Quest

Quest® Security Guardian

User Guide

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our 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.

Security Guardian User Guide
Updated - May 03, 2024

Contents

1

Introducing Quest Security Guardian

About On Demand

Quest On Demand is a Software as a Service (SaaS) application, available through 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 Azure Active Directory 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 Azure Active Directory 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) in your organization secure.

You can:

- Identify Tier Zero objects in Active Directory.
- Certify that objects are indeed Tier Zero and, when Quest Change Auditor version 7.4 is integrated, protect them against unauthorized or accidental modification or deletion.
- Run pre-defined Security Assessments to identify vulnerabilities in Active Directory and create your own Assessments.
- Investigate Findings for Tier Zero 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 a visual representation 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.

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.

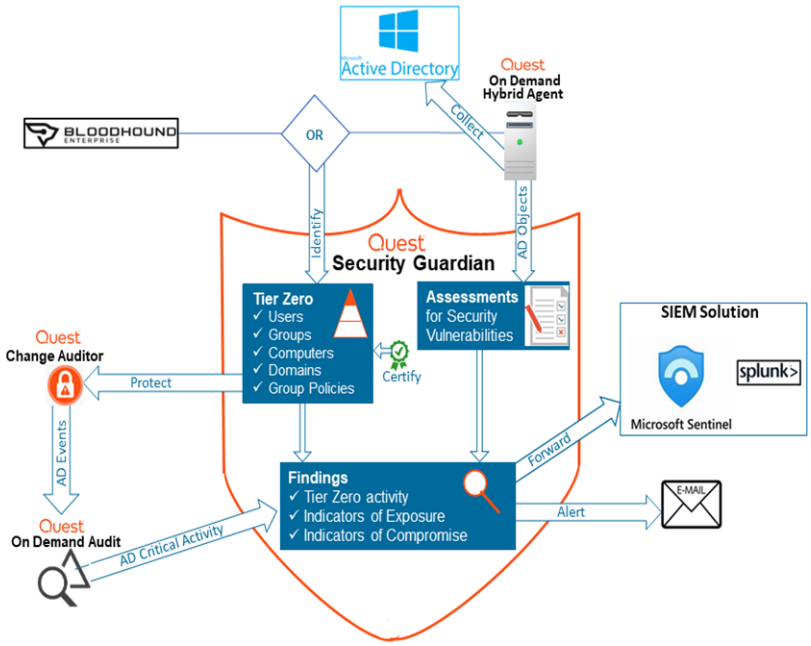
The Security Administrator role gives users full access to Security Guardian, as well as the following permissions for On Demand global settings:

- 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 diagram below illustrates how Security Guardian functions, including how additional components are integrated.



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.	On Demand Global Settings User Guide - Adding an on-premises agent

Component	Purpose	Instructions
		When configuring the agent, ensure that: • the action **Collect Active Directory object data** is selected • any domain for which you want data to be collected is added. **NOTE:** In addition to the permissions required for the hybrid agent, the service account (which the **Collect Active Directory object data** action uses) requires an additional permission to assess certain vulnerabilities.
Quest Change Auditor (via On Demand Audit)	Sends Active Directory events to On Demand Audit for reporting in Security Guardian Findings and allows you to protect Tier Zero objects. **NOTE:** 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 protect Tier Zero objects.	Instructions are provided via a tool tip in the Security Guardian UI. You can also find instructions at On Demand Audit User Guide - Change Auditor Integration
SpecterOps BloodHound Enterprise (Optional)	Identifies Tier Zero assets in your organization's Active Directory domain(s), which you can monitor and assess for security vulnerabilities in Security Guardian. **NOTE:** If BloodHound Enterprise is not configured, Security Guardian will be used as your organization's Tier Zero provider once the Hybrid Agent is configured.	On Demand Audit User Guide - Specter BloodHound Integration
SIEM solution: • Microsoft Sentinel • Splunk Cloud or Enterprise (Optional)	Allows Security Guardian Findings to be forwarded to a configured SIEM tool for further analysis **NOTE:**Regardless of whether your organization uses a SIEM solution, you can also have Finding alerts sent via email.	Configuring a Forwarding Destination

2

Using the Dashboard

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

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
- Highest Severity Findings
- Tier Zero Objects Summary
- Active Exposures and Active Compromises
- Configuration Status

The **Uncertified Tier Zero Objects** tile:

- displays the last time the Tier Zero list was synchronized
- lists the last ten uncertified Tier Zero objects of each type that were added to Security Guardian (you can click **View All** for an object type to view the complete list)

  NOTE: Tier Zero objects that have been certified are excluded from the list.

- provides links that allow you to
    - view object details (by clicking an object name)
    - **NOTE:** From within the Details view you can also certify the object. Once a Tier Zero object is certified, it will no longer display in this tile.
    - Investigate the Finding for the object
    - add a new Tier Zero object
    - if BloodHound Enterprise is configured, log into BloodHound (if you have at least Read permissions) to open the Attack Paths page
    - **NOTE:** If Security Guardian is your Tier Zero provider, this link is hidden.
    - view the Tier Zero Objects list.

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, Exposure, or Compromise)
- 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 **Tier Zero Objects Summary** tile displays a graphical representation of the number of certified vs. uncertified Tier Zero objects.

The **Active Exposures** and **Active Compromises** tile shows the total number of Indicator of Exposure and Indicator of Compromise 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. 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.

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 they are a member of a Tier Zero group (either directly or indirectly).
- **Group Policies**: May be identified as a Tier Zero if they are linked to the Domain, linked to an AD Site, or linked to an organizational unit (OU) that contains a Domain Controller or Read-Only Domain Controller.

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.

NOTE: ***If BloodHound Enterprise is configured*** ***and you see the message*** **No New Tier Zero Objects**, check the BloodHound Enterprise configuration 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

  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

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

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

From the Tier Zero Objects list, you can:

- view an object's details
- 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**

          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

  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.

NOTE: BloodHound Enterprise returns a *maximum* of 1000 related objects for each Tier Zero category.

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.

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.

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**.

   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 Indicators of Compromise and Indicators of Exposure.

By default, any object 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 privileged account security risks.

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.

You can certify one or multiple objects from the Tier Zero Objects list, or individually from the Investigate Finding page or within a New 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.

CAUTION: Once a Tier Zero object has been certified, it cannot be uncertified.

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

1. From the Tier Zero list, 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.

NOTE: Once a Tier Zero object has been certified, it will no longer display in the New Tier Zero Objects tile on the Dashboard.

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 an Indicator of Exposure or Compromise, or from the Tier Zero list.

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

  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.

4

Assessments

Assessments are a set of Discoveries that are evaluated against collected data to identify vulnerabilities in your organization's Active Directory domain(s). They run automatically once added, and then run periodically, depending on how often Active Directory data is collected. This allows you to identify which Active Directory 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

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 a built-in Assessment, Active Directory Security Assessment. It contains all pre-defined Discoveries provided by Quest and is run on all domains configured in On Demand for your organization.

NOTE: If no domains are configured for Active Directory data collection, the status message **Configuration Required** will display in the All Assessments list.

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

NOTE: A built-in Assessment 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 containing the assessed objects (with the option to **Link to Results**)
- **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

  NOTE: This status is used to indicate the absence of an Active Directory domain in On Demand for the organization. This may be because:

  - A domain has not yet been added to On Demand, which will prevent the built-in Assessment from running.
  - The domain selected for the Assessment has since been removed from On Demand.
  - When the Assessment was created, all available domains 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**

  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. Security Guardian comes with several pre-defined Discoveries and you can also create your own Discoveries.

Additional permission 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 Non-privileged accounts can access the gMSA root key, 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**.

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 Discoveries and Vulnerabilities

Quest Security Guardian comes with the following pre-defined Discoveries.

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

Discovery Type	Description
Credential Access	Techniques deployed by adversaries on systems and networks to steal usernames and credentials for re-use.
Defense Evasion	Techniques used by adversaries to avoid detection. Evasion techniques include

Discovery Type	Description
	hiding malicious code within trusted processes and folders, encrypting or obfuscating adversary code, or disabling security software.
Discovery	Techniques used by adversaries to obtain information about systems and networks that they are looking to exploit or use for their tactical advantage.
Initial Access	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.
Lateral Movement	Techniques that allow adversaries to move from one system to another within a network.
Persistence	Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
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.

Discovery for Credential Access Vulnerabilities

Vulnerability Template	Vulnerability	Risk	What to find
Users DES encryption attribute status	**Name:** User accounts using DES encryption to log in **Default scope:** All users DES	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. **Remediation:** To resolve vulnerability, in the account's Account tab - Account options, uncheck “Use only Kerberos DES encryption types for this account”.	User accounts in scope that have “Use only Kerberos DES encryption types for this account **enabled**
Account password reversible encryption status	**Name:** User accounts have a reversible password	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. **Remediation:**	User accounts in scope that have “Store password using reversible encryption” **enabled**

Vulnerability Template	Vulnerability	Risk	What to find
		To resolve vulnerability, in the account's Account tab - Account options, uncheck “Store password using reversible encryption”.	
	Name: Computer accounts with reversible password **Default scope:** All computers	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. **Remediation:** 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.	Accounts in scope that have "Store password using reversible encryption" enabled
Users Kerberos preauthentication status	**Name:** User accounts with Kerberos pre-authentication disabled **Default scope:** All users	User accounts with Kerberos pre-authentication disabled can be compromised as part of ASREP-Roasting attacks. **Remediation:** To resolve vulnerability, in the account’s Account tab - Account options, uncheck "Do not require Kerberos preauthentication".	User accounts in scope that have “Do not require Kerberos preauthentication” **enabled**
Users Service Principal Name status	**Name:** Non-privileged user	User accounts with Service	User accounts in scope that have “Service Principal

Vulnerability Template	Vulnerability	Risk	What to find
	accounts with Service Principal Names **Default scope:** All except Tier Zero users	Principal Names (SPNs) defined are exposed to Kerberos-based authentication attacks, providing an adversary with an entry point to the directory. **Remediation:** 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.	Name" **not empty**
Users delegated account attribute status	**Name:** Administrator account can be delegated **Default scope:** Tier Zero users	Administrator accounts that are not configured to disallow delegation can be delegated and taken control of by an adversary. **Remediation:** To resolve vulnerability, ensure that administrator accounts are configured so that the "This account is sensitive and cannot be delegated" option is enabled and that the accounts are also added as members to the Protected Users group.	User accounts in scope which have "This account is sensitive and cannot be delegated" **disabled** and are not members of the "Protected Users" group
Users Password Never Expires status	**Name:** Non-privileged user accounts configured for Password Never Expires **Default scope:** All except Tier Zero users	User accounts with passwords that are not cycled regularly are more susceptible to brute force password cracking attempts. Accounts that are configured to never require a password change should be remediated accordingly. **Remediation:** To resolve vulnerability, set	User accounts in scope that have "Password Never Expires" **enabled**

Vulnerability Template	Vulnerability	Risk	What to find
		the “Don’t Expire Password” option on the user account to “disabled” and enforce the organizations password policy	
	Name: Privileged user accounts configured for Password Never Expires **Default scope:** 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. **Remediation:** To resolve vulnerability, on the user Properties Account tab, make sure Password never expires is unchecked.	
Protected Users group membership status	**Name:** Protected Users group is not being used **Default scope:** Tier Zero users	The Protected Users group should be used to protect privileged user accounts from attacks to steal their credentials. If the group is not in use, privileged accounts are exposed to possible credential theft. **Remediation:** Members of the Protected Users group are blocked from using NTLM authentication. Therefore, do not add privileged users to the Protected Users group if they require access to resources that require NTLM to authenticate. In addition, accounts for services and computers should never be members of the Protected Users group as it will cause authentication to fail. To resolve this vulnerability, consider adding any privileged account that does	User accounts in scope that **are not** members of the “Protected Users” group

Vulnerability Template	Vulnerability	Risk	What to find
		not require NTLM and is not a service account to the Protected Users group.	
Account last used	**Name:** Enabled privileged user accounts that are inactive **Default scope:** Tier Zero users	The number of privileged accounts in a domain should be limited and closely monitored. Privileged 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. **Remediation:** 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.	Accounts in scope that were last used **more than 90** days ago NOTE: The number of days is editable.
	Name: Privileged computers that have not recently authenticated to the domain **Default scope:** Tier Zero computers	Privileged 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. **Remediation:** Privileged computers that are offline for extended periods of time should be investigated. Domain controllers that are out of sync with the domain over 30 days should be reinstalled or removed.	Accounts in scope that were last used **more than 30** days ago NOTE: The number of days is editable.
Domain controller SMBv1 protocol status	**Name:** Domain Controller is running SMBv1 protocol	The SMBv1 protocol supports legacy insecure authentication protocols. If	Computers in scope that have the SMBv1 protocol enabled

Vulnerability Template	Vulnerability	Risk	What to find
NOTE: For vulnerabilities that use this template, the hybrid agent service account must be a member of the **Domain Admins** group.	**Default scope:** N/A	running, it can allow an adversary to access a domain controller and harvest credentials or execute commands. **Remediation:** Disable the SMBv1 protocol on the impacted domain controllers.	
Domain controller Print Spooler status **NOTE:** For vulnerabilities that use this template, the hybrid agent service account must be a member of the **Domain Admins** group.	**Name:** Printer Spooler service is enabled on a domain controller **Default scope:** N/A	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. **Remediation:** Disable the Printer Spooler service on all domain controllers.	Domain controller that has the Print Spooler service **enabled**
Group Policy "Store passwords using reversible encryption" setting	**Name:** Group Policy allows reversible passwords **Default scope:** All Group Policies	Group Policies containing reversible passwords are an attractive target as those passwords can be easily decrypted and used to elevate an adversary's privileges. **Remediation:** Configure the "Store passwords using reversible encryption" setting located in “Computer Configuration - Policies - Windows Settings - Security Settings - Account Policies - Password Policy” section of the Group Policy to “disabled”. There are a	Group Policy objects in scope that have "Store passwords using reversible encryption" **enabled**

Vulnerability Template	Vulnerability	Risk	What to find
		couple of use cases where this setting would be enabled: Challenge Handshake Authentication Protocol (CHAP) for remote access or Internet Authentication Services (IAS), Internet Information Services (IIS) Digest Authentication Disabling this setting could break these applications. If this is needed for backwards compatibility the recommendation is to apply this to a single user or smallest subset of users vs the full domain.	
Domain "Replicating Directory Changes All" and "Replicating Directory Changes" delegation	**Name:** Non-privileged accounts can steal password hashes (DCSync) **Default scope:** All except Tier Zero accounts	If non-privileged 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. **Remediation:** These delegations should be removed unless there is a compelling reason for their existence.	Domain has "Replicating Changes All" and "Replicating Directory Changes" set to **Allow** for any accounts in scope
Object read-only domain controller msDS-NeverRevealGroup status	**Name:** Protected group credentials exposed on read-only domain controllers **Default scope:** • Administrators • Account Operators • Backup Operators	Read-only domain controllers (RODCs) should be configured so that privileged user and group credentials are not replicated. If privileged passwords are replicated, an adversary who gains access to the RODC can harvest the credentials and elevate their privileges. **Remediation:**	Objects in scope are **not listed** in the read-only domain controller "msDS-NeverRevealGroup" attribute

Vulnerability Template	Vulnerability	Risk	What to find
	• Denied RODC Password Replication Group • Server Operators	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.	
RODC password replication policy	**Name:** Privileged account token can be stolen from a read-only domain controller **Default scope:** All groups except Allowed RODC Password Replication	Read-only domain controllers (RODCs) should be configured so that privileged user and group credentials are not replicated. If privileged passwords are replicated, an adversary who gains access to the RODC can harvest the credentials and elevate their privileges. **Remediation:** 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.	Objects in scope are listed in the read-only domain controller “msDS-RevealOnDemandGroup” attribute
Account password last changed	**Name:** Managed and Group Managed Service accounts that have not cycled their password recently **Default scope:** All Service Accounts	Managed Service Accounts (MSA) and Group Managed Service accounts (gMSA) that have not had their passwords cycled recently could indicate they've been compromised. **Remediation:** The reason that prevented the managed service	Accounts in scope that have not updated its password within last **30** days. NOTE: The number of days is editable.

Vulnerability Template	Vulnerability	Risk	What to find
		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.	
Computer account ms-Msc-AmdPwd attribute permissions	**Name:** Non-default configuration of the Microsoft Local Administrator Password **Default scope**: All except Domain Admins	An incorrectly configured Microsoft Local Administrator Password (ms-Msc-AmdPwd attribute) can expose the local Administrator password for an adversary to steal. Confidential attributes can only be viewed by Domain Admins by default, and unlike other attributes, is not accessible by Authenticated Users. **Remediation:** Review accounts that can view the “ms-mcs-AdmPwd” attribute of a computer account and determine if the access is required. If not required, change the value to Deny read.	Computer ms-Msc-AmdPwd attribute has **Allow Read** set for any account in scope
User permission on Resource-Based Constrained Delegation settings for KRBTGT	Non-privileged user accounts with write permissions over Resource-Based Constrained Delegation on the KRBTGT account **Default scope:** All except Tier Zero users	Non-privileged user accounts that have the permission to write Resource-Based Constrained Delegation (RBCD) on the KRBTGT account can allow an adversary to impersonate any user and take control of the KRBTGT account, and from there, the entire domain. **Remediation:** To resolve vulnerability, review the KRBTGT object	Users in scope that have **Allow Write** permission on Resource-Based Constrained Delegation settings for KRBTGT account

Vulnerability Template	Vulnerability	Risk	What to find
		security to determine if non-privileged user accounts should have Write permissions in the Resource-Based Constrained Delegation attribute. If not required, remove them.	
Privileged computers permission granted on Resource-Based Constrained Delegation	**Name:** Privileged computer that has write permissions on Resource-Based Constrained Delegation granted to a non-privileged account **Default scope:** All except Tier Zero objects	Non-privileged accounts that have the permission to write Resource-Based Constrained Delegation (RBCD) on a privileged computer such as a domain controller can allow an adversary to impersonate any user and take control of the DC. **Remediation:** To resolve vulnerability, review the privileged computer security to determine if non-privileged user accounts should have Write permissions in the Resource-Based Constrained Delegation attribute. If not required, remove Write permissions on the attribute.	Privileged computers that have accounts in scope with **Allow Write** permission on Resource-Based Constrained Delegation
gMSA root key access **NOTE:** For vulnerabilities that use this template, the hybrid agent service account must be a member of the **Domain Admins** or **Enterprise Admins** group.	**Name:** Non-privileged accounts can access the gMSA root key **Default scope**: All except Tier Zero objects	Non-privileged accounts with access to the Group Key Distribution Services Master Root Keys could gain access to any gMSA account in the environment.	Accounts in scope that have **Allow Read or Allow Write** permission for msKds-RootKeyData attribute on msKds-ProvRootKey objects

Vulnerability Template	Vulnerability	Risk	What to find
		NOTE: For Assessment results to be returned for this vulnerability, the account under which the agent service is run must have Domain Admin or Enterprise Admin permissions to read the msKds-ProvRootKey objects in Active Directory **Remediation:** Restrict access to the msKds-ProvRootKey objects in the domain to only privileged users and groups. The default groups that have access to the objects are SYSTEM, Domain Admins, and Enterprise Admins.	
Write access on certificate templates	**Name**: Non-privileged accounts have access to write properties on certificate templates **Default scope:** All except Tier Zero users and groups and Foreign Security Principal (S-1-5-9)	Non-privileged 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. A template is misconfigured at the access control level if it has Access Control Entries (ACEs) that allow unintended, or otherwise non-privileged, AD principals to edit sensitive security settings in the template. **Remediation:** Remove non-privileged users from having any write access to “Certificate Templates” container in Configuration - Services - Public Key Services or any	Accounts in scope have **WriteOwner, WriteDacl or WriteProperty** permissions on NTAuthCertificates objects in the “Certificate Templates” container

Vulnerability Template	Vulnerability	Risk	What to find
		pKICertificateTemplate object in that container.	
AdminSDHolder inheritance status	**Name:** Inheritance is enabled on the AdminSDHolder container **Default scope:** N/A	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 privileged accounts easier for them. **Remediation:** 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”.	AdminSDHolder permission inheritance set to **enabled**
User access to gMSA password	**Name:** Non-privileged users with access to gMSA password **Default scope:** All except Tier Zero users	Non-privileged 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. **Remediation:** Unless there is a business reason, remove non-privileged users from the group that is listed in the Group Managed Service Account’s (gMSA) msDS-groupMSAMembership attribute.	Users in scope that **are** able to retrieve the password for a Group Managed Service Account (gMSA)
Domain trust Kerberos AES encryption support status	**Name:** Domain trust without Kerberos AES encryption enabled	The setting “The other domain supports Kerberos AES Encryption” determines whether the trust supports	Domain trust in scope has Kerberos AES encryption support **disabled**

Vulnerability Template	Vulnerability	Risk	What to find
	Default scope: All Trusted Domains	AES encryption. Trusts that do not have the setting enabled will use RC4 encrypted Kerberos tickets which are considered significantly less secure than AES. **Remediation:** 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".	
KRBTGT account password last changed	**Name:** Kerberos KRBTGT account password has not changed recently **Default scope:** N/A	The KRBTGT account is a domain default account that acts as a service account for the Key Distribution Center (KDC) service. During the Kerberos Authentication process, TGTs are issued to accounts requesting access to resources. These TGTs are encrypted by cryptographic key which is derived from the password of the KRBTGT account. In many Active Directory environments, the password for the KRBTGT account has not been changed since before moving to the 2008 domain functional level. This means that the password is not AES encrypted, which	Kerberos KRBTGT account password has not been updated within the last **180** days

Vulnerability Template	Vulnerability	Risk	What to find
		can expose the account to attack and break trusts with forests that require AES encryption. **Remediation:** There is no specific recommendation from Microsoft regarding password reset frequency for the KRBTGT account, but security organizations recommend that it be reset periodically. 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.	

Discovery for Defense Evasion Vulnerabilities

Vulnerability Template	Vulnerability	Risk	What to find
Built-in Administrator account last used	**Name:** Built-in Administrator account that has been used **Default scope:** N/A	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. **Remediation:** 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.	Built-in Administrator account was last used less than **30 days** ago NOTE: The number of days is editable.
Members of protected groups adminCount attribute value	**Name:** User accounts in protected	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	User objects in scope that are members of protected groups and have

Vulnerability Template	Vulnerability	Risk	What to find
	groups that are not protected by AdminSDHolder (SDProp) **Default scope:** All users	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: • Account Operators (S-1-5-32-548) • Administrators (S-1-5-32-544) • Backup Operators (S-1-5-32-551) • Cert Publishers (S-1-5-domain-517) • Domain Admins (S-1-5-domain-512) • Domain Controllers (S-1-5-domain-516) • Enterprise Admins (S-1-5-root_domain-519) • Read-only Domain Controllers (only since Windows Server 2008) (S-1-5-domain-521) • Replicator (S-1-5-32-552) • Schema Admins (S-1-5-root_domain-518) • Server Operators (S-1-5-32-549) **Remediation:** 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.	adminCount attribute set to **0 or not set.**
Account Primary Group ID permissions	**Name:** User accounts without readable Primary Group ID **Default scope:** All users	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. **Remediation:** To resolve vulnerability, review the User object and remove any Deny Read permissions which would prevent the Primary Group ID from being read.	Accounts in scope that have **Deny Read** set for the "Primary Group ID" attribute
	Name: Computer accounts without readable Primary Group ID **Default scope:** All computers	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. **Remediation:** To resolve vulnerability, review the computer object and remove any Deny read permissions which would prevent the Primary Group ID attribute from being read.	

Vulnerability Template	Vulnerability	Risk	What to find
Active Directory Operator group AdminSDHolder protection status	**Name:** Active Directory Operator groups that are not protected by AdminSDHolder **Default scope:** N/A	The AdminSDHolder object maintains a template of permissions that are automatically applied to privileged 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: • Account Operators • Server Operators • Print Operators • Backup Operators. **Remediation:** 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.	The dsHeuristics attribute on the Directory Service object indicates **some Operator groups** are excluded from AdminSDHolder protection

Discovery for Discovery Vulnerabilities

Vulnerability Template	Vulnerability	Risk	What to find
Account password last changed	Name: Built-in Guest account is enabled Default scope: N/A	The built-in Guest account enables access to Active Directory without requiring a password and should be disabled. **Remediation:** To resolve vulnerability, disable the built-in Guest account (if it has been renamed, the account whose SID is S-1-5-domain-501).	Built-in Guest accounts that are enabled

Discovery for Initial Access Vulnerabilities

Vulnerability Template	Vulnerability	Risk	What to find
Built-in Guest account status	**Name:** Built-in Guest account is enabled **Default scope:** N/A	The built-in Guest account enables access to Active Directory without requiring a password and should be disabled. **Remediation:** To resolve vulnerability, disable the built-in Guest account (if it has been renamed, the account whose SID is S-1-5-domain-501).	Built-in Guest accounts that are **enabled**
Anonymous access to Active Directory status	**Name:** Anonymous access to Active Directory is enabled **Default scope:** N/A	Anonymous access allows accounts to perform reconnaissance against Active Directory by binding to Active Directory over RPC (including over Name Service Provider Interface (NSPI)) without authenticating. Anonymous access to Active Directory is enabled using the fLDAPBlockAnonOps bit in the dsHeuristics attribute of CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration, DC=domain,DC=com. **Remediation:** Set the 7th character (fLDAPBlockAnonOps bit) of the dsHeuristics attribute to 0 to ensure that anonymous access is blocked. The dsHeuristics attribute is located on the Directory Service object in CN=WindowNT,CN=Services,CN=Configuration, DC=domain,DC=com.	The dsHeuristics attribute on the Directory Service object indicates Anonymous access to Active Directory is **enabled**

Discovery for Lateral Movement Vulnerabilities

Vulnerability Template	Vulnerability	Risk	What to find
Account Trusted for Delegation attribute status	**Name:** User accounts with unconstrained delegation **Default scope**: All users	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. **Remediation:** 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	Accounts in scope that have Trusted for Delegation **enabled**

Vulnerability Template	Vulnerability	Risk	What to find
		not selected. If a Kerberos delegation is required, use one that is constrained.	
	Name: Computer accounts with unconstrained delegation **Default scope:** All computers except domain controllers	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. **Remediation:** 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.	Accounts in scope that have Trusted for Delegation **enabled**
Users Password Not Required attribute status	**Name:** User accounts do not require a password **Default scope:** All users	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. **Remediation:** To resolve vulnerability, in the account's Attribute Editor tab, select userAccountControl and remove the PASSWD_NOTREQD value.	User accounts in scope that have "Password not required" **enabled**
Domain Add computers to domain value	**Name:** Non-privileged users can create computer accounts **Default scope**: N/A	Without hardening, non-privileged users have the ability to create computer accounts in the domain. Improperly configured computer accounts are exposed to Kerberos authentication attacks. Only administrators should be able to add new computer accounts. **Remediation:** 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-privileged users from being able to register new computer accounts within the domain.	Domain has the "ms-DS-MachineAccountQuota" attribute set to **more than 0** NOTE: The operator and quota attribute value are editable.
Account "Use any authentication protocol" status	**Name:** Accounts that allow Kerberos	A service configured to allow Kerberos protocol transition will allow a delegated service to use any available authentication	Accounts in scope which have "Use any authentication protocol" **enabled** in delegation

Vulnerability Template	Vulnerability	Risk	What to find
	protocol transition delegation **Default scope:** All users and computers	protocol. This can result in reduced authentication security and increase the chance of services being compromised by an adversary. **Remediation:** In the account Properties -Delegation tab, ensure configured delegation is not set to “Use any authentication protocol.”	
Domain Unexpire Password permission delegation	**Name:** Non-privileged accounts with Unexpire password permission delegation **Default scope:** 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 privileged principal. **Remediation:** 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 **Allow** for any accounts in scope
Domain Migrate SID history permission delegation	**Name:** Non-privileged accounts with Migrate SID history permission delegation **Default scope:** All except Tier Zero users and groups	If the “Migrate SID history” permission is delegated an adversary can use it to elevate their privileges by adding a privileged account to their sIDHistory attribute and obscuring the exploit. **Remediation:** Except for the Domain Admins group, these delegations should be removed unless there is a compelling reason for their existence.	Domain has “Migrate SID history” set to **Allow** for any accounts in scope
Domain Reanimate tombstones permission delegation	**Name:** Non-privileged accounts with Reanimate tombstones permission delegation	If the “Reanimate tombstones” control access right is delegated an adversary could use it to restore and take control of a privileged object. **Remediation:** Except for the Domain Admins group, these delegations should be removed unless there is a compelling reason for their existence.	Domain has “Reanimate tombstones” set to **Allow** for any accounts in scope

Vulnerability Template	Vulnerability	Risk	What to find
	Default scope: All except Tier Zero users and groups		

Discovery for Persistence Vulnerabilities

Vulnerability Template	Vulnerability	Risk	What to find
Foreign Security Principals privileged group membership status	**Name:** Foreign Security Principals are members of a privileged group **Default scope:** N/A	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. Foreign security principals can be added to privileged 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. **Remediation:** Investigate Foreign Security Principals that are members of the protected groups and remove the membership if appropriate.	Foreign Security Principals in scope that **are** members of a privileged group

Discovery for Privilege Escalation Vulnerabilities

Vulnerability Template	Vulnerability	Risk	What to find
Account Primary Group ID	**Name:** User accounts with non-default Primary Group	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. **Remediation:**	Accounts in scope that have a “Primary Group” that is not **Domain Users** or **Domain Guests**

Vulnerability Template	Vulnerability	Risk	What to find
	IDs **Default scope:** All users	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).	
	Name: Computer accounts with non-default Primary Group IDs Default scope: All computers	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. **Remediation:** • The Primary Group ID should be reset to its default value. The default primary group for computer accounts is: • "Domain Computers" (515) • for domain controller accounts, "Domain Controllers" (516) • for read-only domain controllers, "Read-only Domain Controllers" (521).	Accounts in scope that have a “Primary Group” that is not **Domain Computers** or **Domain Controllers or Read-Only Domain Controllers**
Users Service Principal Name status	**Name:** Privileged user accounts with Service Principal Names **Default scope**: Tier Zero users	Privileged 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. **Remediation:** 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. 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.	User accounts in scope that have “Service Principal Name” **not empty**
Number of privileged user accounts	**Name:** Abnormally large number of privileged user accounts in the domain	The number of privileged accounts in a domain should be limited and closely monitored. An abnormally high number of privileged accounts could indicate loose permissioning or group nesting which should be addressed. Tier Zero user accounts are being evaluated for this	Total number of privileged user accounts within a domain is **more than 20**

Vulnerability Template	Vulnerability	Risk	What to find
	Default scope: N/A	vulnerability. **Remediation:** To resolve vulnerability, identify accounts that should not have privileged user credentials and remove those credentials. Resolve any group nesting issues.	
Account SID History status	**Name:** Privileged user accounts with SID History populated **Default scope:** Tier Zero users	If a user account's sIDHistory attribute is populated, then the account has all the privileges that belong to the SID History as well. Privileged 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. **Remediation:** To resolve vulnerability, remove the references in SID History if the user no longer requires the permissions assigned to the security groups listed. If the permissions are required, add the permission or group membership directly to the user object.	Accounts in scope that have SID History **not empty**
	Name: Privileged groups with SID History populated **Default scope:** Tier Zero groups	If a group's sIDHistory attribute is populated, the group members have the privileges that belong to the SID History as well. Privileged 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. **Remediation:** To resolve vulnerability, remove the references in sIDHistory if the group no longer requires the permissions assigned to the security groups listed. If the permissions are required, add the permission or group membership directly to the group object.	
Account SID History local SID status	**Name:** User accounts with SID from local domain in their SID History **Default**	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	Accounts in scope that **have** SID from local domain in their SID History

Vulnerability Template	Vulnerability	Risk	What to find
	scope: All users	compromised the account and granted themselves more privilege than is immediately visible. **Remediation:** To resolve vulnerability, immediately remove the local SID from the compromised user's sIDHistory attribute and investigate who modified the attribute and when.	
	Name: Groups with SID from local domain in their SID History **Default scope**: All groups	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. **Remediation:** To resolve vulnerability, immediately remove the local SID from the compromised group's sIDHistory attribute and investigate who modified the attribute and when.	
User account status	**Name:** Privileged user account is disabled **Default scope:** Tier Zero users	The number of privileged accounts in a domain should be limited and closely monitored. A privileged account that is disabled but still contains privileges through privileged group membership can be compromised by an adversary and used to elevate privileges. **Remediation:** Remove privileged group membership from user accounts that are disabled.	Users in scope that are **disabled**
Group Members Count	**Name:** Privileged groups which should not be in use contain members **Default scope:** Account Operators	Privileged 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. **Remediation:** Remove the members within privileged groups: • Account Operators (S-1-5-32-548)	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
	Backup Operators Cryptographic Operators Hyper-V Administrators Network Configuration Operators Print Operators Remote Desktop Users Replicator Server Operators	• Backup Operators (S-1-5-32-551) • Cryptographic Operators (S-1-5-32-569) • Hyper-V Administrators (S-1-5-32-578) • Network Configuration Operators (S-1-5-32-556) • Print Operators (S-1-5-32-550) • Remote Desktop Users (S-1-5-32-555) • Replicator (S-1-5-32-552) • Server Operators (S-1-5-32-549) NOTE: The Hyper-V Administrators group may have members If a Hyper-V environment is used.	
Schema Admins Group Member Count	**Name:** Schema Admins group contains members **Default scope**: N/A	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. **Remediation:** Remove the members within Schema Admins.	Schema Admins group has **more than 0** members NOTE: The operator and number of days are editable.
Non-members of protected groups adminCount attribute value	**Name:** Ordinary user accounts with hidden privileges (SDProp) **Default scope:** All users	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: • Account Operators (S-1-5-32-548)	User objects in scope that are not members of protected groups and have adminCount attribute set to 1

Vulnerability Template	Vulnerability	Risk	What to find
		• Administrators (S-1-5-32-544) • Backup Operators (S-1-5-32-551) • Cert Publishers (S-1-5-21-<domain>-517) • Domain Admins (S-1-5-21-<domain>-512) • Domain Controllers (S-1-5-21-<domain>-516) • Enterprise Admins (S-1-5-21-<root_domain>-519) • Read-only Domain Controllers (only since Windows Server 2008) (S-1-5-21-<domain>-521) • Replicator (S-1-5-32-552) • Schema Admins (S-1-5-21-<root_domain>-518) • Server Operators (S-1-5-32-549) **Remediation:** 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.	
Verify group membership of DnsAdmins group	**Name:** DnsAdmins group contains members **Default scope:** All users	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 privileged Active Directory administrators are suspicious and increase the attack surface. **Remediation:** Review the members of the DnsAdmins group, determine if any members are not highly privileged Active Directory administrators, and remove them if appropriate.	DnsAdmins group has more than **0** members

Vulnerability Template	Vulnerability	Risk	What to find
Anonymous Logon and Everyone groups are members of Pre-Windows 2000 Compatible Access group	**Name:** Anonymous Logon and Everyone groups are members of the Pre-Windows 2000 Compatible Access group **Default scope:** N/A	The default permissions on many AD objects are set to allow access to the Pre-Windows 2000 Compatible Access group. If wide-open groups such as Everyone (S-1-1-0) or Anonymous Logon (S-1-5-7) are members of the Pre-Windows 2000 Compatible Access group, it creates exposure for an adversary to escalate their privileges. **Remediation:** Remove wide open groups Everyone (S-1-1-0) and Anonymous Logon (S-1-5-7) from the Pre-Windows 2000 Compatible Access group (S-1-5-32-554).	Pre-Windows 2000 Compatible Access group **contains** Anonymous Logon and Everyone groups
Privileged user account ownership	**Name:** Privileged users owned by non-privileged accounts **Default scope:** N/A	The owner of an object can take control over the object and have all of its permissions. A non-privileged user having ownership over a privileged account can be evidence of tampering and represents an abusable attack path for an adversary. **Remediation:** Remove the non-privileged user ownership on the privileged user account and investigate who modified the owner and when.	Privileged user accounts that are owned by **a non-privileged account**
Privileged computer account ownership	**Name:** Privileged computer is owned by a non-privileged account **Default scope:** N/A	The owner of an object can take control over the object and therefore has all of its permissions. In cases where a Domain Controller was promoted after the Windows Server was provisioned, it is possible that a group belonging to the server infrastructure team still owns the computer. If a Domain Controller account is not under the ownership of either the Enterprise Admins, Domain Admins or Administrator account then it is exposed to being compromised and its password hashes stolen. **Remediation:** Update the owner of the Domain Controller to the Domain Admins group or update other Tier Zero computers to Tier Zero owners.	Privileged computer accounts that are owned by a **non-privileged account**
Account password last changed	**Name:** Privileged computer	Privileged computers such as domain controllers will change their computer account password periodically (30 days by default).	Accounts in scope that have not updated its password within

Vulnerability Template	Vulnerability	Risk	What to find
	accounts that have not cycled their password recently **Default scope:** Tier Zero computers	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. **Remediation:** 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: • HKLM\System\CurrentControlSet\Services\ Netlogon\Parameters\ DisablePasswordChange must be 0 or not exist • HKLM\System\CurrentControlSet\Services\ Netlogon\Parameters \MaximumPasswordAge should be 30 If these values are incorrect, they should be reset to the default values and ensure that they are not set by a GPO.	last **30 days**. NOTE: The number of days is editable.
Group Policy "Recovery console: Allow automatic administrative logon" setting	**Name:** Privileged Group Policy allows Recovery mode to be not password-protected **Default scope:** Tier Zero Group Policies	An unprotected Recovery Mode allows an adversary with physical access to a domain controller the ability to gain access to the Active Directory database. **Remediation:** 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”	Group Policy objects in scope "Recovery console: Allow automatic administrative logon" is **enabled**
Privileged computer Group Policy "Allow log on” settings	**Name:** Non-privileged accounts are able to log onto privileged computers **Default**	If a non-privileged user is able to log onto a privileged computer, such as a Domain Controller, locally or by remote session, they can execute code or obtain a copy of all password hashes. **Remediation:** Prevent non-privileged users from logging into	Accounts in scope added to Allow log on locally or **Allow log on through Remote Desktop Services** in privileged Group Policy

Vulnerability Template	Vulnerability	Risk	What to find
	scope: All except Tier Zero users, groups and computers	privileged computers by removing the "Allow log on locally" and "Allow log on through Remote Desktop Services" rights for any non-privileged group. These settings are located in Computer configuration - Policies - Windows Settings - Security Settings - Local Policies - User Rights Assignment.	
Non-privileged Group Policy "Deny log on" for Domain Admin status	**Name:** Domain Admins can log into computers with non-privileged Group Policy **Default scope:** All except Tier Zero Group Policies	When a privileged account logs into a non-privileged computer, their password hash remains in memory and can be harvested by an adversary. If Group Policies do not prevent Domain Admin logons to lower tiers, privileged credentials could be exposed. **Remediation:** Restrict logons to all non-privileged 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.	Group Policies in scope that do not have Domain Admins group added to the **Deny log on locally or Deny log on through Remote Desktop Services** setting
DNS zone dynamic updates status **NOTE:** For vulnerabilities that use this template, the hybrid agent service account must be a member of the **Domain Admins** group.	**Name:** DNS zone configuration allows anonymous record updates **Default scope**: N/A	Dynamic DNS records are created by DNS clients or systems on behalf of DNS clients (Example: DHCP servers). On Microsoft DNS servers, there are three possible configurations for dynamic updates: "None", "Nonsecure and secure", "Secure only". The "Nonsecure and secure" setting allows dynamic updates to be accepted without checking if the source of updates is trusted or not. DNS zones configured to allow anonymous record updates can be exploited by adversaries to receive incoming queries and harvest credentials. **Remediation:** 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.	DNS zone dynamic updates set to **Nonsecure** and **secure**

Vulnerability Template	Vulnerability	Risk	What to find
Computer Resource-Based Constrained Delegation status	**Name:** Privileged computer can be compromised through Resource-Based Constrained Delegation **Default scope:** Tier Zero computers	If Kerberos Resource-Based Constrained Delegation (RBCD) is enabled on a privileged computer such as a domain controller, an adversary can leverage this to elevate from a system under their control to a privileged computer and take effective control over the entire domain. **Remediation:** To resolve vulnerability, in the impacted computer's Delegation tab, select "Do not trust this computer for delegation". 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 <computer>" portion of the command will need to be updated to reflect the display name of the computer account being checked): Get-ADComputer -Identity <computer> -Properties PrincipalsAllowedToDelegateToAccount	Computer accounts in scope for which Resource-Based Constrained Delegation **has values**
	Name: Non-privileged computer can be compromised through Resource-Based Constrained Delegation **Default scope:** All except Tier Zero computers	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. **Remediation:** To resolve vulnerability, in the impacted computer's Delegation tab, select "Do not trust this computer for delegation". 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 <computer>" portion of the command will need to be updated to reflect the display name of the computer account being checked): Get-ADComputer -Identity <computer> -Properties PrincipalsAllowedToDelegateToAccount	
Domain Write Group Policy Object link delegation	**Name:** Non-privileged accounts can link GPOs to	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	Domain has the "Write gPLink" set to **Allow** for any accounts in scope

Vulnerability Template	Vulnerability	Risk	What to find
	the domain **Default scope:** All except Tier Zero users and groups	(GPO) at the domain level they can effectively take over the entire domain. **Remediation:** These delegations should be removed for any non-privileged unless there is a compelling reason for their existence.	
Domain promote a computer to a domain controller delegation	**Name:** Non-privileged accounts that can promote a computer to a domain controller **Default scope**: All except Tier Zero users and groups	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. **Remediation:** The "Add/remove replica in domain" delegation should be removed from any non-privileged account unless there is a compelling reason for its existence.	Domain has “Add/remove replica in domain” set to **Allow** for any account in scope
Active Directory Site Write gPLink delegation	**Name:** Non-privileged accounts can link Group Policy Objects to an Active Directory site **Default scope:** 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 an Active Directory site, they can directly control all objects it contains. **Remediation:** These delegations should be removed unless there is a compelling reason for their existence.	Active Directory Site has “Write gPLink” set to **Allow** for any accounts in scope
Domain Controller OU Write gPLink delegation	**Name:** Non-privileged accounts can link Group Policy Objects to Domain Controller OU	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. **Remediation:**	Domain Controllers OU has “Write gPLink” set to **Allow** for any accounts in scope

Vulnerability Template	Vulnerability	Risk	What to find
	Default scope: All except Tier Zero users and groups	These delegations should be removed unless there is a compelling reason for their existence.	
Computer account group membership status	**Name:** Privileged groups that have computer accounts as members **Default scope:** Tier Zero groups	If a computer account is a member of a privileged group, an adversary who compromises the computer will also elevate their privileges to the privileged group the computer belongs to. Vulnerable objects will not be returned when any computer is a member of Cert Publishers or when a DC\RODC is a member of Domain Controllers, Enterprise Domain Controllers, Read-only Domain Controllers, or Enterprise Read-only Domain Controllers. **Remediation:** Review computer account privileged group membership to determine if the computer should be a member of the privileged group. If not required, remove the account from the group.	Groups in scope that **have** computer accounts as members
KRBTGT account resource-based constrained delegation status	**Name:** KRBTGT accounts with Resource-Based Constrained Delegation **Default scope**: N/A	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. **Remediation:** 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	KRBTGT accounts that **have** Resource-Based Constrained Delegation configured

Vulnerability Template	Vulnerability	Risk	What to find
Domain trust configured insecure status	**Name:** Domain trust configured insecurely **Default scope:** Dependent on the domain(s) selected when an Assessment is created. If a selected domain does not have a trust, it will not be assessed for the vulnerability.	Trusts that have insecure settings are exposed to Kerberos-based authentication vulnerabilities or reduced protection against imposter identities. • A domain trust is considered insecure if it has the trustAttribute TRUST_ ATTRIBUTE_CROSS_ ORGANIZATION_ENABLE_TGT_ DELEGATION (0x00000800) bit enabled. • A domain Privileged Access Management (PAM) trust is considered insecure if it has the trustAttribute TRUST_ATTRIBUTE_PIM_TRUST (0x00000400) bit set. **Remediation:** • Evaluate if EnableTgtDelegation is required and, if not, disable it on your domain trust. • Evaluate if EnablePIMTrust is required and, if not, disable it on your domain PAM trust.	Domain trust in scope has **EnableTgtDelegation or EnablePIMTrust** configured in the trustAttribute

Discovery for Reconnaissance Vulnerabilities

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

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 section for guidance when creating a new Discovery.

To create a Discovery:

1. From the Discoveries list, click **Create**.
2. Enter a **Discovery Type**.
3. Click **Select Vulnerabilities** to display a list of available vulnerability templates.
4. Select each vulnerability template you want to add to the Discovery, then click **Select.**
5. ***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 examples of Risk and Remediation text.

6. 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.

NOTES:

- If the Tier Zero objects checkbox is selected, all applicable Tier Zero objects, both those collected from the Tier Zero 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 privileged 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 Active Directory that are the applicable object type, including both Tier Zero and non-Tier Zero objects.
Select {objects}	Only the AD objects you specify based on your selection criteria (Display Name, Principal Name, or SID) will be included. When finished, click **Add Object** 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 **Add Exceptions** and enter the object(s) as you would if you were adding objects.
All Except Selected {objects}	Only the AD objects you specify based on your selection criteria (Display Name, Principal Name, or SID) will be excluded from the scope. You can add multiple AD objects, separated by semicolons. When finished, click **Add Object** to add the object (s)to the Selected {Object}s list.

7. 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 section for specific Vulnerability templates.)

NOTE: You cannot delete pre-defined Discoveries and the option will be disabled.

To view a Discovery:

Click the Discovery Type link.

To edit a Discovery:

1. Either:
   - In the Discoveries list, select the Discovery that you want to edit.
     OR
   - Open the Discovery that you want to edit.
2. Click **Edit**.

3. Update the Discovery as needed.
4. Click **Save**.

To delete a user-created Discovery:

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. Enter an **Assessment Name** and **Description**.
3. If you want to **Automatically add Discoveries as they are released by Quest**, check this box.

   NOTE: If you check this box, all pre-defined Discoveries that are provided by Quest will be added to the Assessment as they become available.
4. Click **Select Discoveries** to display a list of available Discoveries.
5. Select each Discovery you want to add to the Assessment, then click **Select**.

6. For **Domains**, select the Active Directory domains that you want to **Run this Assessment for**. Use the information in the following table for guidance.

Option	Steps to Complete
Only selected domains	• Select **Only selected domains** from the drop-down. • Click **Select Domains**, select the domains you want add to the Assessment, then click **Select**. The selected domain(s) will display in the list.
All except selected domains	• Select **All except selected domains** from the drop-down. • Click **Exclude Domains**. • Select the domain(s) you want to exclude from the Assessment. • Click **Exclude**. Excluded domains will display in the list. However, when you view the Assessment, all domains will display and those that are excluded are identified in the Status column.
All domains	Select **All domains**. All domains configured for your organization will display in the list.

7. 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.

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:

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 link to results for an Assessment from the All Assessments list.

To access results for a selected Assessment:

Click the corresponding Active Directory domain name in the **Link to Results** column.

NOTE: You can only view Assessment results for one Active Directory domain at a time. If the Assessment was run on more than one domain, you can switch to a different domain 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**.

  NOTE: These field 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*)

NOTE: An Inconclusive state indicates that data could not be collected for one or more objects being assessed for a non-error-related reason (for example, the scope of an Assessment includes Tier Zero objects but no Tier Zero objects were found, or permissions were insufficient to collect the data). Note that some vulnerabilities require additional permissions in order to be assessed.

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
- **Created by** either:
    - System (for pre-defined Discoveries and Vulnerabilities)
    - User (for user-created Discoveries and Vulnerabilities)
- 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
- 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.

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).

Inconclusive

NOTE: An Inconclusive state indicates that data could not be collected for a non-error-related reason (for example, the scope of an Assessment includes Tier Zero objects but no Tier Zero objects were found, or permissions were insufficient to collect the data).

Below the graph is information about the number of **Vulnerable Objects** found out of the total number of **Assessed Objects** for the selected area of the graph.

- If vulnerabilities were detected, a list of vulnerable objects is displayed, which includes reason why each object is considered vulnerable
- If results were inconclusive for an object, hover over the ⓘ icon for a description of the reason.
- If an error occurred, the appropriate message displays.

The Vulnerable Objects list can also be downloaded to a CSV file.

5

Findings

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

- Tier Zero object activity, including the identification of unprotected Tier Zero objects
- Indicators of Exposures and Indicators of Compromise detected by Security Guardian and collected by On Demand Audit.

NOTE: An exposure indicates that objects are susceptible to an adversary attack. A compromise indicates that it's possible an adversary attack has already occurred.

To view Findings:

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

The Findings list displays Active Directory objects, along with the following information for each:

- **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 Indicators of Compromise and Indicators of Exposure that are changes to Tier Zero object security, have significant potential impact to the Active Directory environment, and are not part of the default Active Directory configuration.
High	Generally reserved for Indicators of Exposure that are of high concern but impact single objects, the discovery of new Tier Zero domain objects, and changes to Tier Zero objects that occur more often through normal business operations or are part of the default Active Directory configuration.
Medium	Generally reserved for the addition of Tier Zero user, computer, group, and Group Policy objects.

- **Type** (Tier Zero, Exposure, or Compromise)

- 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:

- Tier Zero objects that have been identified by the Tier Zero provider (Security Guardian or BloodHound Enterprise) or manually by a user
- Exposures and Compromises that have been detected through Security Guardian Assessments and On Demand Audit critical activity.

Click on the Finding you want to investigate.
The Investigate Finding page consists of three sections.

- **What Happened?**
- **Am I Exposed?**
- **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 Activity

The top of a Tier Zero 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)

  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 Tier Zero object, dismiss the Finding, and view history of the Finding.

What Happened?

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

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

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

Link	Description
View Details	The properties of the Tier Zero 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, the date the object was added and the date its information was last updated. **NOTE:** The Date Added field displays the signed-in user's local date and time.
View Relationships	If BloodHound Enterprise is configured, 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 AD objects. **NOTE:** If Security Guardian is the Tier Zero provider, this option will be hidden.
View Recent Activity	This link opens the Quick Search page in On Demand Audit, which lists event data for the selected object. in On Demand Audit, which displays event data for the object being investigated.
	Escalate this Finding
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.

Am I exposed?

Because Tier Zero objects are critical assets, this section recommends that you explore all recent activity, inbound and outbound control, and relationships to determine the level of exposure produced by the Tier Zero object. Included are links to additional active Findings that can be considered related based on object type of the Tier Zero object currently being investigated. When investigating a given Finding, related active Findings will be displayed in one of the following sections based on its source:

- Assessment Findings
- Audit Findings

- Protection Findings

How Do I fix this?

This section provides recommendations for investigation and remediation.

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

Investigating Indicators of Exposure and Compromise

Findings for Indicators of Exposure and Indicators of Compromise are raised when:

- vulnerabilities are detected when a Security Guardian Assessment is run

AND/OR

- critical activity anomalies are detected by On Demand Audit.

> **NOTE:** An exposure indicates that objects are susceptible to an adversary attack. A compromise indicates that it's possible an adversary attack has already occurred.

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

- the **Severity** of the Finding
- the Finding **Type** (Exposure or Compromise)
- the **Finding Status** (Active or Inactive)
- the number of **Affected Objects**
- **Last Updated** (that is, the last time the Finding was detected)

  > **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?

The What Happened? section for Indicators of Exposure and Indicators of Compromise provides a description of the Finding and lists the objects that are affected. The following information is included for each object:

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

- **First Discovered** date and time

  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 objects)

    OR

  - Not Tier Zero

  NOTE: A status of "Status Not Available" may occur if the object has been deleted from Active Directory 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
	For Selected Objects in the list
Object Name (for a single object)	The properties of the object, including whether or not it is Tier Zero, identifiers used for the object within Active Directory, the date the object was added and the date its information was last updated. **NOTE:** This field displays the signed-in user's local date and time.
Mute Object button	See Muting Findings for Indicators of Exposure and Compromise.
View Activity button (for a single object)	This link opens the Quick Search page in On Demand Audit, which lists event data for the object being investigated.
View Assessment button (for a single object)	***If the indicator was raised by a Security Guardian Assessment***, this link opens the Assessment Results Vulnerability Detail page that includes the selected object. **NOTE:** This button is enabled only when a single object is selected.
View critical activity link	***If the indicator was raised by an On Demand Audit critical activity event***, this link opens Critical Activity event details in On Demand Audit.
	Escalate this Finding
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.

Am I exposed?

This section displays additional active Findings that can be considered related to the Finding currently being investigated. The Findings are considered related based on object type, similar attributes impacted, and possible exposed attack type. When investigating a given Finding, related active Findings will be displayed in one of the following sections based on its source:

- Assessment Findings
- Audit Findings
- Protection Findings

How Do I fix this?

This section provides the recommended remediation.

Muting Findings for Indicators of Exposure and Compromise

You can mute Findings for indicators of exposure or compromise, or individual objects within those Findings, to prevent future Findings from being raised for the object(s).

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.

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? page, select the object(s) you want to mute.
2. Click **Mute Object**.

NOTE: You can **unmute** muted objects from the Findings Investigation What Happened? 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 an Indicator of Exposure or Indicator of Compromise, 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 object.

  NOTES:

  - Only certified Tier Zero objects can be dismissed. If a Tier Zero object is not certified, the Dismiss option will be disabled. However, you can dismiss a Tier Zero 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 an Indicator of Exposure or Compromise, the confirmation dialog also includes a check box that allows you to mute the Finding at the same time.

To dismiss one or more Findings from the Findings list:

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

NOTE: If your selection contains only indicators of Exposure or Compromise, you will also have the option to mute the Finding(s). If the selection includes Tier Zero Findings, the option to mute will be unavailable. Any uncertified Tier Zero objects in the selection will not be dismissed.

Viewing Finding History

You can view the history of all actions associated with a Finding from the Findings list or the Findings Investigation page.

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

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

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

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

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

Click the **View History** button.

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

- **Date**

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

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

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

- when the object was detected and whether the source was the Tier Zero provider (Security Guardian or BloodHound Enterprise) or Manually added.
- when the Finding was created by Security Guardian.

For an **Indicator of Exposure or Indicator of Compromise**, the history will include:

- when an exposed or compromised 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 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

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 object activity
- The following exposures and compromises:
  - Security Assessment vulnerabilities detected by Security Guardian
  - Critical Activity and unprotected Tier Zero objects collected by On Demand Audit.

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.

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 Indicators of Compromise and Indicators of Exposure that are changes to Tier Zero object security, have significant potential impact to the Active Directory environment, and are not part of the default Active Directory configuration.
 **High**	Generally reserved for Indicators of Exposure that are of high concern but impact single objects, the discovery of new Tier Zero domain objects, and changes to Tier Zero objects that occur more often through normal business operations or are part of the default Active Directory configuration.
 **Medium**	Generally reserved for the addition of Tier Zero user, computer, group, and Group Policy objects.

- **Type** (Tier Zero, Exposure, or Compromise)
- **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:

Either:

- Click the link for the indicator.

  OR

- Select the indicator and click **View Indicator**.

  NOTE: If more than one indicator in the list is selected, the View Indicator button will be disabled.

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.

NOTES:

- New Tier Zero [*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**.

Appendix - Security Guardian Indicator Details

This appendix provides details of all indicators in Security Guardian, listed both by severity and by source.

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 Guardian, from most to least severe.

Indicator	Indicator Type	Severity	Source
Possible Golden Ticket Kerberos exploit	Compromise	Critical	On Demand Audit
Unsafe encryption used in Kerberos ticket (vulnerable to Kerberoasting)	Exposure	Critical	On Demand Audit
Groups with SID from local domain in their SID History	Compromise	Critical	Assessments
User accounts with SID from local domain in their SID History	Compromise	Critical	Assessments
Groups with well-known SIDs in their SID History	Compromise	Critical	Assessments
User accounts with well-known SIDs in their SID History	Compromise	Critical	Assessments
Potential sIDHistory injection detected	Compromise	Critical	On Demand Audit
File changes with suspicious file extensions	Compromise	Critical	On Demand Audit
Irregular domain controller registration detected (DCShadow)	Compromise	Critical	On Demand Audit
Irregular Active Directory replication activity detected	Compromise	Critical	On Demand Audit

Indicator	Indicator Type	Severity	Source
(DCSync)			
AD Database (NTDS.dit) file modification attempt detected	Compromise	Critical	On Demand Audit
Active Directory Database (NTDS.dit) access attempt detected	Compromise	Critical	On Demand Audit
Inheritance is enabled on the AdminSDHolder container	Compromise	Critical	Assessments
Non-privileged accounts that can promote a computer to a domain controller	Exposure	Critical	Assessments
Non-privileged accounts can steal password hashes (DCSync)	Exposure	Critical	Assessments
Privileged users owned by non-privileged accounts	Compromise	Critical	Assessments
Privileged computer is owned by a non-privileged account	Compromise	Critical	Assessments
User accounts with non-default Primary Group IDs	Compromise	Critical	Assessments
Computer accounts with non-default Primary Group IDs	Compromise	Critical	Assessments
User accounts without readable Primary Group ID	Compromise	Critical	Assessments
Computer accounts without readable Primary Group ID	Compromise	Critical	Assessments
Managed and Group Managed Service accounts that have not cycled their password recently	Compromise	Critical	Assessments
Non-privileged users with access to gMSA password	Exposure	Critical	Assessments
Non-privileged accounts can access the gMSA root key	Exposure	Critical	Assessments
Non-privileged accounts have access to write properties on certificate templates	Exposure	Critical	Assessments
Non-privileged user accounts with write permissions over Resource-Based Constrained Delegation on the KRBTGT account	Exposure	Critical	Assessments
Active Directory Operator groups that are not protected by AdminSDHolder	Exposure	Critical	Assessments
Ordinary user accounts with hidden privileges (SDProp)	Compromise	Critical	Assessments
User accounts in protected groups that are not protected by AdminSDHolder (SDProp)	Compromise	Critical	Assessments
KRBTGT accounts with Resource-Based Constrained Delegation	Exposure	Critical	Assessments
Built-in Administrator account that has been used	Compromise	Critical	Assessments
Anonymous Logon and Everyone groups are members of the Pre-Windows 2000 Compatible Access group	Exposure	Critical	Assessments

Indicator	Indicator Type	Severity	Source
Built-in Guest account is enabled	Exposure	Critical	Assessments
Schema Admins group contains members	Exposure	Critical	Assessments
Privileged groups which should not be in use contain members	Exposure	Critical	Assessments
DNSAdmin group contains members	Exposure	Critical	Assessments
Non-privileged accounts with Reanimate tombstones permission delegation	Exposure	Critical	Assessments
Non-privileged accounts with Migrate SID history permission delegation	Exposure	Critical	Assessments
Non-privileged accounts with Unexpire password permission delegation	Exposure	Critical	Assessments
Privileged Group Policy allows Recovery Mode to be not password-protected	Exposure	Critical	Assessments
Privileged groups with SID History populated	Compromise	Critical	Assessments
Privileged user accounts with SID History populated	Compromise	Critical	Assessments
Tier Zero group policy object changes	Exposure	Critical	On Demand Audit
Domain level group policy linked changes detected	Compromise	Critical	On Demand Audit
Non-privileged accounts can link GPOs to the domain	Exposure	Critical	Assessments
Non-privileged accounts can link Group Policy Objects to Domain Controller OU	Exposure	Critical	Assessments
Non-privileged accounts can link Group Policy Objects to an Active Directory site	Exposure	Critical	Assessments
Security changes to Tier Zero group policy objects	Exposure	Critical	On Demand Audit
Privileged user accounts with Service Principal Names	Exposure	Critical	Assessments
User ServicePrincipalName attribute changed (vulnerable to Kerberoasting)	Exposure	Critical	On Demand Audit
Non-privileged user accounts with Service Principal Names	Exposure	Critical	Assessments
Tier Zero group changes	Exposure	Critical	On Demand Audit
Unusual increase in failed AD changes	Compromise	Critical	On Demand Audit
Unusual increase in permission changes to AD objects	Compromise	Critical	On Demand Audit
Security changes to Tier Zero group objects	Exposure	Critical	On Demand Audit
Security changes to Tier Zero user objects	Exposure	Critical	On Demand Audit
Administrative privilege elevation detected (adminCount attribute)	Exposure	Critical	On Demand Audit
Non-privileged accounts are able to log onto privileged	Exposure	Critical	Assessments

Indicator	Indicator Type	Severity	Source
computers			
Tier Zero user logons to computers that are not Tier Zero	Exposure	Critical	On Demand Audit
Domain Admins can log into computers with non-privileged Group Policy	Exposure	Critical	Assessments
Unusual increase in failed AD Federation Services sign-ins	Compromise	Critical	On Demand Audit
Unusual increase in failed on-premises sign-ins	Compromise	Critical	On Demand Audit
Unusual increase in AD account lockouts	Compromise	Critical	On Demand Audit
Unusual increase in file renames	Compromise	Critical	On Demand Audit
Unusual increase in share access permission changes	Compromise	Critical	On Demand Audit
Unusual increase in file deletes	Compromise	Critical	On Demand Audit
Unusual increase in successful AD Federation Services sign-in	Compromise	Critical	On Demand Audit
Unusual increase in successful on-premises sign-ins	Compromise	Critical	On Demand Audit
Tier Zero domain and forest configuration changes	Exposure	Critical	On Demand Audit
Security changes to Tier Zero domain objects	Exposure	Critical	On Demand Audit
AD schema configuration changes	Exposure	Critical	On Demand Audit
New Tier Zero Domain detected	Tier Zero	High	Security Guardian
Domain trust configured insecurely	Exposure	High	Assessments
Privileged computer accounts that have not cycled their password recently	Exposure	High	Assessments
Privileged computers that have not recently authenticated to the domain	Exposure	High	Assessments
Protected group credentials exposed on read-only domain controllers	Exposure	High	Assessments
Privileged account token can be stolen from a read-only domain controller	Exposure	High	Assessments
User accounts do not require a password	Exposure	High	Assessments
Group Policy allows reversible passwords	Exposure	High	Assessments
User accounts have a reversible password	Exposure	High	Assessments
Administrator account can be delegated	Exposure	High	Assessments
Computer accounts with reversible password	Exposure	High	Assessments
User accounts with Kerberos pre-authentication disabled	Exposure	High	Assessments

Indicator	Indicator Type	Severity	Source
User accounts with unconstrained delegation	Exposure	High	Assessments
Computer accounts with unconstrained delegation	Exposure	High	Assessments
User accounts using DES encryption to log in	Exposure	High	Assessments
Privileged user accounts whose passwords have not changed recently	Exposure	High	Assessments
Privileged user accounts configured for Password Never Expires	Exposure	High	Assessments
Non-privileged user accounts configured for Password Never Expires	Exposure	High	Assessments
Non-privileged accounts with Microsoft Local Administrator Password (LAPS) access	Exposure	High	Assessments
Privileged computer can be compromised through Resource-Based Constrained Delegation	Exposure	High	Assessments
Privileged computer that has write permissions on Resource-Based Constrained Delegation granted to a non-privileged account	Exposure	High	Assessments
Non-privileged computer can be compromised through Resource-Based Constrained Delegation	Exposure	High	Assessments
Accounts that allow Kerberos protocol transition delegation	Exposure	High	Assessments
DNS zone configuration allows anonymous record updates	Exposure	High	Assessments
Tier Zero computer changes	Exposure	High	On Demand Audit
Security changes to Tier Zero computer objects	Exposure	High	On Demand Audit
Tier Zero user changes	Exposure	High	On Demand Audit
Foreign Security Principals are members of a privileged group	Exposure	High	Assessments
Domain Controller is running SMBv1 protocol	Exposure	High	Assessments
Non-privileged users can create computer accounts	Exposure	High	Assessments
Protected Users group is not being used	Exposure	High	Assessments
Abnormally large number of privileged user accounts in the domain	Exposure	High	Assessments
Enabled privileged user accounts that are inactive	Exposure	High	Assessments
Privileged groups that have computer accounts as members	Exposure	High	Assessments
Anonymous access to Active Directory is enabled	Exposure	High	Assessments
New Tier Zero GPO detected	Tier Zero	Medium	Security Guardian

Indicator	Indicator Type	Severity	Source
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	Exposure	Medium	Protection
Unprotected Active Directory database	Exposure	Medium	Protection
Unprotected Tier Zero Group Policy	Exposure	Medium	Protection
Unprotected Tier Zero Group	Exposure	Medium	Protection
Unprotected Tier Zero Computer	Exposure	Medium	Protection
Unprotected Tier Zero User	Exposure	Medium	Protection
Printer Spooler service is enabled on a domain controller	Exposure	Medium	Assessments
Privileged user account is disabled	Exposure	Medium	Assessments
Domain with obsolete domain functional level	Exposure	Medium	Assessments
NTLM version 1 authentications	Exposure	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 Audi, .

Indicator	Indicator Type	Severity
Active Directory Database (NTDS.dit) access attempt detected	Compromise	Critical
AD Database (NTDS.dit) file modification attempt detected	Compromise	Critical
AD schema configuration changes	Exposure	Critical
Administrative privilege elevation detected (adminCount attribute)	Exposure	Critical

Indicator	Indicator Type	Severity
Domain level group policy linked changes detected	Compromise	Critical
File changes with suspicious file extensions	Compromise	Critical
Irregular Active Directory replication activity detected (DCSync)	Compromise	Critical
Irregular domain controller registration detected (DCShadow)	Compromise	Critical
NTLM version 1 authentications	Exposure	Medium
Possible Golden Ticket Kerberos exploit	Compromise	Critical
Potential sIDHistory injection detected	Compromise	Critical
Security changes to Tier Zero computer objects	Exposure	High
Security changes to Tier Zero domain objects	Exposure	Critical
Security changes to Tier Zero group objects	Exposure	Critical
Security changes to Tier Zero group policy objects	Exposure	Critical
Security changes to Tier Zero user objects	Exposure	Critical
Tier Zero computer changes	Exposure	High
Tier Zero domain and forest configuration changes	Exposure	Critical
Tier Zero group changes	Exposure	Critical
Tier Zero group policy object changes	Exposure	Critical
Tier Zero user changes	Exposure	High
Tier Zero user logons to computers that are not Tier Zero	Exposure	Critical
Unsafe encryption used in Kerberos ticket (vulnerable to Kerberoasting)	Exposure	Critical
Unusual increase in AD account lockouts	Compromise	Critical
Unusual increase in failed AD changes	Compromise	Critical
Unusual increase in failed AD Federation Services sign-ins	Compromise	Critical
Unusual increase in failed on-premises sign-ins	Compromise	Critical
Unusual increase in file deletes	Compromise	Critical
Unusual increase in file renames	Compromise	Critical
Unusual increase in permission changes to AD objects	Compromise	Critical
Unusual increase in share access permission changes	Compromise	Critical
Unusual increase in successful AD Federation Services sign-in	Compromise	Critical
Unusual increase in successful on-premises sign-ins	Compromise	Critical
User ServicePrincipalName attribute changed (vulnerable to Kerberoasting)	Exposure	Critical

Indicators from Security Guardian Assessments

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

Indicator	Indicator Type	Severity
Abnormally large number of privileged user accounts in the domain	Exposure	High
Accounts that allow Kerberos protocol transition delegation	Exposure	High
Active Directory Operator groups that are not protected by AdminSDHolder	Exposure	Critical
Administrator account can be delegated	Exposure	High
Anonymous access to Active Directory is enabled	Exposure	High
Anonymous Logon and Everyone groups are members of the Pre-Windows 2000 Compatible Access group	Exposure	Critical
Built-in Administrator account that has been used	Compromise	Critical
Built-in Guest account is enabled	Exposure	Critical
Computer accounts with non-default Primary Group IDs	Compromise	Critical
Computer accounts with reversible password	Exposure	High
Computer accounts with unconstrained delegation	Exposure	High
Computer accounts without readable Primary Group ID	Compromise	Critical
DNS zone configuration allows anonymous record updates	Exposure	High
Domain Admins can log into computers with non-privileged Group Policy	Exposure	Critical
Domain Controller is running SMBv1 protocol	Exposure	High
Domain trust configured insecurely	Exposure	High
Domain with obsolete domain functional level	Exposure	Medium
Enabled privileged user accounts that are inactive	Exposure	High
Foreign Security Principals are members of a privileged group	Exposure	High
Group Policy allows reversible passwords	Exposure	High
Groups with SID from local domain in their SID History	Compromise	Critical
Groups with well-known SIDs in their SID History	Compromise	Critical
Inheritance is enabled on the AdminSDHolder container	Compromise	Critical
KRBTGT accounts with Resource-Based Constrained Delegation	Exposure	Critical
Managed and Group Managed Service accounts that have not cycled their password recently	Compromise	Critical

Indicator	Indicator Type	Severity
Non-privileged accounts are able to log onto privileged computers	Exposure	Critical
Non-privileged accounts are members of DnsAdmins group	Exposure	Critical
Non-privileged accounts can access the gMSA root key	Exposure	Critical
Non-privileged accounts can link GPOs to the domain	Exposure	Critical
Non-privileged accounts can link Group Policy Objects to an Active Directory site	Exposure	Critical
Non-privileged accounts can link Group Policy Objects to Domain Controller OU	Exposure	Critical
Non-privileged accounts can perform a DCSync attack *Name to change	Exposure	Critical
Non-privileged accounts have access to write properties on certificate templates	Exposure	Critical
Non-privileged accounts that can promote a computer to a domain controller	Exposure	Critical
Non-privileged accounts with Microsoft Local Administrator Password (LAPS) access	Exposure	High
Non-privileged accounts with Migrate SID history permission delegation	Exposure	Critical
Non-privileged accounts with Reanimate tombstones permission delegation	Exposure	Critical
Non-privileged accounts with Unexpire password permission delegation	Exposure	Critical
Non-privileged computer can be compromised through Resource-Based Constrained Delegation	Exposure	High
Non-privileged user accounts configured for Password Never Expires	Exposure	High
Non-privileged user accounts with Service Principal Names	Exposure	Critical
Non-privileged user accounts with write permissions over Resource-Based Constrained Delegation on the KRBTGT account	Exposure	Critical
Non-privileged users can create computer accounts	Exposure	High
Non-privileged users with access to gMSA password	Exposure	Critical
Ordinary user accounts with hidden privileges (SDProp)	Compromise	Critical
Printer Spooler service is enabled on a domain controller	Exposure	Medium
Privileged account token can be stolen from a read-only domain controller	Exposure	High
Privileged computer accounts that have not cycled their password recently	Exposure	High

Indicator	Indicator Type	Severity
Privileged computer can be compromised through Resource-Based Constrained Delegation	Exposure	High
Privileged computer is owned by a non-privileged account	Compromise	Critical
Privileged computer that has write permissions on Resource-Based Constrained Delegation granted to a non-privileged account	Exposure	High
Privileged computers that have not recently authenticated to the domain	Exposure	High
Privileged Group Policy allows Recovery Mode to be not password-protected	Exposure	Critical
Privileged groups that have computer accounts as members	Exposure	High
Privileged groups which should not be in use contain members	Exposure	Critical
Privileged groups with SID History populated	Compromise	Critical
Privileged user account is disabled	Exposure	Medium
Privileged user accounts configured for Password Never Expires	Exposure	High
Privileged user accounts whose passwords have not changed recently	Exposure	High
Privileged user accounts with Service Principal Names	Exposure	Critical
Privileged user accounts with SID History populated	Compromise	Critical
Privileged users owned by non-privileged accounts	Compromise	Critical
Protected group credentials exposed on read-only domain controllers	Exposure	High
Protected Users group is not being used	Exposure	High
Schema Admins group contains members	Exposure	Critical
User accounts do not require a password	Exposure	High
User accounts have a reversible password	Exposure	High
User accounts in protected groups that are not protected by AdminSDHolder (SDProp)	Compromise	Critical
User accounts using DES encryption to log in	Exposure	High
User accounts with Kerberos pre-authentication disabled	Exposure	High
User accounts with non-default Primary Group IDs	Compromise	Critical
User accounts with SID from local domain in their SID History	Compromise	Critical
User accounts with unconstrained delegation	Exposure	High
User accounts with well-known SIDs in their SID History	Compromise	Critical
User accounts without readable Primary Group ID	Compromise	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 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	Exposure	Medium	Protection
Unprotected Active Directory Database	Exposure	Medium	Protection
Unprotected Tier Zero Computer	Exposure	Medium	Protection
Unprotected Tier Zero Group	Exposure	Medium	Protection
Unprotected Tier Zero Group Policy	Exposure	Medium	Protection
Unprotected Tier Zero User	Exposure	Medium	Protection

About us

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

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