that have computer accounts as members	Hygiene	High
Tier Zero groups with SID History populated	Hygiene	Critical
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
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 Kerberos pre-authentication disabled	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

## Indicators from Security Guardian and Protection for Tier Zero Objects

The following table contains an alphabetical list of all indicators that originate from Security Guardian and for protection for Tier Zero objects.

Indicator	Indicator Type	Severity	Source
New Privileged Entra ID Group Detected	Tier Zero	High	Security Guardian
New Privileged Entra ID Role Detected	Tier Zero	Medium	Security Guardian
New Privileged Entra ID Service Principal Detected	Tier Zero	Medium	Security Guardian

<b>Indicator</b>	<b>Indicator Type</b>	<b>Severity</b>	<b>Source</b>
New Privileged Entra ID Tenant Detected	Tier Zero	Medium	Security Guardian
New Privileged Entra ID User Detected	Tier Zero	Medium	Security Guardian
New Tier Zero Domain detected	Tier Zero	High	Security Guardian
New Tier Zero GPO detected	Tier Zero	Medium	Security Guardian
New Tier Zero Group detected	Tier Zero	Medium	Security Guardian
New Tier Zero Computer detected	Tier Zero	Medium	Security Guardian
New Tier Zero User detected	Tier Zero	Medium	Security Guardian
Unprotected Tier Zero Domain	Tier Zero	Medium	Protection
Unprotected Active Directory Database	Tier Zero	Medium	Protection
Unprotected Tier Zero Computer	Tier Zero	Medium	Protection
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

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

## 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