semperis

Purple Knight

Version: 5.0

User Guide

June 2025 (1)

Legal Notice

semperis

Contents

Published: June 2025

Preface

Welcome to the *Purple Knight User Guide*. This document is intended for Security and IT professionals interested in performing a security posture assessment on a hybrid identity environment, which may include Active Directory, Entra ID, or Okta. It explains how to run the tool as well as how to generate a Security Assessment report that provides details about potential vulnerabilities found in Active Directory, Entra ID, or Okta. It also provides a description of the comprehensive Security Assessment report that is generated.

Join the Purple Knight Slack channel to follow the community now using Purple Knight to minimize their attack surface and stay ahead of ever-evolving threats.

Document Revisions

The following revisions have been made to this document.

Table 1: Document Revisions

Product Version	Date	Document Revision	Comments
5.0	June 2025	1	Updated for 5.0 release; More granular severity levels; Updated system requirements

Styles and Conventions used in this Document

The following styles are used in this document.

Table 2: Document conventions and styles

Typeface	Description
Bold	Used for names of UI elements, such as buttons, pages, menus, options, fields, and columns.
Italics	Used for references to documents that are not hyperlinks to other documents or topics. Also used for dialog names and to introduce new terms.

Typeface	Description
`Monospace`	Used for command-line input and code examples.
<PLACE HOLDER>	Brackets denote place holder text that is to be replaced with a user-specified value.

The following styles are used for notices:

> ***NOTE:***
> *This notice style is used to provide additional information and background overview.*

> ***IMPORTANT!***
> *This notice style is used to present additional important information or warnings.*

Contacting Semperis

Thank you for your interest in Semperis and Purple Knight. We are here to answer any questions you may have.

For product inquiries or feature requests, contact pk-community@semperis.com.

Join the Purple Knight Slack channel to follow the community now using Purple Knight to minimize their attack surface and stay ahead of ever-evolving threats.

CHAPTER 1

Purple Knight Overview

Purple Knight is a security assessment tool that provides valuable insight into the security posture of your hybrid identity environment. It runs as a stand alone utility that queries your Active Directory environment and performs a comprehensive set of tests against many aspects of Active Directory's security posture, including AD Delegation, Account security, AD Infrastructure security, Group Policy security, Kerberos security. If applicable, Purple Knight can also query your Entra ID environment focusing on some of the most common attack vectors that threat actors use to gain unauthorized access or your Okta environment checking for activities that may indicate unauthorized access attempts, suspicious behavior, or potential threats within the Okta infrastructure.

Each security indicator is mapped to security frameworks such as MITRE ATT&CK® tactic categories, MITRE D3FEND™ cybersecurity countermeasures, and the French National Agency for the Security of Information Systems (ANSSI) rules, explains what was evaluated, and indicates how likely an exposure will compromise Active Directory, Entra ID, or Okta. The output of the utility is a comprehensive Security Assessment report that provides an overall security posture score for each environment included in the assessment, as well as detailed results about each Indicator of Exposure (IOE) found. Each IOE found highlights weak configurations and provides actionable guidance on how to close gaps before they are exploited by attackers. Using this report you can determine how you are doing from a security perspective, compared to best practice environments.

Purple Knight provides a snapshot of the current security posture of your hybrid identity environment by detecting software and configuration weaknesses using Indicators of Exposure (IOEs). IOEs help you understand how your Active Directory, Entra ID, or Okta environment may be compromised and spot changes that could indicate nefarious behavior.

Purple Knight is intended to augment your security team with know-how from a community of security researchers to minimize your attack surface and stay ahead of the ever-changing threat landscape.

Published: June 2025

What's New

The following features and enhancements are available in Purple Knight 5.0.

Purple Knight 5.0

In this release of Purple Knight, the security indicators are assigned a more granular severity level. In addition, Purple Knight was migrated to .NET 8 and indicators now run on PowerShell 7. Please note that .NET and PowerShell are now included in Purple Knight and no longer need to be installed in advance.

More Granular Severity Levels

Security indicators are assigned a more granular severity level to better align with the updated Security Posture scoring algorithm previously introduced in Purple Knight.

> ***NOTE**:*
> *The use of these more granular severity levels may impact the security posture score in your environment. This is because the algorithm currently used places emphasis on the severity of the indicators in addition to "failed" indicators and the volume of objects found for each indicator.*

The new severity level assignments are:

Table 3: Severity level map

New severity level (Purple Knight 5.x)	Previous severity levels (Purple Knight 4.x)
Info (weight: 1)	Info (weight: 1-4)
Low (weight: 2-3)	
Medium (weight: 4-5)	Warning (weight 5-7)
High (weight: 6-7)	
Critical (weight: 8-10)	Critical (8-10)

System Requirements

> ***NOTE**:*
> *.NET and PowerShell are now included in Purple Knight and no longer need to be installed in advance. For your information, Purple Knight was migrated to .NET 8 and indicators now run on PowerShell 7.*

For a list of bug fixes, improvements, and known issues, please see the PK_<*version*>_ ReleaseNotes.txt file.

CHAPTER 2

Getting Started

This topic lists the system requirements for Purple Knight and explains how to unblock the zip file and extract the executable to ensure you can run the tool.

System Requirements

Purple Knight runs on a domain-joined computer in the forest to be evaluated or using "Run As" credentials to a trusted forest.

To run Purple Knight from a non-domain joined computer:

1. Run the following command from the directory where the PurpleKnight.exe file is located:

   ```
   runas /env /netonly /user:<domainname>\<username>
   PurpleKnight.exe
   ```

2. You may need to manually enter the forest name in the forest enumeration screen.

Ensure the following system requirements are met when running Purple Knight.

Table 4: System requirements

Software/Hardware	Requirement
Operating system	Supported operating systems include: • Windows 8.1 • Windows 10 • Windows 11 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025
Network access	The following ports are required to run Purple Knight: • Local client -> DC (TCP 389): Used for domain discovery; Also used by scans that use LDAP queries • Local client -> DC (TCP 445): Used for domain discovery; Also used by scans that attempt RPC calls, such as ZeroLogon and PrintSpooler • Local client -> Any server running AD CS web enrollment endpoint (HTTPS 443): Used by AD Certificate Authority security indicator; attempts authentication to CS web servers Purple Knight does NOT support running from an untrusted network location. If running Purple Knight from a workgroup or untrusted forest, the machine running Purple Knight must be able to resolve DNS towards the forest to be scanned.
Supported browsers	The latest versions of the following browsers are supported: • Google Chrome • Microsoft Edge The browser is needed for viewing the assessment report and is not required on the machine where Purple Knight is running.

Table 4: System requirements

Software/Hardware	Requirement
Display resolution	Minimum: 1024 x 768
Logo size	Company logo requirements include: • 160 x 70 px • .jpg, .png, pr .jpeg format • no larger than 250 KB • file name must be logo.png, logo.jpg, or logo.jpeg For more information on how to add your company logo to the Security Assessment report, see *How to Add Company Branding*.

***NOTE**:*
.NET and PowerShell are now included in Purple Knight and no longer need to be installed in advance. For your information, Purple Knight was migrated to .NET 8 and indicators now run on PowerShell 7.

In addition, for those wanting to run the Entra ID security indicators, the following system requirements also apply. For more information on configuring Entra ID to run Purple Knight security indicators, see *Create and Configure Application Registration*.

Table 5: Microsoft Entra ID connection requirements

Azure/Entra Component	Requirement
Entra tenant	Supports only one Entra tenant per Purple Knight instance.
Azure application registration	Before you can configure the Entra ID connection in Purple Knight, you must create and configure an application registration that has the ability to generate a client secret. Required permissions (API permissions > Microsoft Graph > Application permissions): • User.Read.All • Application.Read.All In addition, the following permissions must be granted to the application in order to run the Entra ID security indicators: • AdministrativeUnit.Read.All • Application.Read.All *

Table 5: Microsoft Entra ID connection requirements

Azure/Entra Component	Requirement
	• AuditLog.Read.All • Device.Read.All • Directory.Read.All • GroupMember.Read.All • IdentityRiskyUser.Read.All • MailboxSettings.Read • OnPremDirectorySychronization.Read.All • Policy.Read.All • PrivilegedAccess.Read.AzureAD • Reports.Read.All • RoleEligibilitySchedule.Read.Directory • RoleManagement.Read.All • RoleManagement.Read.Directory • User.Read.All * • UserAuthenticationMethod.Read.All * The Application.Read.All and User.Read.All permissions are required for both the application itself and to run some of the Entra ID security indicators. ***NOTE**:* *When selecting the type of permissions required for the Purple Knight application, you must select **Application permissions**.*

For those wanting to run Okta security indicators, the following system requirements also apply.

Table 6: Okta connection requirements

Okta Component	Requirement
Okta domain	Supports only one Okta domain per Purple Knight instance.
Permissions	To run all of the Okta security indicators, the user running Purple Knight must be assigned the "Super Admin" role. A user with "Read-Only Administrator" role can be used. However, the Okta indicators that require higher privileges (such as, the indicators that read policies) will not run due to insufficient permissions.

Additional Permission Requirements

Some security indicators require additional permissions in order to run. By granting the Purple Knight user (user running Purple Knight) READ access to specific containers (as described below) , these security indicators will run as expected.

Privileged Users with Weak Password Policy

If an account that has a fine-grained password policy applied, the **Privileged Users with Weak Password Policy** security indicator requires access to the *CN=Password Settings Container,CN=System,<Domain Distinguished Name>* container in each domain of the forest.

By default, only Enterprise and Domain Admin accounts are granted access to this container. To run this indicator against accounts with fine-grained password policies, the Purple Knight user must be granted READ access to "This object and all descendant objects" on the *CN=Password Settings Container,CN=System,<Domain Distinguished Name>* container in each domain of the forest.

***NOTE**:*
Further details can be found in the Microsoft document AD DS: Fine-Grained Password Policies.

Unsecured DNS Configuration

In order to run the **Unsecured DNS Configuration** security indicator, the Purple Knight user must be granted READ access to "This object and all descendant objects" on the containers where the DNS zones are stored (CN=MicrosoftDNS,DC=ForestDnsZones,<*Domain Distinguished Name*> and CN=MicrosoftDNS,DC=DomainDnsZones,<*Domain Distinguished Name*> containers) within each DNS application partition in the forest.

Trusted User Reporting

To resolve the SAM Account Name of principals in trusted domains, the Purple Knight user must be granted READ access to "This object and all descendant objects" on the CN=ForeignSecurityPrincipals,<*Domain Distinguished Name*> container in each domain of the forest.

Create and Configure Application Registration

***NOTE**:*
These configuration instructions apply to those wanting to run the Entra ID security indicators available in Purple Knight. If you have no intention of running a security scan of an Entra tenant, you can skip these configuration steps and proceed to Running Purple Knight.

Before you can configure the Entra ID connection in Purple Knight, you must create and configure an application registration that has the ability to generate a client secret (referred to here as the Purple Knight application).

To summarize, the following Azure resources must be available BEFORE you can configure the Entra ID connection in Purple Knight to run the Entra ID security indicators:

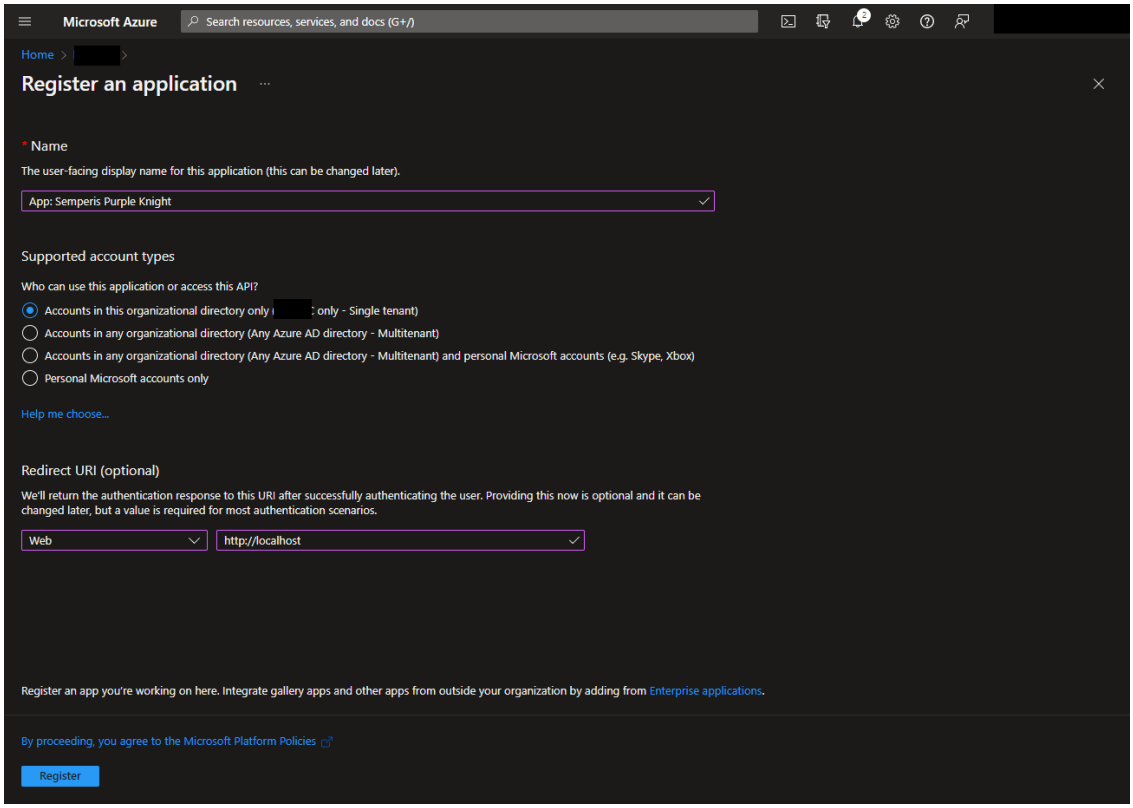
- Entra tenant
- Purple Knight application, which includes:
    - Granting the required permissions.
    - Creating a client secret for the application.

***TIP**:*
To run Purple Knight in your Entra ID environment, you need to create and update the app registration in Microsoft Entra with a defined and consented set of application permissions for the Microsoft Graph. To automate this step, Semperis provides a PowerShell script, which is available in GitHub.
In summary, the script supports the following:

- *Create and update the application registration in Microsoft Entra in order for Purple Knight to be able to scan for vulnerabilities in Entra ID.*
- *Delete the application registration from Entra ID.*
- *Assign the required Microsoft Graph Application Permissions and consent these permissions, when either creating or updating the application.*
- *Create a client secret that by default is valid for one hour, when either creating or updating the application. If needed, it is possible to provide a customer lifetime in days for the client secret.*
- *Delete all client secrets from the application registration in Microsoft Entra.*
- *Display the tenant ID, application ID, assigned and consented permissions, and client secret to be used in the Purple Knight executable.*

To create a Purple Knight application registration:

1. In the Azure portal (portal.azure.com), select the **Microsoft Entra** service.
2. In the Microsoft Entra portal, select **App registrations** under the **Manage** menu in the navigation pane.
3. Click **+ New registration**.
4. On the *Register an application* screen, enter a descriptive name for your Purple Knight application. You can use the default settings for the other settings (that is, Supported account types: Single tenant, Redirect URI: Web).



5. Click the **Register** button.

   Once the application is registered in Entra ID, the page for the newly registered application is displayed.

To add permissions to the Purple Knight application:

1. In the Microsoft Entra portal, select the Purple Knight application.
2. Select **API permissions** under the **Manage** menu in the navigation pane.

   The *Configured permissions* table on the *API permissions* screen displays the access granted to the application. Initially, you will see the default permission (User.Read) is assigned to the application.
3. Click **+ Add a permission**.
4. In the *Request API permissions* pane (right pane), select **Microsoft Graph**.
5. Click **Application permissions**.

In the *Select permissions* pane, search for and select the following application permissions:

- AdministrativeUnit.Read.All
- Application.Read.All
- AuditLog.Read.All
- Device.Read.All
- Directory.Read.All
- GroupMember.Read.All
- IdentityRiskyUser.Read.All
- MailboxSettings.Read
- OnPremDirectorySychronization.Read.All
- Policy.Read.All
- PrivilegedAccess.Read.AzureAD
- Reports.Read.All
- RoleEligibilitySchedule.Read.Directory
- RoleManagement.Read.All
- RoleManagement.Read.Directory
- User.Read.All
- UserAuthenticationMethod.Read.All

Click the **Add permissions** button.

6. Back on the *API permissions* screen, click ✓ **Grant admin consent for <*Tenant name*>**.

   On the *Grant admin consent confirmation* message at the top of the page, click **Yes**. Once the permissions are successfully granted, the **Status** displays a green check and "Granted for <*Tenant name*>" status message for the above permissions.

To create a client secret for the Purple Knight application:

IMPORTANT!
In the Microsoft Entra portal, the client secret value is only shown ONCE. Once the page refreshes or if you navigate to another page, only the hidden value (contains first few characters followed by asterisks) will be displayed and cannot be retrieved (copied) from the Microsoft Entra portal. The most secure way to retrieve this information for inclusion in Purple Knight is to copy and paste the secret key id and value directly into the Entra ID Connection settings page in Purple Knight. However, if this is not an option, you'll want to copy and paste these values into an application, such as Notepad, so they are available when configuring the Entra ID connection in Purple Knight.

It is highly recommended to not store client secrets in an insecure location; but rather store the client secrets in a secure password vault that is accessible by authorized persons only.

1. In the Microsoft Entra portal, select the Purple Knight application, and select **Overview** in the navigation menu.
   - From the **Overview** page, copy the value of the **Directory (tenant) ID** and paste it into the **Tenant ID** field of the **Entra ID Environment** page in Purple Knight.
   - From the **Overview** page, copy the value of the **Application (client) ID** and paste it into the **Application ID** field on the **Entra ID Environment** page in Purple Knight.
2. In the Microsoft Entra portal, while in the Purple Knight application, select **Certificate & secrets** under the **Manage** menu in the navigation menu.
   - Under the *Client secret* pane, click **+ New client secret**.
   - In the *Add a client secret* pane (right pane), enter the following information:
     - **Description**: Enter descriptive text for your client secret.
     - **Expires**: Select the life span for the client secret.

     Click **Add**.
3. Back on the **Certificates & secrets** screen, the secret is displayed.

   Copy the **Value** of the secret and paste it into the **Application Secret** field of the **Entra ID Environment** page in Purple Knight.

Running Purple Knight

To run Purple Knight, simply copy the contents of the zip file to a folder on your domain-joined machine. Please review the following instructions to ensure the zip file is unblocked and that you can run the PowerShell scripts included in the tool.

The license is built-in, which allows the utility to be run without entering a product license.

To run Purple Knight:

1. Download/copy the PurpleKnight.zip file.
2. Unblock the zip file.
    - Open the **Properties** dialog for the zip file.
    - On the **General** tab, select the **Unblock** check box in the **Security** section.
3. Extract the contents of the PurpleKnight.zip file to a folder with write permissions on a domain-joined computer (Windows workstation or server).

    ***NOTE**:*
    If you did not unblocked the zip file before expanding, you can unblock the individual files all at once using the following PowerShell command:
    `Get-ChildItem -Path e:\PK -Recurse | Unblock-File`
    Where: `e:\PK` is the folder where the files are to be extracted.

4. Ensure that your PowerShell Execution Policy is not blocking scripts from running on your machine. Purple Knight runs with the following execution permissions:
    - RemoteSigned
    - Unrestricted
    - Bypass

    To check your current execution policy:

    a. Run the following PowerShell cmdlet to determine what's the effective policy for your session:

    ```
    Get-ExecutionPolicy
    ```

    b. If the policy is "Unrestricted" or "RemoteSigned", proceed with running Purple Knight.

c. If the policy is "Restricted" or "AllSigned", run the following PowerShell cmdlet to determine where the value is coming from.

```
Get-ExecutionPolicy -list
```

d. If the hardened value is set in UserPolicy or MachinePolicy, contact your administrator.

e. If the hardened value is set in CurrentUser or LocalMachine, run the following cmdlet to set the execution permission on the "CurrentUser" scope:

```
Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
```

If you have an undefined execution policy it acts like a restricted policy, which means you are not allowed to run any scripts. In this case, run the `Set-ExecutionPolicy` PowerShell cmdlet mentioned above to set the execution permission on the "CurrentUser" scope.

5. Double-click the PurpleKnight.exe file to run Purple Knight.

After extracting the zip file, ensure that the **PurpleKnight** folder contains the following folder and file structure:

<*drive/path*>\PurpleKnight

\Scripts (Folder containing PowerShell scripts)

Scripts.config.xml (Scripts configuration settings)

package.version.xml (XML file containing product versioning information)

PurpleKnight.exe (Utility executable)

PK_<*version*>_ReleaseNotes.txt (Product release notes)

semperis_sat.lic (Built-in license file)

Settings.xml (Utility settings)

In addition, after the tool has run, the following folders are added to the **PurpleKnight** and **ProgramData** folders where you can find the reports and logs generated from the tool:

<*drive/path*>\PurpleKnight

\Output\<*date stamp*> (Folder where the full security assessment report is automatically stored and the default folder where the scan result files are saved.)

\Config (Folder where ignore file templates are created when a security indicator returns an **IOE found** result. These templates can then be used to define the objects to be added to the security indicator's ignore list. For more information, see *Security Indicators: Ignore Lists*.)

%ProgramData%\Semperis

\Logs

PurpleKnight.Log

PurpleKnightResults.Log

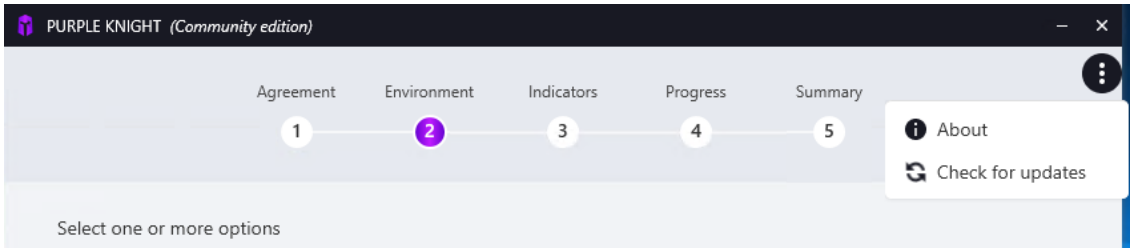
Viewing Version Information

The product version is displayed in the initial screen when Purple Knight is run and in the **About** box within the product.

The **About** box can be viewed from all pages in the product except the **Agreement** page.

To view version information:

1. After launching Purple Knight, proceed to the **Environment** page.
2. Click the ⋮ (**More**) button in the top right corner of the page and select **About**.



   The **About** box displays the current product version, Semperis contact information, and copyright statement.

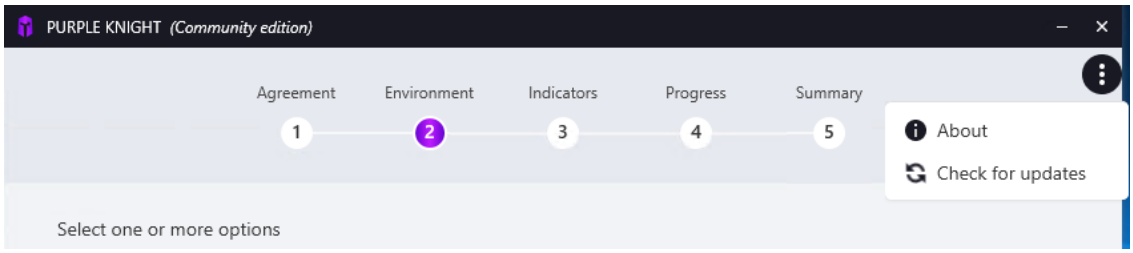
3. Click **OK** to close the **About** box.

Checking for New Version

To check if there is an updated version of Purple Knight available, click the (**More**) button in the top right corner of any page within Purple Knight, except the **Agreement** page.

To check for an updated version:

1. After launching Purple Knight, proceed to the **Environment** page.
2. Click the (**More**) button in the top right corner of the page and select **Check for updates**.



The **Check for updates** dialog displays, which includes two panes: **PK version** and **Security indicators**.

Once the check is completed you will be presented with the results in the **PK version** pane.

- If you are using the latest version, a message displays stating you are using the latest version. Click the (**Close**) button in the top right corner of the dialog to close the **Check for updates** dialog and proceed with running Purple Knight.
- If a newer version is available, a message displays stating that a newer version is available. You can either:
  - Click the **View** button to display the Purple Knight website to download the updated package.
  - Click the (**Close**) button in the top right corner of the dialog to close the *Check for updates* dialog and use the current version.

Checking for Security Indicator Updates

Purple Knight also allows you to check for and download updated security indicator packages without having to run a new version of Purple Knight.

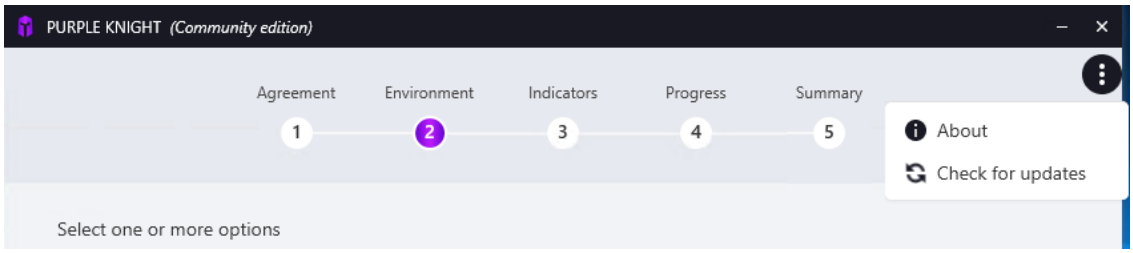
To check if there is an updated security indicator package available, click the (**More**) button in the top right corner of any page within Purple Knight, except the **Agreement** page.

When you select to update the security indicator package, the update package includes all the security indicators, not just updated or new ones. For a list of the new and updated security indicators included in a security update package, see the changelog.html file.

NOTE:
*The changelog.html file contains a list of the updated and new indicators. When you click **Check for Updates**, a new changelog.html file is temporarily saved in PurpleKnight/Scripts/Nuget/ChangeLog. Once indicators are updated, this directory and changelog.html file are automatically removed.*

To check for updated security indicator package:

1. After launching Purple Knight, proceed to the **Environment** page.
2. Click the (**More**) button in the top right corner of the page and select **Check for updates**.



The **Check for updates** dialog displays, which includes two panes: **PK version** and **Security indicators**.

Once the check is completed you will be presented with the results in the **Security indicators** pane:

- If you are using the latest security indicator package, a message displays stating you are using the latest version. Click the (**Close**) button in the top right corner of the dialog to close the **Check for updates** dialog and proceed with running Purple Knight.
- If an updated security indicator package is available, a message displays stating that a new update package is available. You can either:
  - Click the **UPDATE** button to download the updated package. A progress bar displays as the updates are being downloaded. Once the security indicators are successfully downloaded, a "Security Indicators successfully updated" message displays.

    For a limited time, a **CANCEL** button is available, which if clicked cancels the download process and reverts to using the previous security indicators before the update.
  - Click the (**Close**) button in the top right corner of the dialog to close the *Check for updates* dialog and use the currently loaded security indicator package.

CHAPTER 3

Running a Security Assessment Report

Purple Knight is a stand alone utility that runs Windows PowerShell scripts to assess Active Directory, Entra ID, and/or Okta environments and produce a security posture report. The tool has no dependency on any other Semperis product and does not require any special privileges to run. A normal authenticated user from the forest that is being scanned is usually sufficient.

To run a security assessment report:

1. Double-click the PurpleKnight.exe file.
2. Follow the prompts on the wizard pages:
    - *Agreement page*: Accept the terms of the license agreement.
    - *Environment page*: Check for updated version. Select the type of environment to be scanned (Active Directory, Entra ID, and/or Okta) to see the overall security posture across your hybrid identity environment. Provide connection details to establish a connection to the selected environments.
    - *Indicators page*: Select the security indicators to be run.
    - *Progress page*: Monitor the progress of the assessment.
    - *Report Summary page*: View the overall security posture scores for each environment included or view and save the full report.
3. On the **Report Summary** page, use the buttons at the bottom of the page as described below:
    - **NEW SCAN**: Click to start a new scan. Clicking this button returns you to the *Environment page* in order to select the environment (Active Directory, Entra ID, Okta) and if applicable, the AD forest and domains to be used in the new scan.

- **SAVE AS**: Click to save the full assessment report in .PDF format or the scan results data in a series of .CSV files.
- **VIEW REPORT**: Click to view the full detailed Security Assessment report in your default browser.

4. Click the **X** (**Close**) button in the top right corner to exit Purple Knight.

Agreement page

The initial page displays the Purple Knight license agreement. You must accept the license terms in order to proceed.

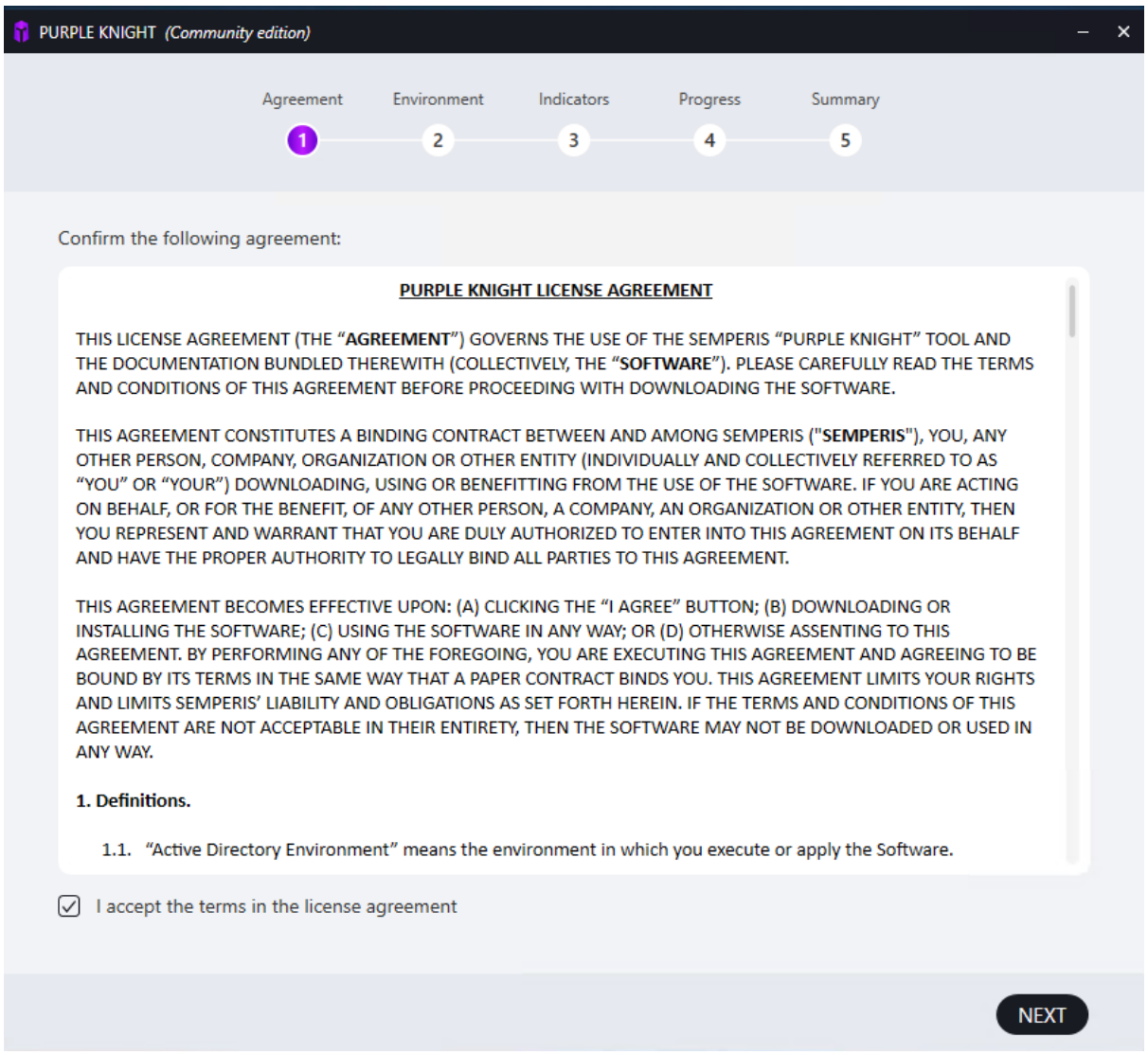


Figure 1: Agreement page

To confirm and continue:

1. Read the license agreement and select the **I accept the terms in the license agreement** check box at the bottom of the page.
2. Click **NEXT**.

Environment page

From the **Environment** page select the type of environments to be scanned: Active Directory, Entra ID, and/or Okta. You can select multiple environments if you want to see the overall security posture across your hybrid identity environment.

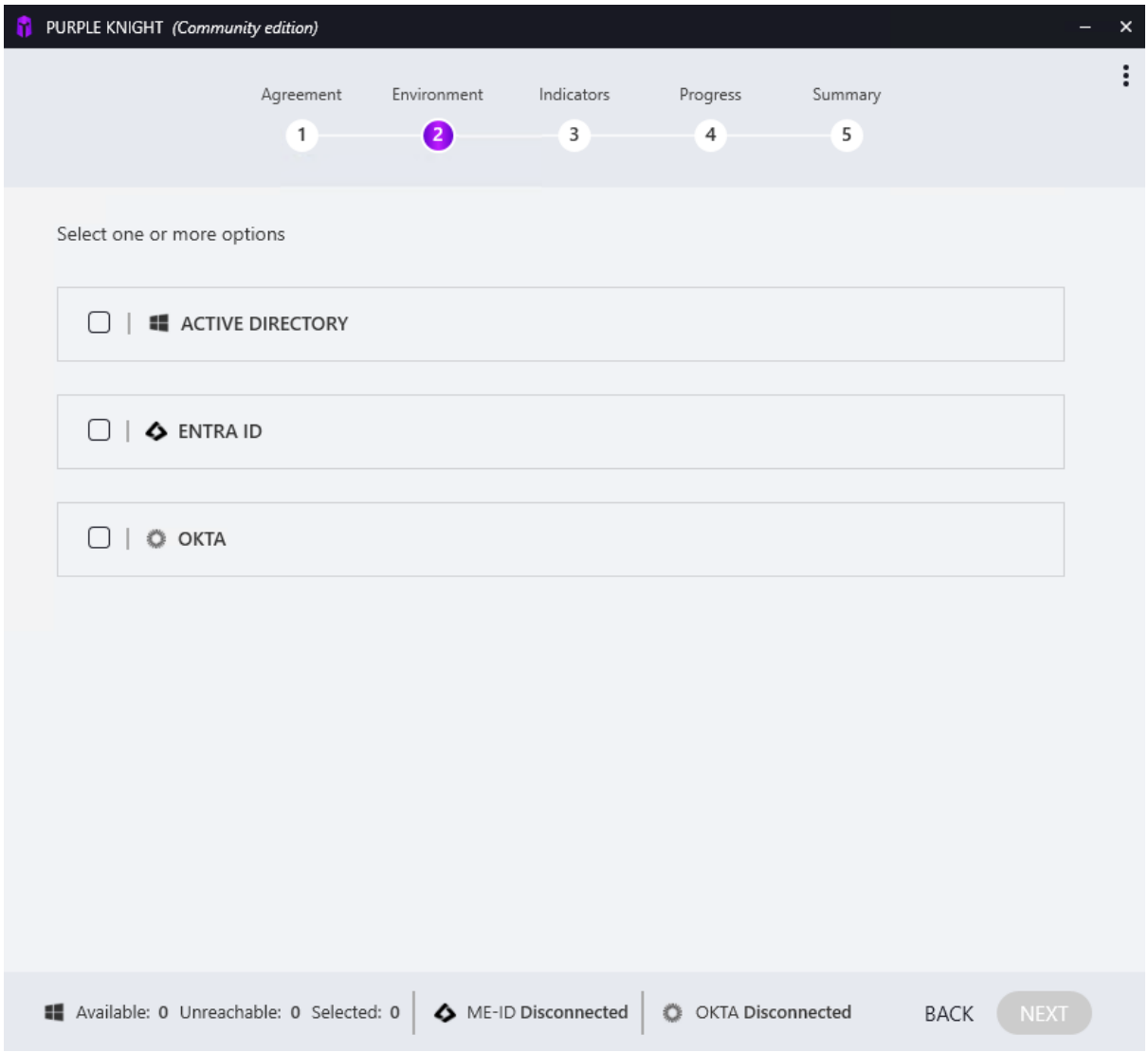


Figure 2: Environment page

Depending on your selection, you will be presented with additional connection details that must be specified in order to establish a connection with the selected environments.

- *Environment page: Active Directory*
- *Environment page: Entra ID*
- *Environment page: Okta*

Environment page: Active Directory

Select **ACTIVE DIRECTORY** on the **Environment** page to select the AD forest and domains to be included in the security assessment.

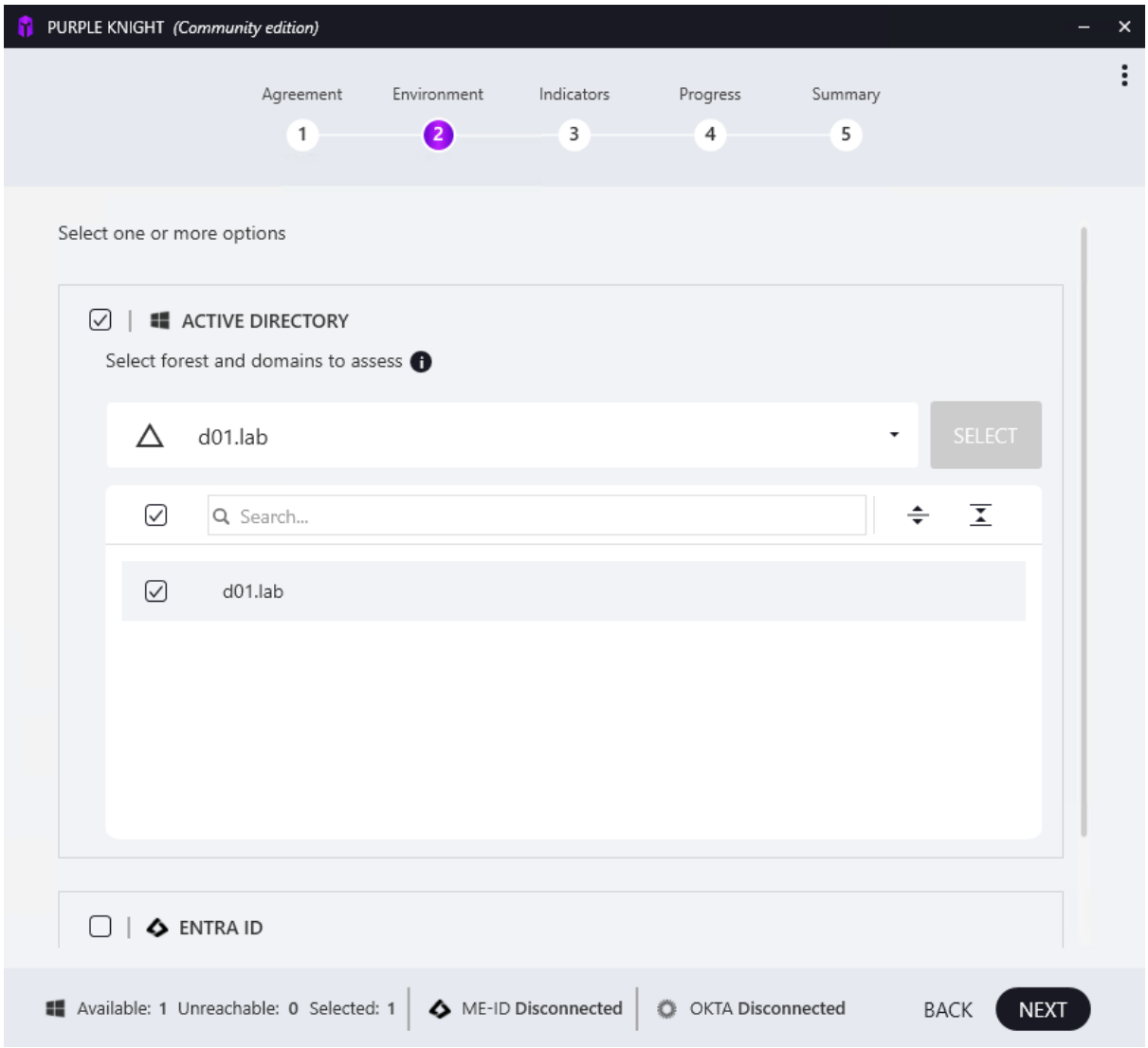


Figure 3: Environment page: Active Directory

Forest selection

Purple Knight discovers the topology and detects the current forest. By default, the current forest is displayed; or if no forest is detected the field will be blank. You can specify a trusted forest by entering the forest's FQDN, NetBios name, or IP address.

Domain selection

Once the forest is validated by clicking the **SELECT** button, Purple Knight validates the connection and user credentials. If insufficient credentials are found, you will be prompted to enter valid credentials (that is, you need Read permissions to query the forest). Once the connection and user credentials are validated, Purple Knight returns a list of available domains.

All available domains are selected by default. The row above the domains list includes controls that allow you to select or clear all domains in the selected forest, search for a domain by name, and expand or collapse the domains list.

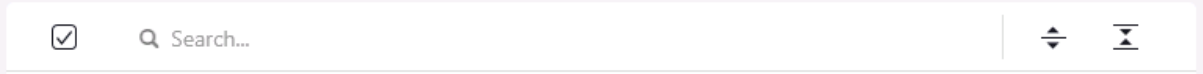


Figure 4: Domain selection tool bar

Use the domain selection controls as described below:

Selection control. This control indicates the following:

- A check mark indicates that all domains and child domains are selected. (Default)
- A filled in square indicates that only some domains or child domains are selected.
- An empty check box indicates that no domains or child domains are selected.

Enter a string of characters to search the domain list by domain name. As you enter characters, the domain list refreshes displaying domains whose name contains the partial string entered.

Click **x** to clear the search box and redisplay the entire list.

(**Expand**) Click to expand the domain list to display all child domains.

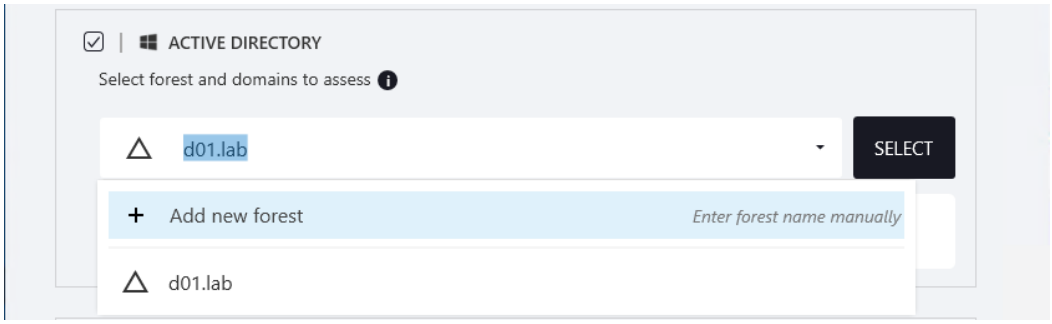
(**Collapse**) Click to collapse the domain list to hide all child domains.

To select the forest and domains:

BEST PRACTICE:
For an accurate assessment, select all of the domains in the selected forest.

NOTE:
In large enterprise environments, it may be beneficial to run Purple Knight in stages; excluding very large domains or those connecting across the WAN at first.

1. In the **ACTIVE DIRECTORY** pane, select the forest.
   - By default, the current forest is displayed.
   - To select an alternate forest, click the drop-down arrow, select **Add new forest**, and enter the FQDN, NetBios name, or IP address of the forest.



2. After selecting a forest, click **SELECT**. Clicking this button initiates a search for domains within the selected forest.

   NOTE:
   Domains that cannot be reached will be excluded from the scan. In the domain list, the ⊘ icon to the left of a domain's name indicates that the domain is unreachable.

3. Select the domains to be included.
   - To select all domains in the forest, select the "select all" check box in the row above the domain list. (Default)

- To select individual domains, clear the check box associated with the domains to be excluded from the report. You can also clear the "select all" check box and select the check box to the left of the domains to be included.
- If the domain contains child domains, the number of child domains are listed to the right of the domain name. Click the expansion arrow for the domain to display the child domains. Either clear the check box associated with the child domains to be excluded or clear the "select all" check box and select the check box to the left of the child domains to be included.

Below the domains list you will see the number of available, unreachable, and selected domains and buttons that allow you to navigate to the next or previous page. (The OKTA and Entra ID connection status do not apply to your Active Directory connection.)

4. If you want to see the overall security posture across your hybrid identity environment, select the appropriate environments.
   - Select the **ENTRA ID** check box to specify the Entra tenant to be included in the assessment. For more information, see *Environment page: Entra ID*.
   - Select the **OKTA** check box to specify the Okta domain to be included in the assessment. For more information, see *Environment page: Okta*.
5. At the bottom of the **Environment** page, ensure all selected environments have been successfully connected.
6. Click **NEXT**.

Environment page: Entra ID

Use the **ENTRA ID** pane on the **Environment** page to establish an Entra tenant connection. All of the information you need can be copied from the Microsoft Entra portal and pasted into the designated fields in this pane.

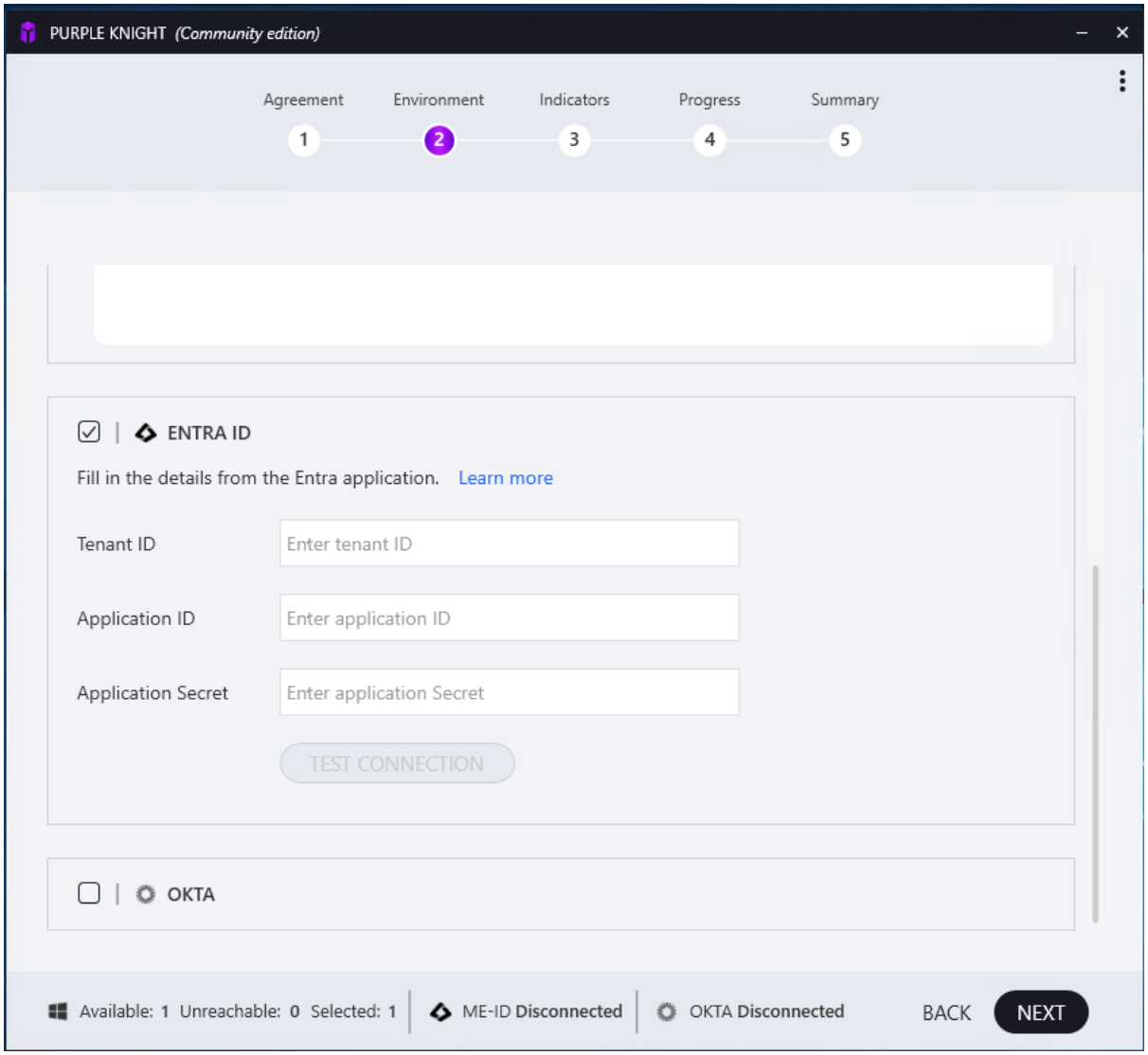


Figure 5: Environment page: Entra ID

***NOTE**:*
Only one Entra tenant can be registered per Purple Knight instance. The time it takes to create the initial connection to Entra ID could take several minutes to complete.

Before you begin:

Ensure the Entra tenant is configured. This includes registering the Purple Knight application, setting the appropriate permissions, and creating a client secret for the application.

For more information, see *Create and Configure Application Registration*.

To configure an Entra tenant connection:

1. On the **Environment** page, select **ENTRA ID**.
2. In the expanded **ENTRA ID** pane, enter the following information from your Microsoft Entra portal:
    - **Tenant ID**: The unique tenant identifier assigned to the Entra tenant where the Purple Knight application is registered.

      (Microsoft Entra portal: The **Tenant ID** can be found in the *Basic Information* pane at the top of the **Overview** page for the Entra tenant.)
    - **Application ID**: The unique application identifier assigned to the Purple Knight application.

      (Microsoft Entra portal: The **Application (client) ID** can be found in the *Essentials* pane at the top of the **Overview** page for the application.)
    - **Application Secret**: The value assigned to the secret key ID.

      (Microsoft Entra portal: The Secret ID and Value can be found on the **Certificates & secrets** page under the **Manage** menu.)
3. After entering the required information, click **TEST CONNECTION**.

   If the connection was successful, a **Connected** indicator is added to the upper right corner of the **ENTRA ID** pane. In addition, "**ME-ID Connected**" displays across the bottom of the page. (The domain counts (Available, Unreachable, and Selected) do not apply to your Entra ID connection.)
4. If you want to see the overall security posture across your hybrid identity environment, select the appropriate environments.
    - Select the **ACTIVE DIRECTORY** check box to select the forest and domains to be included in the assessment. For more information, see *Environment page: Active Directory*.

- Select the **OKTA** check box to specify the Okta domain to be included in the assessment. For more information, see *Environment page: Okta*.

5. At the bottom of the **Environment** page, ensure all selected environments have been successfully connected.
6. Click **NEXT**.

Environment page: Okta

Use the **OKTA** pane on the **Environment** page to establish a connection to your Okta identity platform.

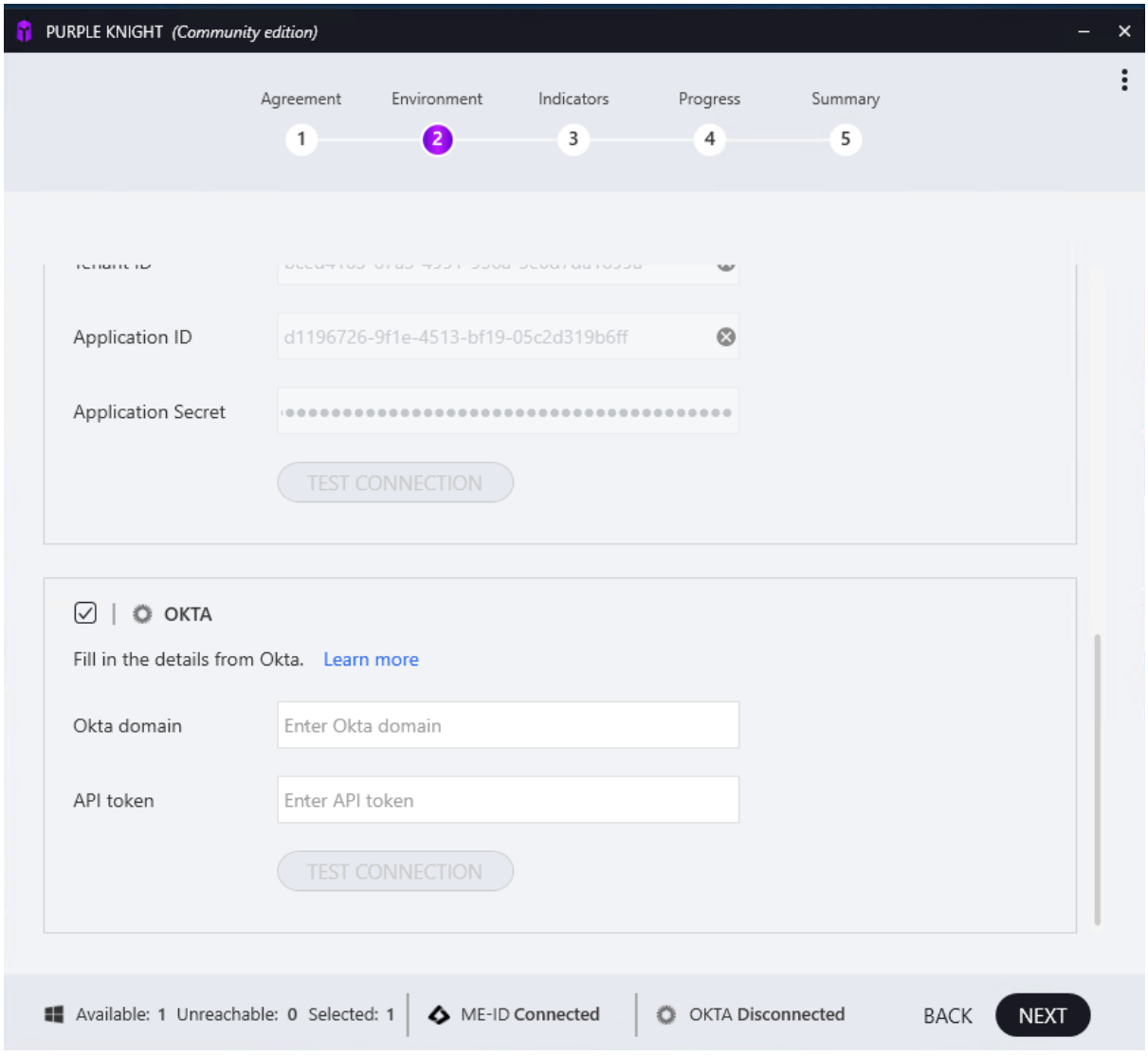
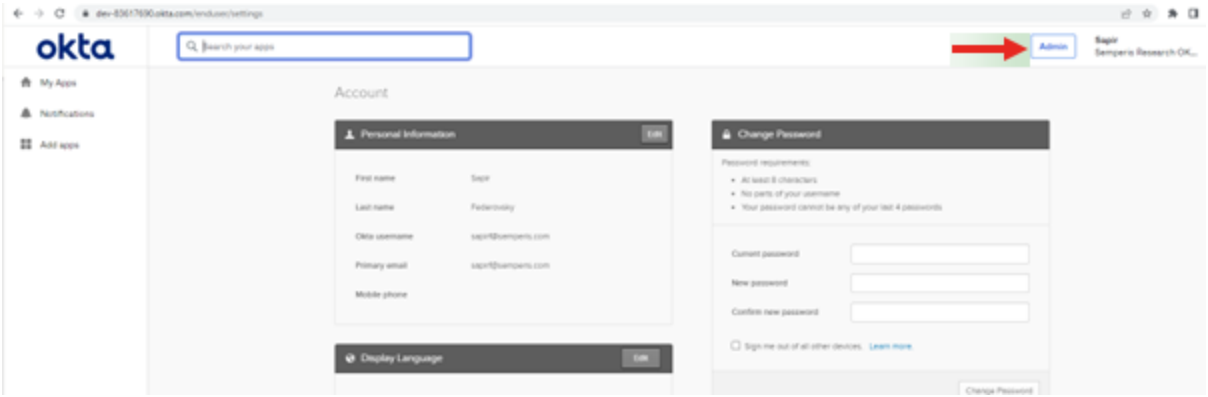


Figure 6: Environment page: Okta

Before you begin:

Ensure that your Okta identity platform is configured and available. All of the information you need to connect to Purple Knight can be found in the Okta Admin console.

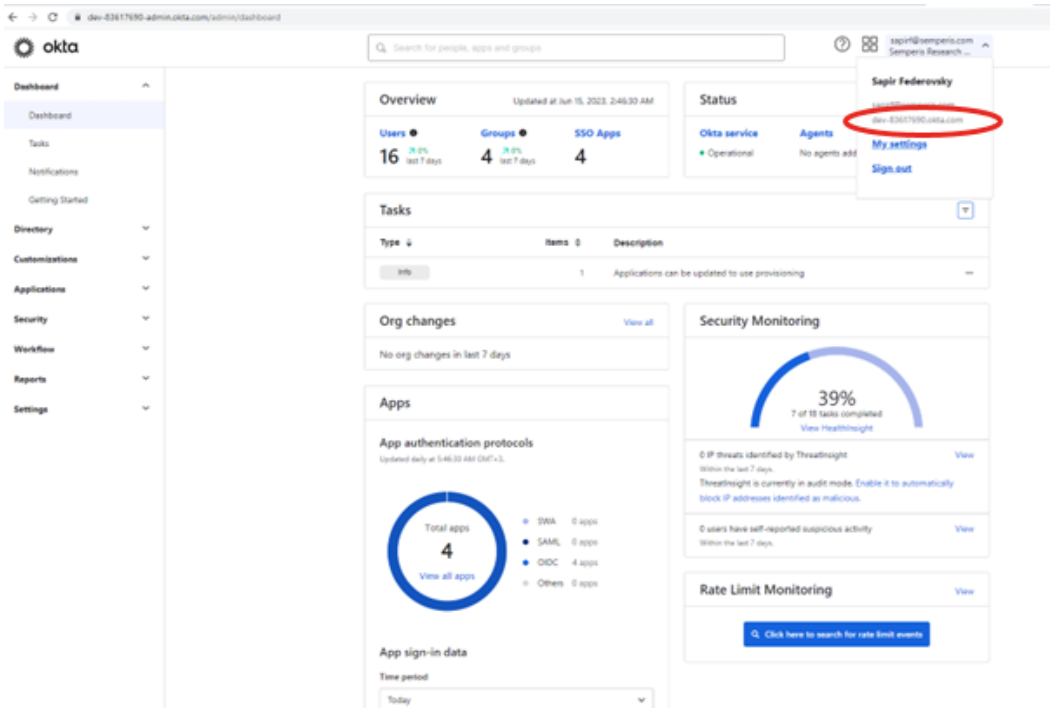
To connect to the Admin console, log in as an Admin user to Okta and click the **Admin** button.



To configure an Okta connection:

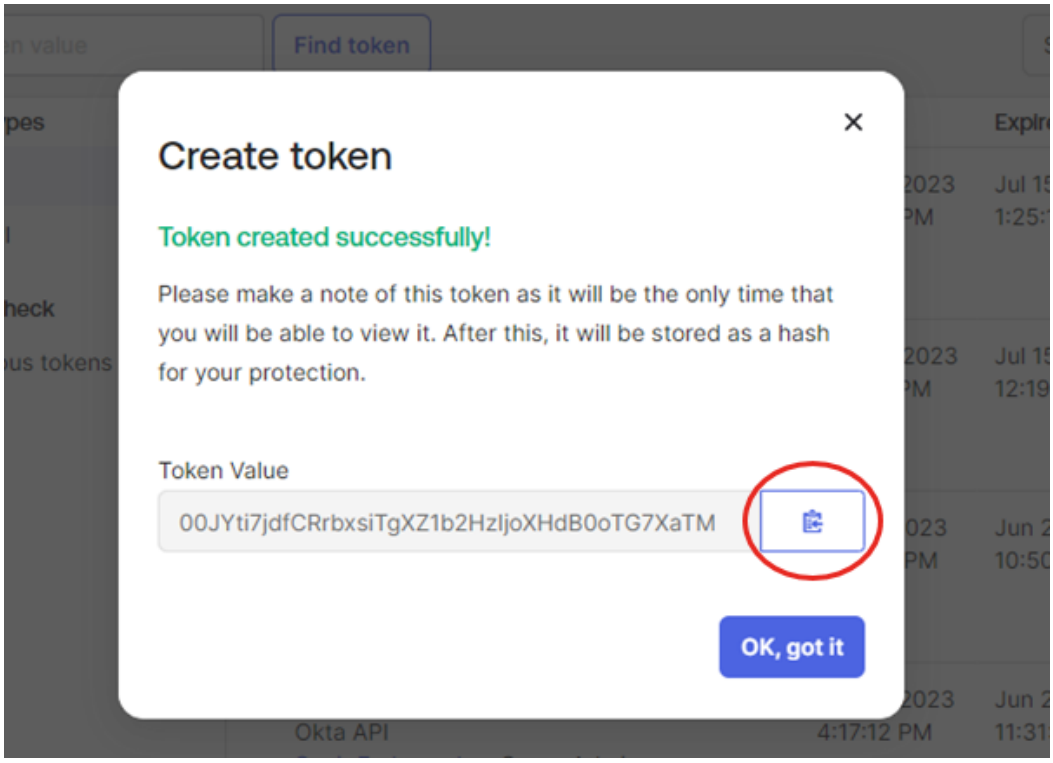
1. On the **Environment** page in Purple Knight, select **OKTA**.
2. In the expanded **OKTA** pane, enter the following information from the Okta Admin console:
    - **Okta domain**: The **Admin** domain URL, which is the same as the domain URL but includes "-admin". For example, if the domain URL is: testing123.okta.com, the Admin domain URL would be: testing123-admin.okta.com.

      (Okta Admin console: The domain URL can be found under the user's properties, which can be viewed by expanding the user's account in the header row).

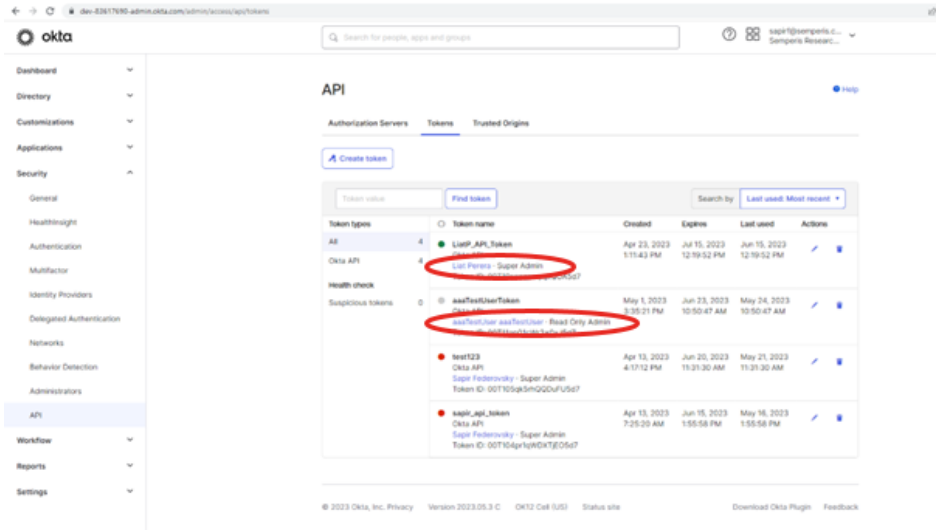


- **API token**: The unique application identifier to be assigned to the Purple Knight application.

  (Okta Admin console: For the API token, navigate to the **Security > API > Tokens** tab and select **Create token**. On the "Token created successfully" dialog, use the copy button to the right of the **Token Value** field to capture the API token. This is the value that Purple Knight requires and as the dialog message states is only available from this dialog.)



***NOTE**:*
*The token's permissions are inherited from the user associated with it. Therefore, if you change the user's role, the associated token's permissions will also change. You can view the user associated with a token and its permissions from the **Security > API > Tokens** tab.*



3. After entering the required information, click **TEST CONNECTION**.

   If the connection was successful, a **Connected** indicator is added to the upper right corner of the **OKTA** pane. In addition, "**OKTA Connected**" displays across the bottom of the page. (The domain counts (Available, Unreachable, and Selected) do not apply to your Okta connection.)

4. If you want to see the overall security posture across your hybrid identity environment, select the appropriate environments.

   - Select the **ACTIVE DIRECTORY** check box to select the forest and domains to be included in the assessment. For more information, see *Environment page: Active Directory*.
   - Select the **ENTRA ID** check box to specify the Entra tenant to be included in the assessment. For more information, see *Environment page: Entra ID*.

5. At the bottom of the **Environment** page, ensure all selected environments have been successfully connected.

6. Click **NEXT**.

Indicators page

From the **Indicators** page, select the security indicators (scripts) to be included in the assessment. The security indicators are divided into categories and you can select a category to include all the security indicators assigned to the category or individual security indicators.

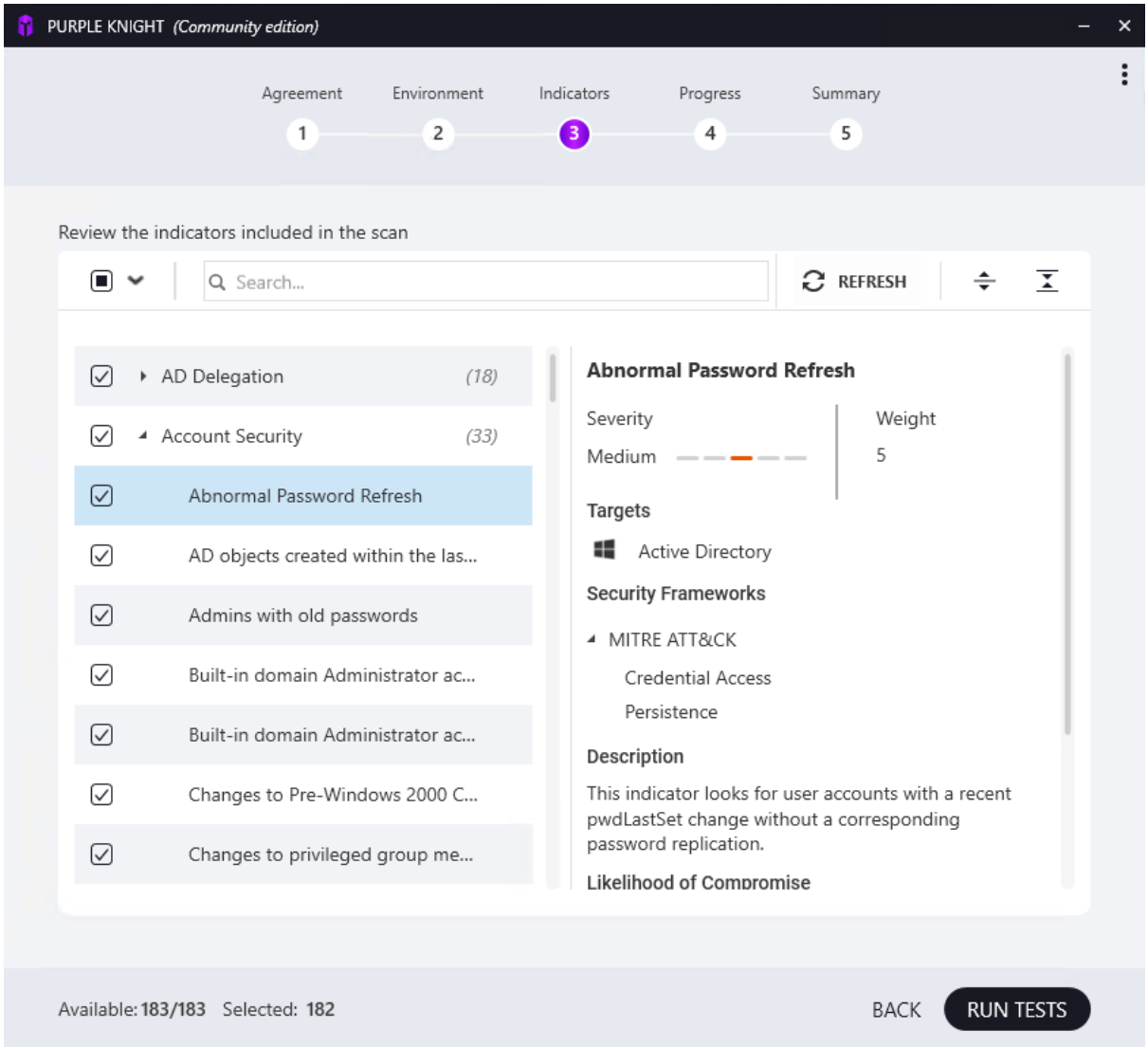


Figure 7: Indicators page

Security indicator selection

All but one of the security indicators are selected by default. The **AD Infrastructure Security > Zerologon vulnerability** security indicator is not selected by default, because it can take hours to complete in a large enterprise environment. To include this security indicator in your assessment report, you will need to select it using the controls described below.

The row above the security indicators list includes controls that allow you to select or clear all security indicators, search for a security indicator, and expand or collapse the security indicators list.

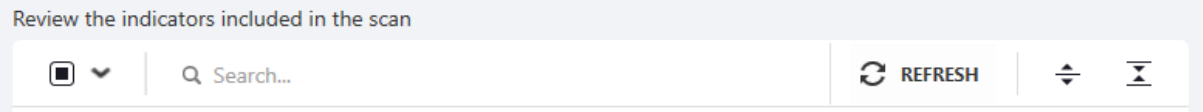


Figure 8: Security Indicator selection tool bar

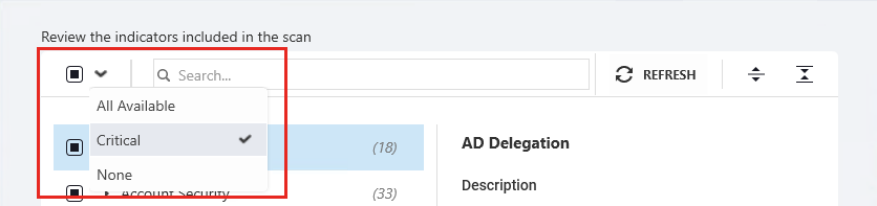
Use the security indicator selection controls as described below:

Selection control. This control indicates the following:

- A filled in square indicates that only some security indicators are selected. (Default)
- A check mark indicates that all available security indicators are selected.
- An empty check box indicates that no security indicators are selected.

Click the down arrow to perform a bulk selection. From the menu select one of the following options:

- **All Available**: Select all available security indicators.
- **Critical**: Select only security indicators assigned a critical severity.
- **None**: Clear all selected check boxes (security indicators).



Search... Enter a string of characters to search the security indicator list. As you enter characters, the list refreshes displaying security indicators whose name or description contains the partial string entered.

Click **x** to clear the search box and redisplay the entire list.

REFRESH Click to re-verify the permissions and indicator list.

(**Expand**) Click to expand the list to display all relevant security indicators per category.

(**Collapse**) Click to collapse the list to hide all security indicators and just show the categories list.

The left pane in the security indicators list, lists the security indicators available by category. The right pane displays details about the selected category or security indicator. Selecting a category displays a general description of the type of security indicators included within the category and its assigned weight. Selecting a security indicator displays the following details about the selected security indicator:

- Severity
- Weight
- Targets (Active Directory, Entra ID, or Okta)
- Required permissions (Only displayed for indicators that require specific permissions, for example Entra ID indicators.)
- Security frameworks
- Description
- Likelihood of Compromise

In addition, if you are not certain if the indicator applies to the Active Directory, Entra ID, or Okta platform, hovering your cursor over a security indicator displays a tool tip that includes the platform information.

***BEST PRACTICE**:*
For an accurate assessment, select all of the security indicators. However, keep in mind Entra ID security indicators that do not have the required permissions cannot be selected.

***NOTE**:*
In large enterprise environments, if you are interested in getting a "quick glance" at your AD security posture, it is recommended that you exclude the following security indicators from your initial run:

- ***Account Security > Enabled users that are inactive***
- ***AD Infrastructure Security > Zerologon Vulnerability** (excluded by default)*

These particular tests could take hours to complete in a large enterprise environment.

To select a security indicator:

1. From the left pane of the security indicators list, select the security indicators to be run:
   - To select all available security indicators, select the "select all" check box in the row above the security indicators list. (Default)
   - To select all security indicators within a category, clear the "select all" check box and then select the check box to the left of the category.
   - To select individual security indicators, clear the "select all" check box, click the expansion arrow to the left of the category, and select the check box to the left of an individual security indicator. You can also click the (**Expand**) button to expand all the categories and clear the check box associated with the security indicators to be excluded.

   Below the security indicators list you will see the number of available and selected security indicators and buttons that allow you to run the selected tests or return to the previous page.
2. After selecting the security indicators to be evaluated, click **RUN TESTS**.

***NOTE**:*
*Entra ID indicators that do not have the required application permissions cannot be included in the assessment. A warning banner is displayed along with a "permissions missing" icon (⊘) next to the **Entra ID** category heading. Select an unchecked security indicator, to view the permissions that are missing (**Required permissions** in right pane).*

*After granting the missing application permissions, click **Refresh**. Clicking **Refresh** will trigger a new permission verification check and if sufficient permissions are assigned the security indicator can now be selected for inclusion in the assessment.*

Progress page

The **Progress** page shows the progress as the selected security indicators are evaluated. All selected security indicators are displayed in a collapsed list organized by category.

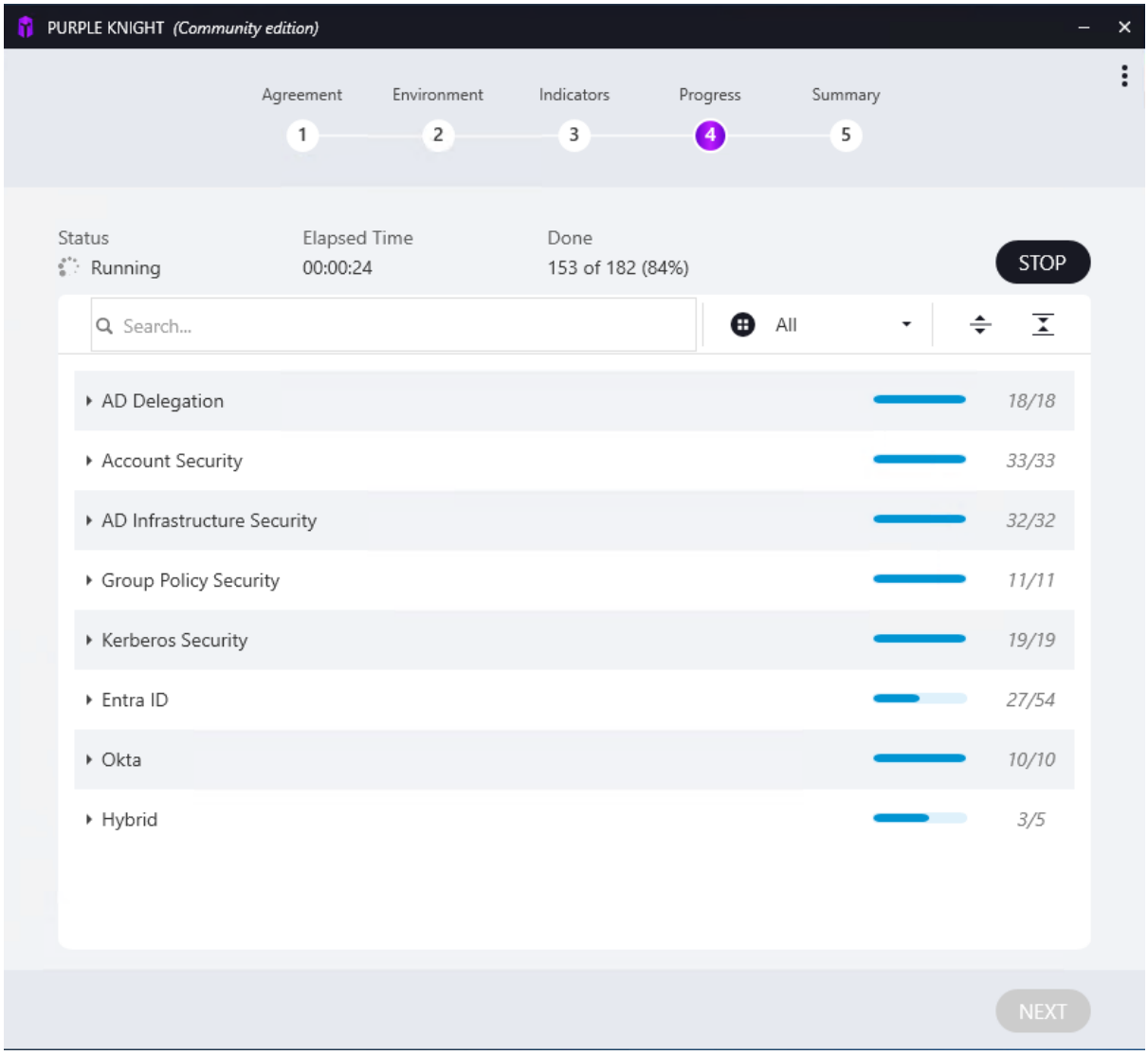


Figure 9: Progress page

Overall report progress

This page shows the following details for the overall report progress:

- **Status**: The current overall status of the tests being run.
- **Elapsed Time**: The amount of time it is taking to run the assessment report.
- **Done**: How many tests have completed against the total number of selected tests to be run. The completed test count includes security indicators that passed without finding any IOE and those that found an IOE. It does not include security indicators that failed to run.

Individual security indicator progress

Each category shows a progress bar and indicates the number of tests within the category that have completed.

Use the controls above the category/security indicator list to search for an individual security indicator by name, filter the progress by status, and expand or collapse the categories to show or hide associated security indicators.

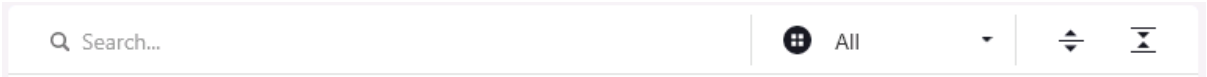


Figure 10: Progress page tool bar

Use the Progress page controls as described below:

Enter a string of characters to search the security indicator list by security indicator name. As you enter characters, the list refreshes displaying security indicators whose name contains the partial string entered.

Click **x** to clear the search box and redisplay the entire list.

Click the expansion arrow to select the status filter to be applied to the progress page. By default, **All** is selected, which indicates the progress of all security indicators is displayed regardless of their status. When a different status filter is selected, the categories are automatically expanded to display the individual security indicators.

(**Expand**) Click to expand the category list to display all relevant security indicators per category.

(**Collapse**) Click to collapse the category list to hide all security indicators.

As the security indicators are evaluated, the status of each individual security indicator can be displayed by clicking the expansion arrow to the left of a category or the (**Expand**) button above the category/security indicator list.

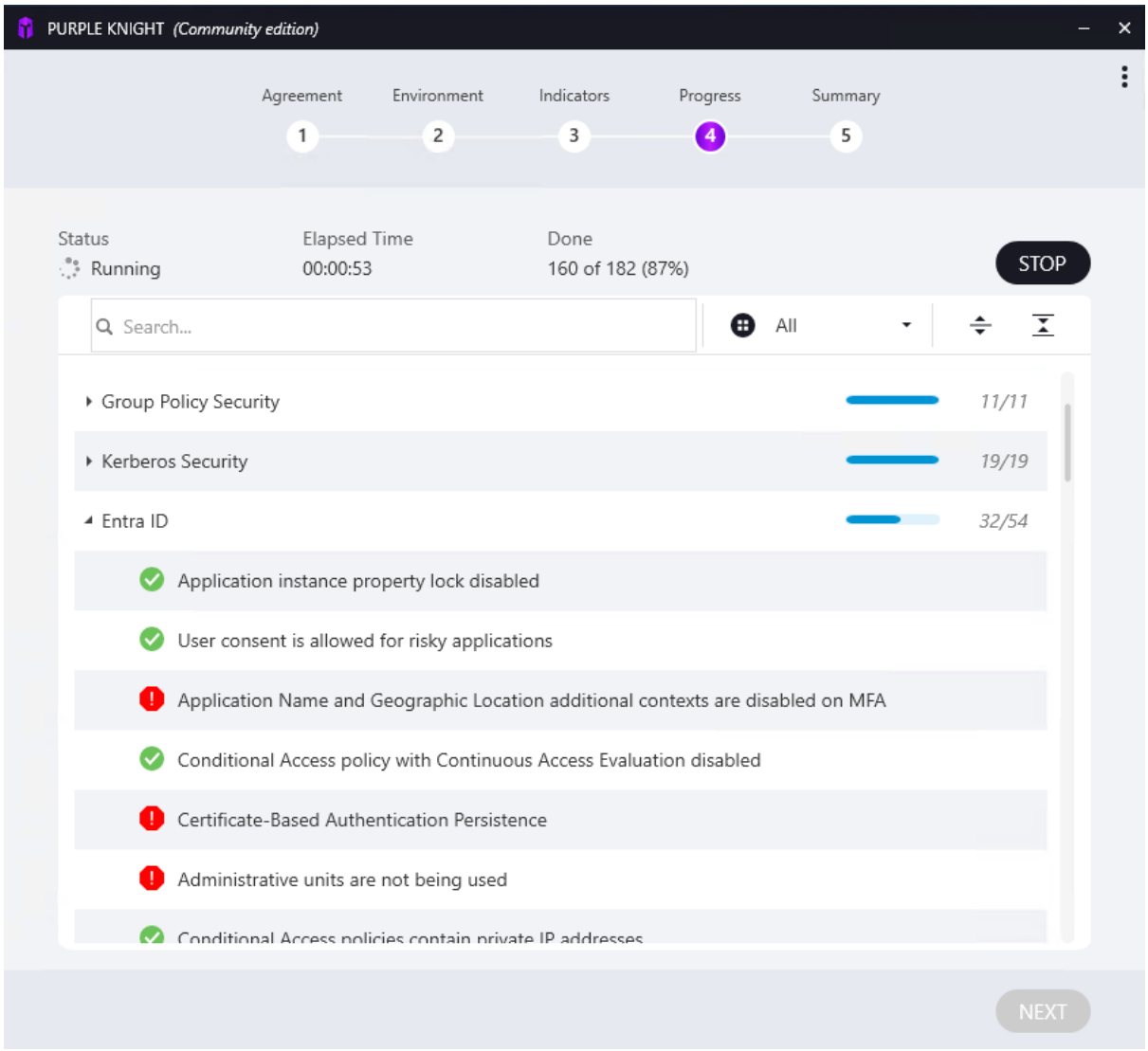


Figure 11: Progress page with category expanded

When the evaluation is completed, the **Report Summary** page is automatically displayed.

To stop running the tests in progress:

1. Click the **STOP** button to stop evaluating the security indicators.
2. On the confirmation dialog, select **No** to continue to run the tests or **Yes** to stop running the tests that are in progress and not run any that are pending.
3. The **Report Summary** page displays. A report is generated based on the security indicators that have completed prior to clicking the **STOP** button.

***NOTE**:*
*Stopping the report on the **Progress** page, does NOT cancel the generation of the report; it only stops running any security indicators that are in progress or that have not yet run. The Security Assessment report that is generated is a partial report that includes only the security indicators that ran prior to stopping. This partial report does however indicate the number of security indicators that were canceled and not included in the assessment.*

Report Summary page

The **Report Summary** page summarizes the results of the security assessment, including the overall security posture score (percentage and letter score) and environment details, such as where (AD forest, Entra tenant, Okta domain) the assessment was performed and who ran the assessment.

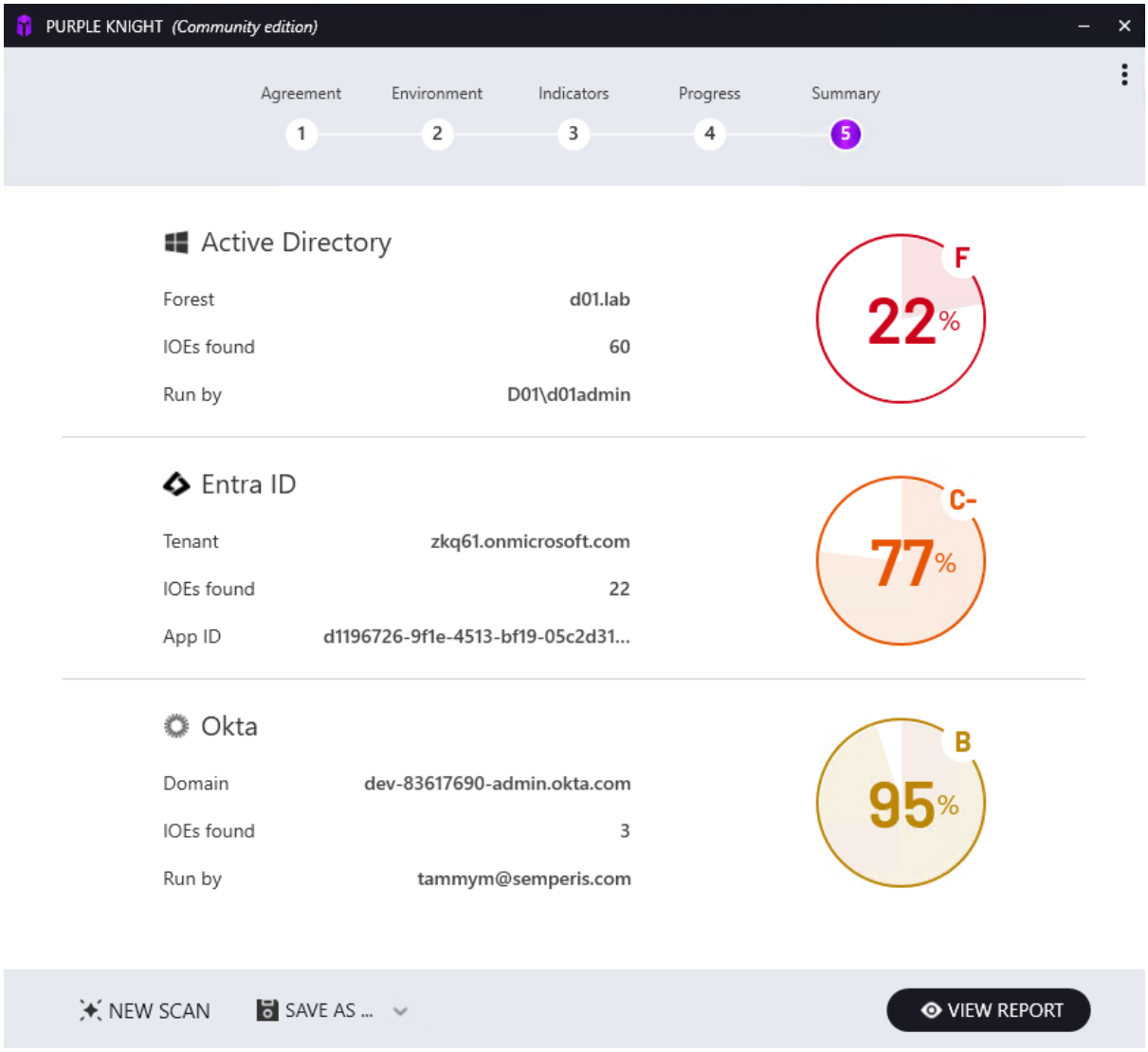


Figure 12: Report Summary page

Active Directory

When an Active Directory environment is included in the assessment, the following information is provided:

- **Forest**: The name of the forest that was evaluated.
- **IOEs found**: Total number of IOEs found across all selected Active Directory security indicators.
- **Run by**: The name of the account that ran the assessment report.
- **Security posture**: Displays the results of the Active Directory security assessment with an overall security posture score (percentage and letter score).

Entra ID

When an Entra ID environment is included in the assessment, the following environment and run details are provided:

- **Tenant**: The name of the Entra tenant that was evaluated.
- **IOEs found**: Total number of Indicators of Exposure (IOEs) found across all selected Entra ID security indicators.
- **App ID**: The application ID of the application that ran the assessment report.
- **Security posture**: Displays the results of the Entra ID security assessment with an overall security posture score (percentage and letter score).

Okta

When an Okta environment is included in the assessment, the following environment and run details are provided:

- **Domain**: The name of the Okta domain that was evaluated.
- **IOEs found**: Total number of Indicators of Exposure (IOEs) found across all selected Okta security indicators.
- **Run by**: The name of the account that ran the assessment report.
- **Security posture**: Displays the results of the Okta security assessment with an overall security posture score (percentage and letter score).

The report, in HTML format, and an Excel file containing the scan results are automatically saved to the **Output** folder in the **PurpleKnight** directory where the

PurpleKnight.exe file is located, for example, **<*drive/path*>\PurpleKnight\Output**. A folder is added for each security assessment report generated, using the date and time stamp as the folder name. This folder may contain the following output files:

- Security_Assessment_Report_<*forest-name*>_<*date/time stamp*>.html: Report in HTML format.
- Security_Assessment_Report_<*forest-name*>_<*date/time stamp*>.xlsx: An Excel spreadsheet containing the full results returned from the assessment.

> ***NOTE**:*
> *An Excel file that includes all of the scan results is automatically created and saved in the **Output** folder under the **PurpleKnight** directory. This Excel spreadsheet contains multiple tabs (Summary tab and a tab for each indicator that returned results) that lists all of the directory objects returned.*
>
> *If the creation of the Excel file fails due to Excel's limitations for number of columns, rows, or characters in a cell, a .csv file is created for each Excel tab and is saved in the **Output** folder under the **PurpleKnight** directory.*

- Security_Assessment_Report_<*forest-name*>_<*date/time stamp*>_<*indicator ID_name*>.csv: A .CSV file for each security indicator whose scan returned results.

  .CSV files are saved for each security indicator whose scan returned results if the **Save As > Result data as CSVs** is selected on the **Report Summary** page.

Use the buttons at the bottom of this page to save the report, view the full detailed report, or exit Purple Knight.

NEW SCAN Click to start a new scan. Clicking this button returns you to the *Environment page* in order to select the environment (Active Directory, Entra ID, and/or Okta) and if applicable, the AD forest and domains to be used in the new scan.

> ***NOTE**:*
> *When you launch a new scan, the current **Report Summary** will no longer be available. However, the full report that contains the results of the current scan is available in the PurpleKnight/Output folder.*

SAVE AS Select one of the report options:

- **Full PDF report**: Click to save the full report results in .PDF format.

  Clicking this button displays the *Save As* dialog allowing you to change the name of the .PDF file or location where the file is to be saved. By default, the file is saved in the **Output** folder created under the **PurpleKnight** directory.

- **Result data as CSVs**: Click to save a series of .CSV files that contain the results of the assessment. That is, for each security indicator whose scan returned results, a .CSV file is generated containing the result details.

  Clicking this button displays the *Browse for Folder* dialog allowing you to select the location where the files are to be saved. Once the results have been successfully saved, you are asked whether you want to open the output file.

VIEW REPORT Click to view the full detailed Security Assessment report in your default browser.

CHAPTER 4

Security Assessment Report

The **Report Summary** page in the Purple Knight tool summarized the results of the security assessment, including an overall security posture score (percentage and letter score), environment summary, and evaluation results summary for each environment included in the security assessment. Whereas, the full Security Assessment report provides the overall security posture score (percentage and letter score), detailed findings for each security indicator test, and recommended actions that can be taken to address any weaknesses or risky configurations that are found.

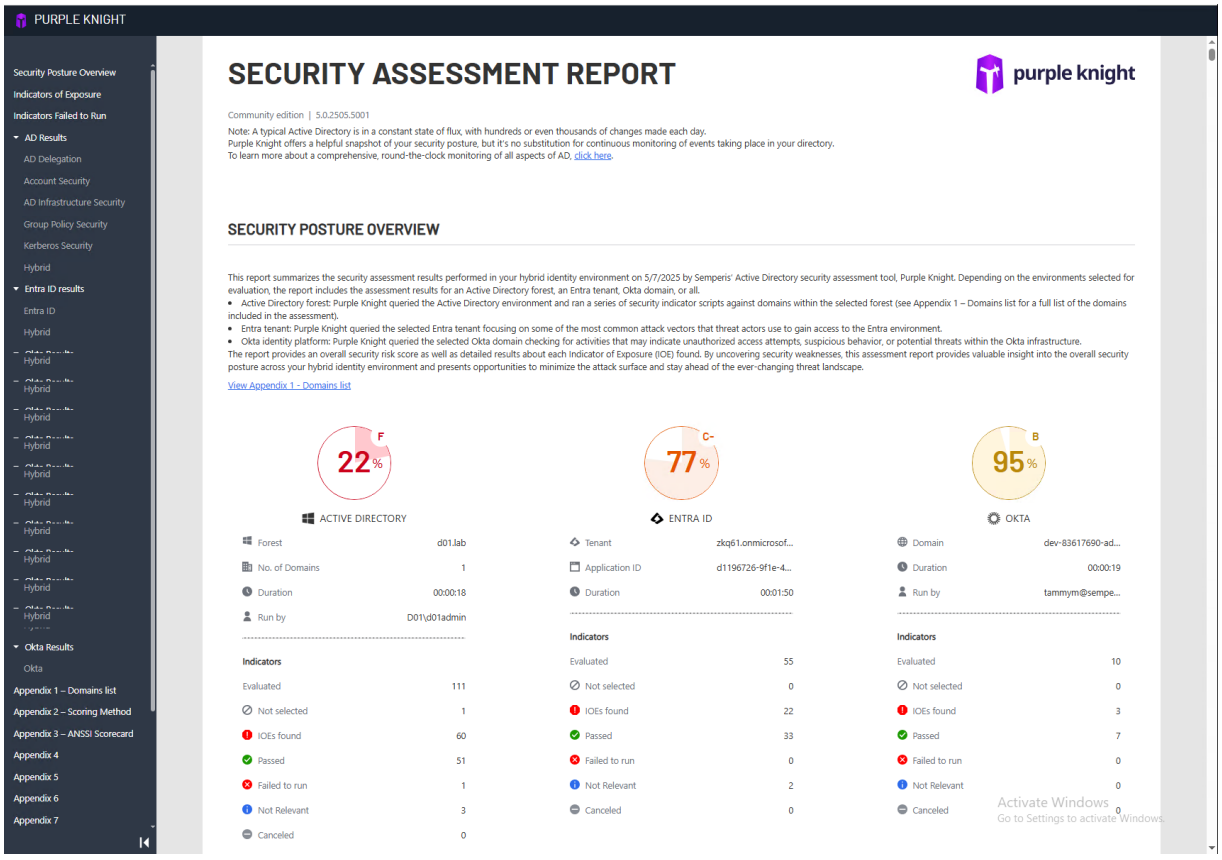


Figure 13: Security Assessment Report

You can either scroll through the report or use the navigation pane to navigate to a specific section within the report. That is, click a section heading in the navigation pane (left pane) to display that section within the report. The report is divided into the following sections:

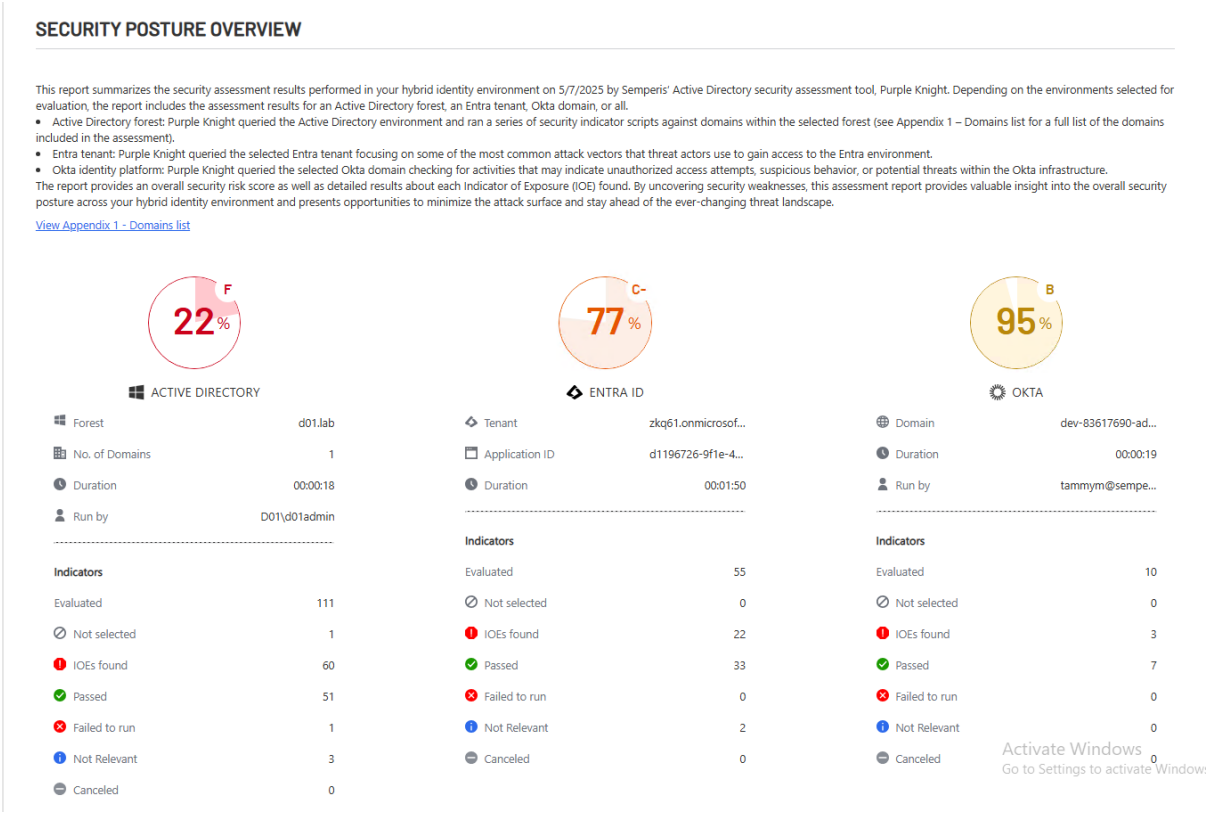
- *Security Posture Overview*: Provides overall security posture score (percentage and letter score), environment details, run details, and evaluation results for each environment included in the security assessment.
- Indicators of Exposure: Includes the following information about the Indicators of Exposure (IOEs) found that focus on risky configurations.
    - *Critical IOEs Found*: Reveals a list of critical Indicators of Exposure (IOEs) found during the assessment.
    - *Additional IOEs Found*: Displays a list of IOEs with a severity level of warning or informational found during the assessment.
- *Indicators Failed To Run*: Displays a list of security indicators that failed to run.
- *Active Directory Results*: Provides a recap of the category scores and details about the individual Active Directory security indicators.
    - *Categories: Active Directory*: Lists the categories, the score for the category, a brief description, and a link to the individual security indicator test descriptions and results.
    - *Test Result Details: Active Directory*: The test results are organized by category and includes details about each security indicator within each category. For each Active Directory security indicator evaluated, the report provides a description of what was evaluated and the meaning of the findings. It also displays the actual test results including potential vulnerabilities and risky configurations that were found.
- *Entra ID Results*: Provides a recap of the Entra ID category score and details about the individual Entra ID security indicators.
    - *Categories: Entra ID*: Lists the categories, the score for the category, a brief description, and a link to the individual security indicator test descriptions and results.
    - *Test Result Details: Entra ID*: For each Entra ID security indicator evaluated, the report provides a description of what was evaluated and the meaning of the findings. It also displays the actual test results including potential vulnerabilities and risky configurations that were found.

- *Okta Results*: Provides a recap of the Okta category score and details about the individual Okta security indicators.
    - *Categories: Okta*: Lists the categories, the score for the category, a brief description, and a link to the individual security indicator test descriptions and results.
    - *Test Result Details: Okta*: For each Okta security indicator evaluated, the report provides a description of what was evaluated and the meaning of the findings. It also displays the actual test results including potential vulnerabilities and risky configurations that were found.
- *Report Appendices*: Appendices are included at the end of the report, which lists the Active Directory domains included in the assessment, explains the scoring method used, provides a breakdown of security indicators within the ANSSI framework, and if applicable provides a list of directory objects returned (that is, if a security indicator scan returns more than 10 objects).

***NOTE**:*
To customize the report, you can add your company logo and replace the introductory paragraph. For more information, see How to Add Company Branding.

Security Posture Overview

The **Security Posture Overview** provides a general description for the Security Assessment report, including the date when report was run, and a link to the Domains list appendix. It also contains the overall security posture score (percentage and letter score), environment details, run details, and evaluation results summary for each environment included in the security assessment.



SECURITY POSTURE OVERVIEW

This report summarizes the security assessment results performed in your hybrid identity environment on 5/7/2025 by Semperis' Active Directory security assessment tool, Purple Knight. Depending on the environments selected for evaluation, the report includes the assessment results for an Active Directory forest, an Entra tenant, Okta domain, or all.

- Active Directory forest: Purple Knight queried the Active Directory environment and ran a series of security indicator scripts against domains within the selected forest (see Appendix 1 – Domains list for a full list of the domains included in the assessment).
- Entra tenant: Purple Knight queried the selected Entra tenant focusing on some of the most common attack vectors that threat actors use to gain access to the Entra environment.
- Okta identity platform: Purple Knight queried the selected Okta domain checking for activities that may indicate unauthorized access attempts, suspicious behavior, or potential threats within the Okta infrastructure.

The report provides an overall security risk score as well as detailed results about each Indicator of Exposure (IOE) found. By uncovering security weaknesses, this assessment report provides valuable insight into the overall security posture across your hybrid identity environment and presents opportunities to minimize the attack surface and stay ahead of the ever-changing threat landscape.

View Appendix 1 - Domains list

F 22% ACTIVE DIRECTORY		C- 77% ENTRA ID		B 95% OKTA	
Forest	d01.lab	Tenant	zkq61.onmicrosof...	Domain	dev-83617690-ad...
No. of Domains	1	Application ID	d1196726-9f1e-4...	Duration	00:00:19
Duration	00:00:18	Duration	00:01:50	Run by	tammym@sempe...
Run by	D01\d01admin				
Indicators		**Indicators**		**Indicators**	
Evaluated	111	Evaluated	55	Evaluated	10
Not selected	1	Not selected	0	Not selected	0
IOEs found	60	IOEs found	22	IOEs found	3
Passed	51	Passed	33	Passed	7
Failed to run	1	Failed to run	0	Failed to run	0
Not Relevant	3	Not Relevant	2	Not Relevant	0
Canceled	0	Canceled	0	Canceled	0

Figure 14: Security Assessment Report > Security Posture Overview

Active Directory

When an Active Directory environment is included in the assessment, the following environment and run details are provided:

- **Forest**: The name of the forest that was evaluated.
- **No. of Domains**: The number of domains that were evaluated.
- **Duration**: The amount of time (hh:mm:ss) it took to generate the assessment report.
- **Run by**: The name of the account that ran the assessment report.

Entra ID

When an Entra ID environment is included in the assessment, the following environment and run details are provided:

- **Tenant**: The name of the Entra tenant that was evaluated.
- **Application ID**: The identifier assigned to the Purple Knight application when it was created in Microsoft Entra.
- **Duration**: The amount of time (hh:mm:ss) it took to generate the assessment report.

Okta

When an Okta environment is included in the assessment, the following environment and run details are provided:

- **Domain**: The name of the Okta domain that was evaluated.
- **Duration**: The amount of time (hh:mm:ss) it took to generate the assessment report.
- **Run by**: The name of the account that ran the assessment report.

The **Security Posture Overview** also summarizes the results of the security indicators included in the current assessment. This summary includes the following information for each environment included in the assessment report:

- **Evaluated**: Number of security indicator tests that successfully completed (returned a result of **Passed** or **IOE Found**).
- **Not selected**: Number of security indicators that were not included in the current assessment.
- **IOEs found**: Number of security indicator tests that returned an **IOE Found** result. That is, a security indicator test that found a security incident or change event regardless of when it occurred.
- **Passed**: Number of tests that passed without finding an IOE.
- **Failed to run**: Number of tests that failed to run.
- **Not relevant**: Number of tests that did not run because they do not apply to the selected environment. For example, if Microsoft LAPS is not implemented in the selected environment, the "Changes to MS LAPS read permissions" security

indicator will return a **Not Relevant** status.

- **Canceled**: Number of tests that were canceled before they finished.

Indicators of Exposure

The **INDICATORS OF EXPOSURE** section includes the following information about the Indicators of Exposure (IOEs) found that focus on risky configurations that could be exploited by an attacker:

- *Critical IOEs Found*: Lists the security indicator tests that found critical IOEs in your Active Directory, Entra ID, or Okta environment.
- *Additional IOEs Found*: Lists the security indicator tests that found an IOE with a warning or informational severity level during the assessment.

Critical IOEs Found

The **CRITICAL IOEs FOUND** section lists the security indicator tests that found critical IOEs in your hybrid identity environment.

Critical IOEs uncover vulnerabilities where an intruder could gain control of the host, which could potentially lead to the compromise of areas within the network system. Vulnerabilities at this level include authentication, encryption, and code issues leading to data manipulation.

To effectively enhance your security posture score, it's essential to focus on addressing the most critical indicators of exposure (IOEs). These IOEs carry the greatest weight in influencing your score. Focusing on remediating these critical items will significantly improve your score and overall security posture.

For each critical IOE found, the following information is provided:

- Indicator representing the environment to which the indicator belongs:
  - : Active Directory
  - : Entra ID
  - : Okta
- Name of the security indicator.
- A partial description of what was evaluated.

- ***Read More***: A link to view the full description and detailed test results for the security indicator.

Additional IOEs Found

The **ADDITIONAL IOEs FOUND** section lists the security indicator tests that found an IOE with a warning or informational severity level.

- IOEs assigned a warning severity level reveal that an intruder may be able to collect sensitive information from the host, such as the precise version of installed software. With this information, an intruder can easily exploit known vulnerabilities specific to software versions.
- IOEs assigned an informational severity level disclose when an intruder can collect information about the host (such as open ports, services, and so on) and may be able to use this information to find other vulnerabilities.

This list includes the following information for each additional IOE found:

- **NAME**: The name of the security indicator.
- **PLATFORM**: The environment evaluated: AD, Entra ID, or Okta.
- **SEVERITY LEVEL**: The severity level assigned to the security indicator.
- **ACTION**: Click the ***Read More*** link to display the description and detailed test results for the security indicator.

Indicators Failed To Run

The **INDICATORS FAILED TO RUN** section lists the security indicator tests that failed to run. Note that indicators that fail to run do NOT affect the security posture scores.

This list includes the following information for each security indicator test that failed to run:

- **Name**: The name of the security indicator.
- **Platform**: The environment to which the security indicator applies: AD, Entra ID, or Okta.
- **Severity Level**: The severity level assigned to the security indicator.
- **Action**: Click the ***Read More*** link to display a description of the security indicator including a message as to why the security indicator did not run.

Active Directory Results

The **Active Directory Results** section in the assessment report provides a recap of the category scores and details about the individual Active Directory security indicators.

- *Categories: Active Directory*
- *Test Result Details: Active Directory*

Categories: Active Directory

The **Categories** subsection in the **Active Directory Results** section provides a recap of the category scores.

> ***NOTE:***
> *It is important to note that category scores do not contribute to the calculation of the overall security posture score. As such, there is no direct correlation between category scores and the overall score. Instead, each category score should be regarded as an independent metric that can be compared to its future values, serving as a valuable tool for tracking progress in remediation efforts.*

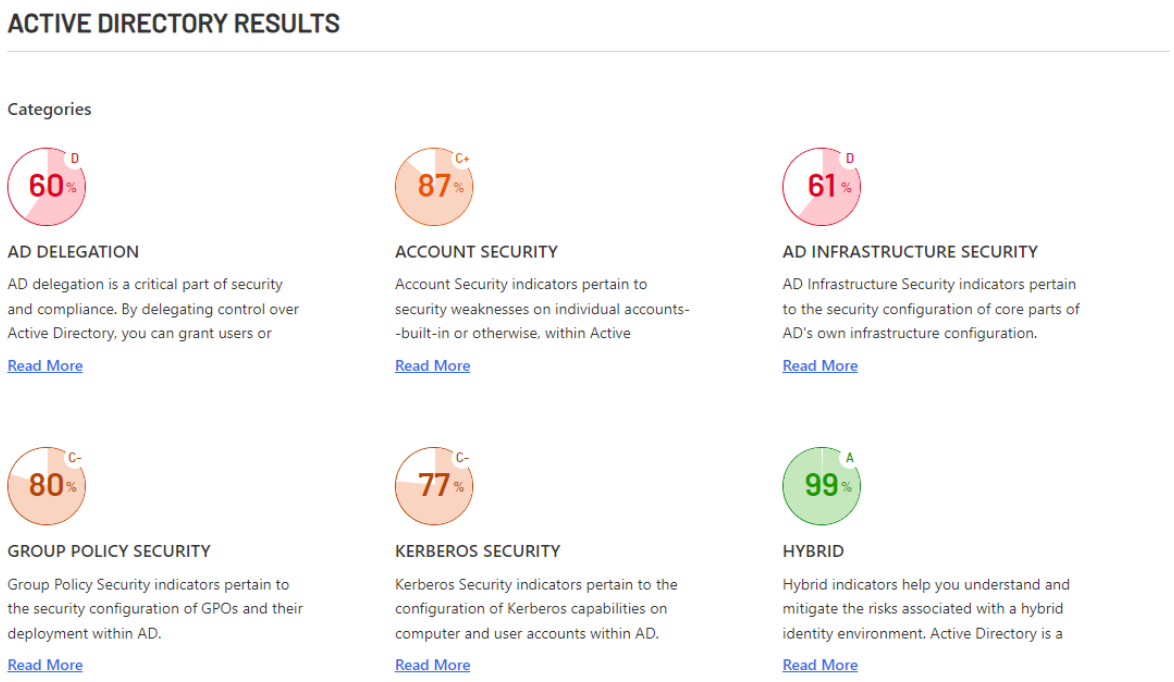


Figure 15: Security Assessment report: AD Results > Categories

The following category summary information is provided:

- **Score**: A percentage and letter grade for each category based on the test results and weight of each security indicator that was evaluated within the selected category. For more information on the scoring method used, see the *Scoring method* appendix.

  N/A is displayed if no security indicators within the category were selected for inclusion in the assessment report, if all the scripts within the category failed to run, or the assessment was canceled on the **Progress** page before any security indicator tests completed.
- **Category name and description**: The name of the category followed by a partial description of the type of security indicators included in the category.
- ***Read More***: A link to the full description and detailed test results for each security indicator in the category.

Test Result Details: Active Directory

For each Active Directory security indicator evaluated, the Security Assessment report provides details about the individual security indicator and any potential weaknesses or risky configurations found. This section is organized by category and includes details about each security indicator within each category.

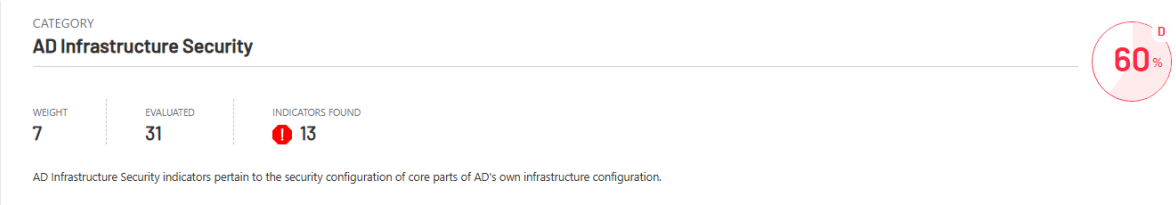


Figure 16: Security Assessment report: AD Infrastructure Security category results

Each security indicator is listed under its associated category and includes the following category information:

- **Category name**: The name of the category.
- **Category score**: A percentage and letter grade for the category based on the test results and weight of each security indicator that was evaluated within the category.

  N/A is displayed if there were no security indicators within the category selected for inclusion in the report or if the test failed to run.

- **Weight**: The weight assigned to the category, which is based on the weight of each security indicator evaluated within the relevant category.
- **Evaluated**: The number of security indicators in the category selected for evaluation.
- **Indicators Found**: The total number of indicators that returned an **IOE Found** results within the category.
- **Description**: A general description of the type of security indicators included in the category.

Following the category summary, the test result details for each security indicator is displayed.

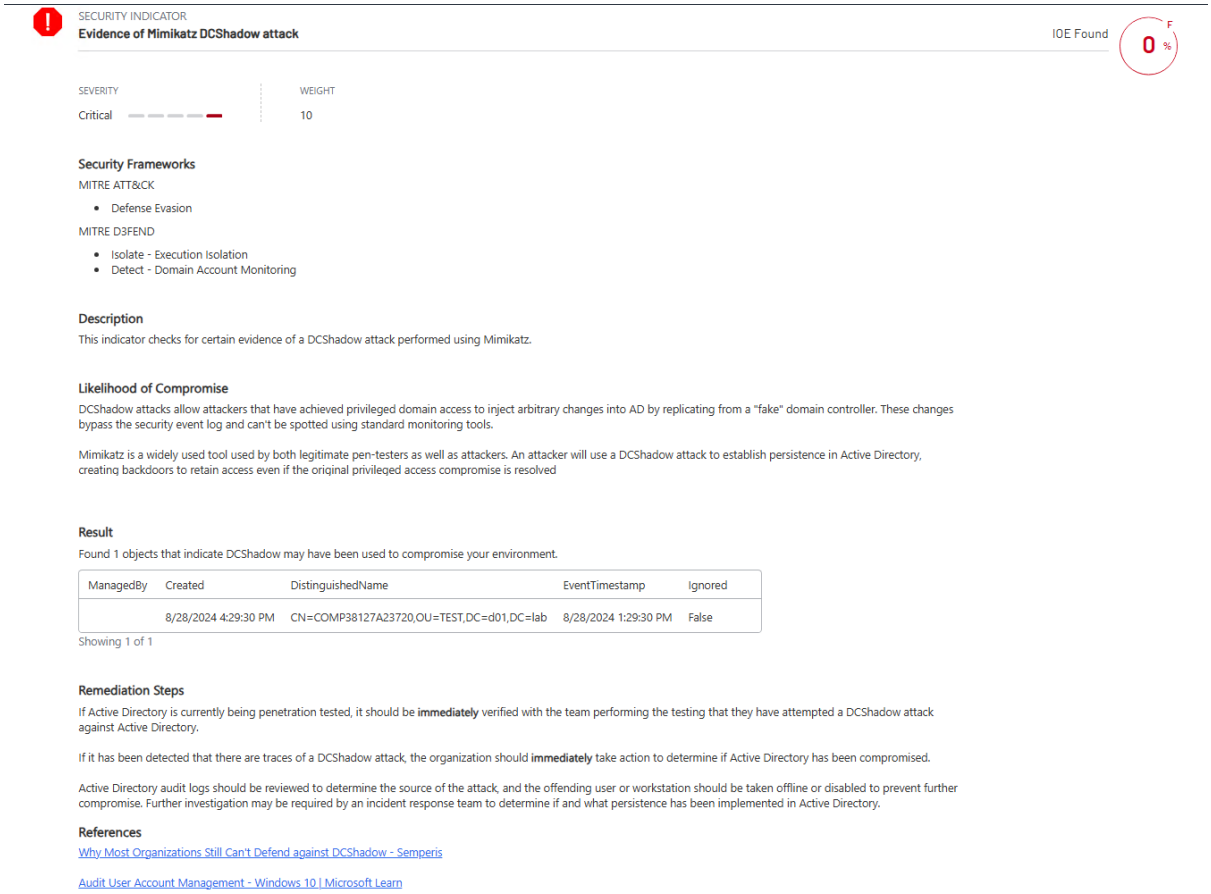


*Figure 17: Security Assessment report: **IOE Found** results for an AD indicator*

The following details are provided for each security indicator that was evaluated:

- **Status Indicator**: Indicates the results state of the security indicator test that was run:

   IOE Found.

   Pass. Passed without triggering an indicator.

   Failed to Run.

   Not Relevant. Security indicator does not apply to selected environment.

   Canceled. Canceled before test completed.

   Not Selected. Security indicator was not selected for inclusion in the current report.

- **Name**: The name of the security indicator.
- **Status**: Displays whether the security indicator script successfully ran and if an IOE was found.
  - **IOE Found**: Security indicator script completed successfully but found an event (IOE).
  - **Pass**: Security indicator script completed successfully and did not trigger an indicator.
  - **Failed to run**: Security indicator script failed to run (e.g. inefficient credentials).
  - **Canceled**: Security indicator test was canceled before it completed.
  - **Not Relevant**: Security indicator test that cannot be run because it does not apply to the selected environment. For example, if Microsoft LAPS is not implemented in the selected environment, the "Changes to MS LAPS read permissions" security indicator will return a **Not Relevant** status.
  - **Not Selected**: Security indicator was not selected for inclusion in the current report.
- **Score**: A percentage and letter grade for the individual security indicator.

  N/A is displayed if the security indicator was not selected for inclusion in the report, if the script failed to run, or if it was canceled before it completed.

- **Severity**: The severity level assigned to the security indicator based on proven risk analysis. Valid severity levels include: Informational (Blue), Low (Yellow), Medium (Orange), High (Red), and Critical (Dark Red).
- **Weight**: The weight, which is a value between 1 and 10, assigned to the security indicator, based on the likelihood of compromise and a defined rating/risk level. Security indicators that expose riskier vulnerabilities in an AD environment are assigned a higher weight.
- **Security Frameworks**: The different security frameworks that are addressed by the security indicator. For example, the MITRE ATT&CK® categories, MITRE D3FEND™ cybersecurity countermeasure, or ANSSI rules that correlate to the adversary tactic, technique, or process being evaluated by the security indicator.
- **Description**: A general description of what was evaluated and the meaning of the findings.
- **Likelihood of Compromise**: Indicates how likely the exposed weakness or risky configuration is to cause a compromise in Active Directory, as well as the severity of the potential compromise if not addressed.
- **Result**: The security indicator test results or findings.
    - If the security indicator test found an IOE, this field provides a list of AD objects found that caused the security event (IOE). For example, for users with the "password never expires" flag set, this pane displays the users that are found to have this setting.

      If the list is lengthy (more than 10 objects by default), there will be a link to the results appendix instead of including all the results within the report.

NOTE:
*An Excel file that includes all of the scan results is automatically created and saved in the **Output** folder under the **PurpleKnight** directory. This Excel spreadsheet contains multiple tabs (Summary tab and a tab for each indicator that returned results) that lists all of the directory objects returned.*

*If the creation of the Excel file fails due to Excel's limitations for number of columns, rows, or characters in a cell, a .csv file is created for each Excel tab and is saved in the **Output** folder under the **PurpleKnight** directory.*

  - If the security indicator test failed to run, this field displays an error message describing why the script failed.
  - If the security indicator test passed without detecting an event (IOE), this field displays **No evidence of exposure**.
  - If the security indicator was not selected, the **Result** section is not displayed.
- **Remediation Steps**: Provides suggested corrective action that can be taken to reduce your Active Directory attack surface.
  - If the security indicator test passed without detecting an event (IOE) or failed to run, this field displays **None**.
  - If the security indicator was not selected for evaluation, the **Remediation Steps** section is not displayed.

Entra ID Results

The **Entra ID Results** section in the assessment report provides a recap of the category scores and details about the individual Entra ID security indicators.

- *Categories: Entra ID*
- *Test Result Details: Entra ID*

Categories: Entra ID

The **Categories** subsection in the **Entra ID Results** section provides a recap of the category scores.

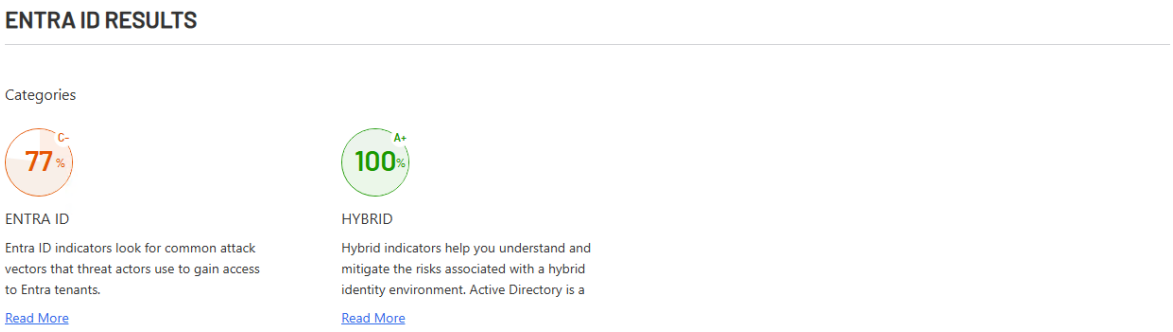


Figure 18: Security Assessment report: Entra ID Results > Categories

The following category summary information is provided:

- **Score**: A percentage and letter grade for each category based on the test results and weight of each security indicator that was evaluated within the selected category. For more information on the scoring method used, see the *Scoring method* appendix.

  N/A is displayed if no security indicators within the category were selected for inclusion in the assessment report, if all the scripts within the category failed to run, or the assessment was canceled on the **Progress** page before any security indicator tests completed.
- **Category name and description**: The name of the category followed by a partial description of the type of security indicators included in the category.
- ***Read More***: A link to the full description and detailed test results for each security indicator in the category.

Test Result Details: Entra ID

For each Entra ID security indicator evaluated, the Security Assessment report provides details about the individual security indicator and potential weaknesses or risky configurations found. This section is organized by category and includes details about Entra ID security indicators.

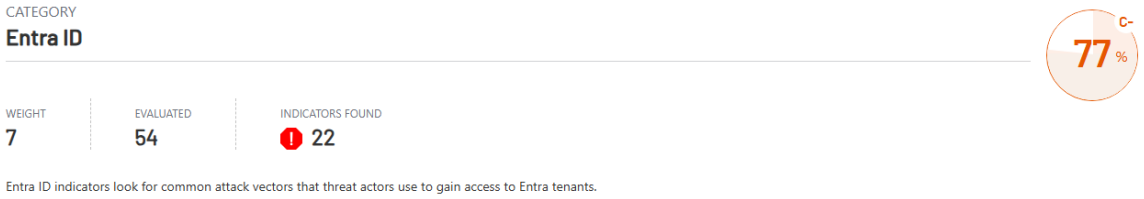


Figure 19: Security Assessment Report: Entra ID category results

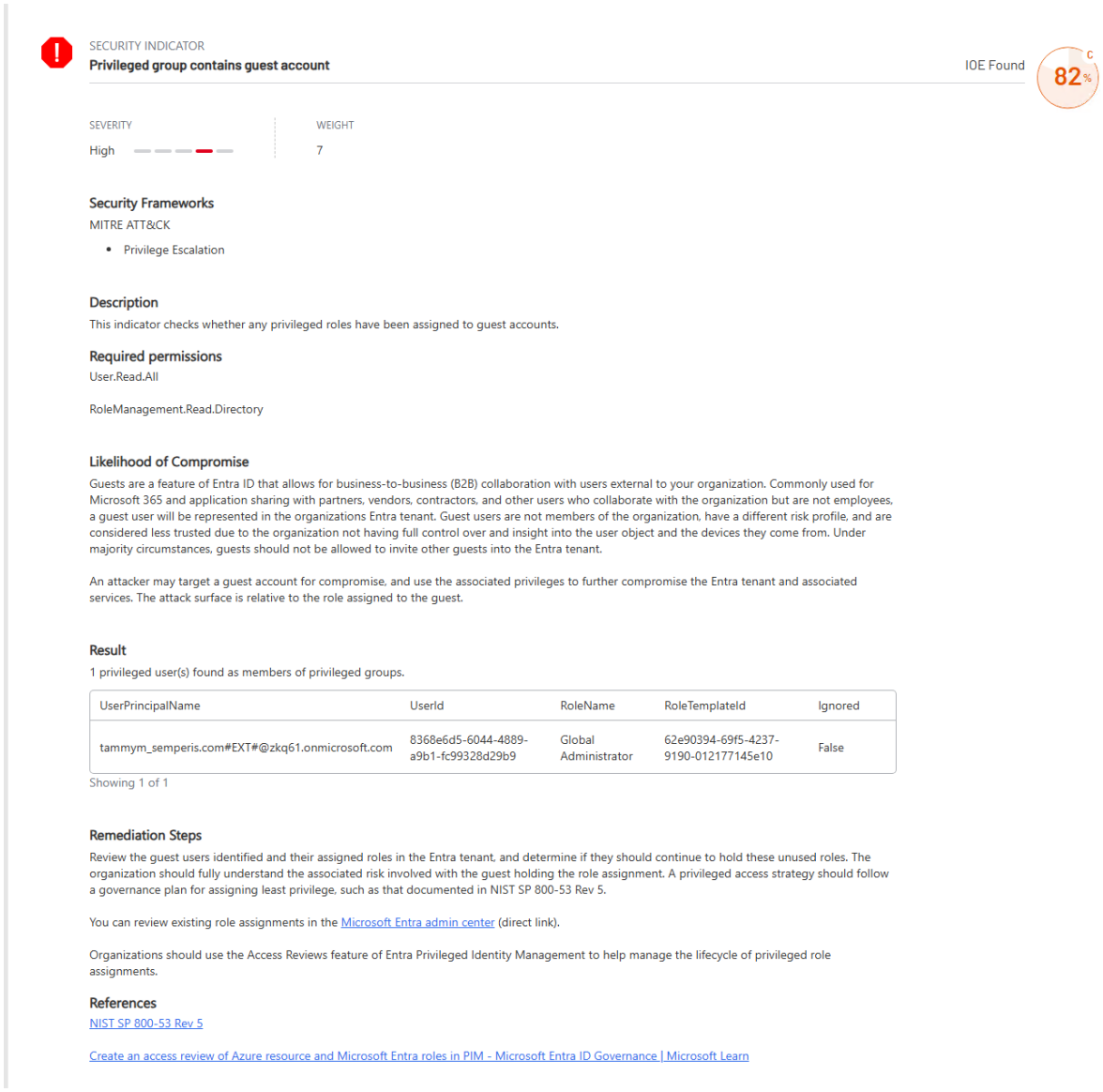
Entra ID indicators are listed under its associated category and includes the following category information:

- **Category name**: The name of the category (Entra ID or Hybrid).
- **Category score**: A percentage and letter grade for the Entra ID category based on the test results and weight of each security indicator that was evaluated within the category.

  N/A is displayed if there were no security indicators within the category selected for inclusion in the report.

- **Weight**: The weight assigned to the category, which is based on the weight of each security indicator evaluated within the category.
- **Evaluated**: The number of security indicators in the category selected for evaluation.
- **Indicators Found**: The total number of indicators that returned an **IOE Found** results within the category.
- **Description**: A general description of the type of security indicators included in the Entra ID category.

Following the category summary, the test result details for each security indicator is displayed.



SECURITY INDICATOR

Privileged group contains guest account

IOE Found

82%

SEVERITY	WEIGHT
High	7

Security Frameworks

MITRE ATT&CK

- Privilege Escalation

Description

This indicator checks whether any privileged roles have been assigned to guest accounts.

Required permissions

User.Read.All

RoleManagement.Read.Directory

Likelihood of Compromise

Guests are a feature of Entra ID that allows for business-to-business (B2B) collaboration with users external to your organization. Commonly used for Microsoft 365 and application sharing with partners, vendors, contractors, and other users who collaborate with the organization but are not employees, a guest user will be represented in the organizations Entra tenant. Guest users are not members of the organization, have a different risk profile, and are considered less trusted due to the organization not having full control over and insight into the user object and the devices they come from. Under majority circumstances, guests should not be allowed to invite other guests into the Entra tenant.

An attacker may target a guest account for compromise, and use the associated privileges to further compromise the Entra tenant and associated services. The attack surface is relative to the role assigned to the guest.

Result

1 privileged user(s) found as members of privileged groups.

UserPrincipalName	UserId	RoleName	RoleTemplateId	Ignored
tammym_semperis.com#EXT#@zkq61.onmicrosoft.com	8368e6d5-6044-4889-a9b1-fc99328d29b9	Global Administrator	62e90394-69f5-4237-9190-012177145e10	False

Showing 1 of 1

Remediation Steps

Review the guest users identified and their assigned roles in the Entra tenant, and determine if they should continue to hold these unused roles. The organization should fully understand the associated risk involved with the guest holding the role assignment. A privileged access strategy should follow a governance plan for assigning least privilege, such as that documented in NIST SP 800-53 Rev 5.

You can review existing role assignments in the Microsoft Entra admin center (direct link).

Organizations should use the Access Reviews feature of Entra Privileged Identity Management to help manage the lifecycle of privileged role assignments.

References

NIST SP 800-53 Rev 5

Create an access review of Azure resource and Microsoft Entra roles in PIM - Microsoft Entra ID Governance | Microsoft Learn

*Figure 20: Security Assessment Report: **IOE Found** results for an Entra ID indicator*

The following details are provided for each Entra ID security indicator that was evaluated:

- **Status Indicator**: Indicates the results state of the security indicator test that was run:

   IOE Found.

   Pass. Passed without triggering an indicator.

   Failed to Run.

   Not Relevant.

   Canceled. Canceled before test completed.

   Not Selected. Security indicator was not selected for inclusion in the current report.

- **Name**: The name of the security indicator.
- **Status**: Displays whether the security indicator script successfully ran and if an IOE was found.
  - **IOE Found**: Security indicator script completed successfully but found an event (IOE).
  - **Pass**: Security indicator script completed successfully and did not trigger an indicator.
  - **Failed to run**: Security indicator script failed to run (e.g. inefficient credentials).
  - **Canceled**: Security indicator test was canceled before it completed.
  - **Not Relevant**: Security indicator test that cannot be run because it does not apply to the selected environment.
  - **Not Selected**: Security indicator was not selected for inclusion in the current report.
- **Score**: A percentage and letter grade for the individual security indicator.

  N/A is displayed if the security indicator was not selected for inclusion in the report, or if the script failed to run, was not relevant, or was canceled before it completed.
- **Severity**: The severity level assigned to the security indicator based on proven risk analysis. Valid severity levels include: Informational (), Low (Yellow), Medium (Orange), High (Red), and Critical (Dark Red).

- **Weight**: The weight, which is a value between 1 and 10, assigned to the security indicator, based on the likelihood of compromise and a defined rating/risk level. Security indicators that expose riskier vulnerabilities in an Entra ID environment are assigned a higher weight.
- **Security Frameworks**: The different security frameworks that are addressed by the security indicator. For example, the MITRE ATT&CK® categories, MITRE D3FEND™ cybersecurity countermeasure, or ANSSI rules that correlate to the adversary tactic, technique, or process being evaluated by the security indicator.
- **Description**: A general description of what was evaluated and the meaning of the findings.
- **Likelihood of Compromise**: Indicates how likely the exposed weakness or risky configuration is to cause a compromise in Entra ID, as well as the severity of the potential compromise if not addressed.
- **Result**: The security indicator test results or findings.
    - If the security indicator test found an IOE, this field explains the results that were found to cause the IOE.
    - If the security indicator test failed to run, this field displays an error message describing why the script failed.
    - If the security indicator test passed without detecting an event (IOE), this field displays **No evidence of exposure**.
    - If the security indicator was not selected, the **Result** section is not displayed.
- **Remediation Steps**: Provides suggested corrective action that can be taken to reduce your Entra ID attack surface.
    - If the security indicator test passed without detecting an event (IOE), or the script failed to run or was not relevant, this field displays **None**.
    - If the security indicator was not selected for evaluation, the **Remediation Steps** section is not displayed.

Okta Results

The **Okta Results** section in the assessment report provides a recap of the category scores and details about the individual Okta security indicators.

- *Categories: Okta*
- *Test Result Details: Okta*

Categories: Okta

The **Categories** subsection in the **Okta Results** section provides a recap of the Okta category score.

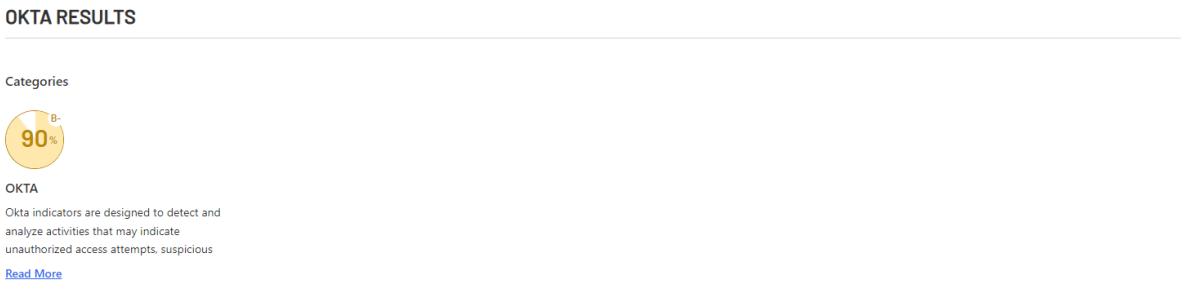


Figure 21: Security Assessment report: Okta Results > Categories

The following category summary information is provided:

- **Score**: A percentage and letter grade for each category based on the test results and weight of each security indicator that was evaluated within the selected category. For more information on the scoring method used, see the *Scoring method* appendix.

  N/A is displayed if no security indicators within the category were selected for inclusion in the assessment report, if all the scripts within the category failed to run, or the assessment was canceled on the **Progress** page before any security indicator tests completed.
- **Category name and description**: The name of the category followed by a partial description of the type of security indicators included in the category.
- ***Read More***: A link to the full description and detailed test results for each security indicator in the category.

Test Result Details: Okta

For each Okta security indicator evaluated, the Security Assessment report provides details about the individual security indicator and potential weaknesses or risky configurations found. This section is organized by category and includes details about Okta security indicators.

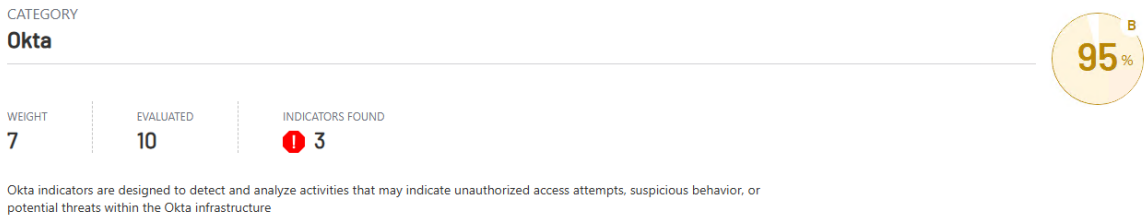


Figure 22: Security Assessment Report: Okta category results

Okta indicators are listed under its associated category and includes the following category information:

- **Category name**: The name of the category (Okta).
- **Category score**: A percentage and letter grade for the Okta category based on the test results and weight of each security indicator that was evaluated within the category.

  N/A is displayed if there were no security indicators within the category selected for inclusion in the report.
- **Weight**: The weight assigned to the category, which is based on the weight of each security indicator evaluated within the category.
- **Evaluated**: The number of security indicators in the category selected for evaluation.
- **Indicators Found**: The total number of indicators that returned an **IOE Found** results within the category.
- **Description**: A general description of the type of security indicators included in the Okta category.

Following the category summary, the test result details for each security indicator is displayed.

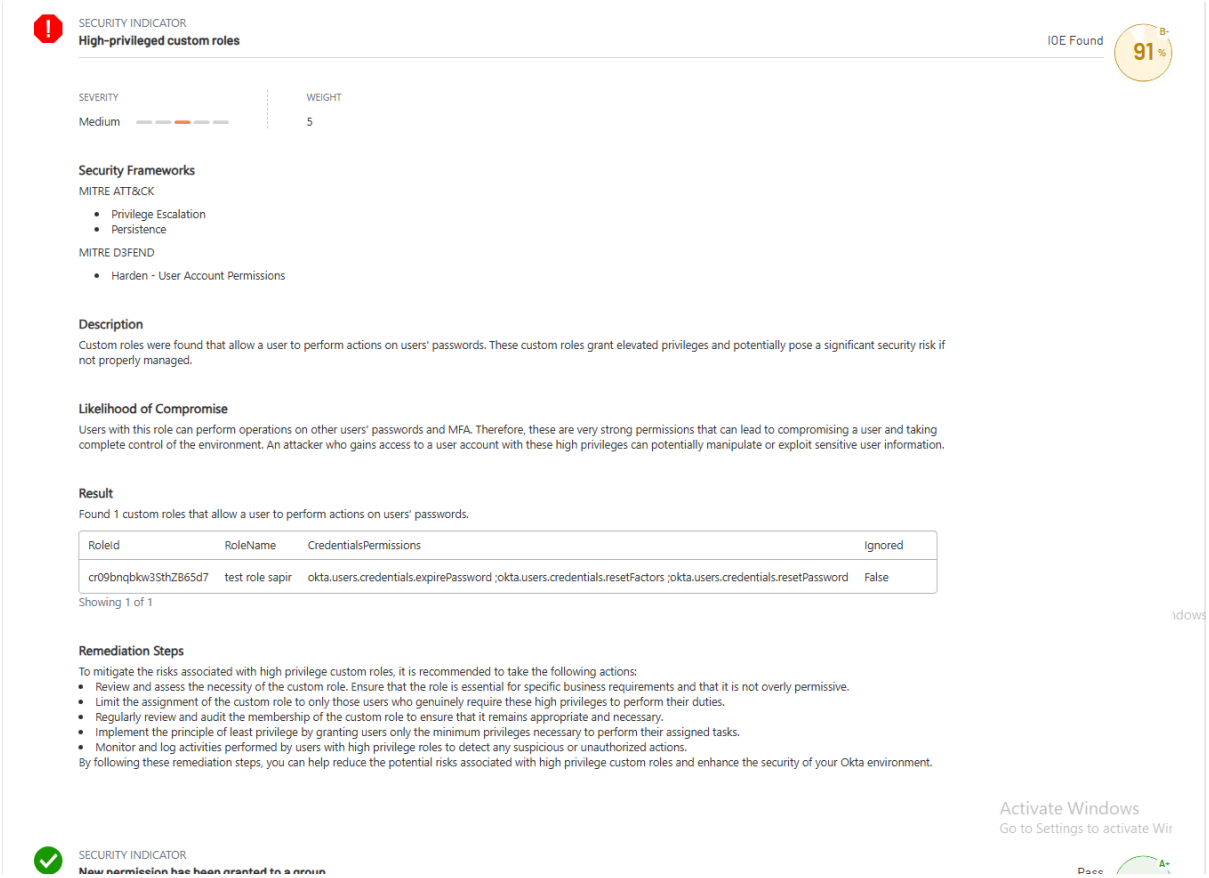


*Figure 23: Security Assessment Report: **IOE Found** results for an Okta indicator*

The following details are provided for each Okta security indicator that was evaluated:

- **Status Indicator**: Indicates the results state of the security indicator test that was run:

  IOE Found.

  Pass. Passed without triggering an indicator.

  Failed to Run.

  Not Relevant.

  Canceled. Canceled before test completed.

  Not Selected. Security indicator was not selected for inclusion in the current report.

- **Name**: The name of the security indicator.

- **Status**: Displays whether the security indicator script successfully ran and if an IOE was found.
  - **IOE Found**: Security indicator script completed successfully but found an event (IOE).
  - **Pass**: Security indicator script completed successfully and did not trigger an indicator.
  - **Failed to run**: Security indicator script failed to run (e.g. inefficient credentials).
  - **Canceled**: Security indicator test was canceled before it completed.
  - **Not Relevant**: Security indicator test that cannot be run because it does not apply to the selected environment.
  - **Not Selected**: Security indicator was not selected for inclusion in the current report.
- **Score**: A percentage and letter grade for the individual security indicator.

  N/A is displayed if the security indicator was not selected for inclusion in the report, or if the script failed to run, was not relevant, or was canceled before it completed.
- **Severity**: The severity level assigned to the security indicator based on proven risk analysis. Valid severity levels include: Informational (Blue), Low (Yellow), Medium (Orange), High (Red), and Critical (Dark Red).
- **Weight**: The weight, which is a value between 1 and 10, assigned to the security indicator, based on the likelihood of compromise and a defined rating/risk level. Security indicators that expose riskier vulnerabilities in an Okta environment are assigned a higher weight.
- **Security Frameworks**: The different security frameworks that are addressed by the security indicator. For example, the MITRE ATT&CK® categories, MITRE D3FEND™ cybersecurity countermeasure, or ANSSI rules that correlate to the adversary tactic, technique, or process being evaluated by the security indicator.
- **Description**: A general description of what was evaluated and the meaning of the findings.
- **Likelihood of Compromise**: Indicates how likely the exposed weakness or risky configuration is to cause a compromise in your Okta infrastructure, as well as the severity of the potential compromise if not addressed.

- **Result**: The security indicator test results or findings.
  - If the security indicator test found an IOE, this field explains the results that were found to cause the IOE.
  - If the security indicator test failed to run, this field displays an error message describing why the script failed.
  - If the security indicator test passed without detecting an event (IOE), this field displays **No evidence of exposure**.
  - If the security indicator was not selected, the **Result** section is not displayed.
- **Remediation Steps**: Provides suggested corrective action that can be taken to reduce your Okta attack surface.
  - If the security indicator test passed without detecting an event (IOE), or the script failed to run or was not relevant, this field displays **None**.
  - If the security indicator was not selected for evaluation, the **Remediation Steps** section is not displayed.

Report Appendices

The Security Assessment report contains the following appendices, which provide additional supporting information:

- **Domains list** appendix provides a list of domains included in the Active Directory assessment.
- **Scoring method** appendix provides a brief description of the scoring method used to calculate the percentage and letter grades presented in the report.
- **ANSSI Scorecard** appendix displays a breakdown of security indicators within the French National Agency for the Security of Information Systems (ANSSI) framework. Clicking the ***Full Results*** link in the **ACTION** column displays the assessment details for the selected indicator.
- **Results** appendix displays the results of individual security indicator scans that return a long list of directory objects that caused the security event (IOE). The security indicator results (list of directory objects) is usually included in the test results within the assessment report; it is only included as an appendix when the list exceeds the defined limit, which is more than 10 directory objects by default.

***NOTE**:*
*An Excel file that includes all of the scan results is automatically created and saved in the **Output** folder under the **PurpleKnight** directory. This Excel spreadsheet contains multiple tabs (Summary tab and a tab for each indicator that returned results) that lists all of the directory objects returned.*

*If the creation of the Excel file fails due to Excel's limitations for number of columns, rows, or characters in a cell, a .csv file is created for each Excel tab and is saved in the **Output** folder under the **PurpleKnight** directory.*

APPENDIX A

Scoring method

The scores included in this report reveal the security posture of the environments that were assessed. Scores are represented by percentage and letter grade. These grades, which offer a nuanced view of the environment's security state, serve as a complementary metric to help you interpret your security posture.

It is recommended to aim for the highest score possible; a 100% (A+) score indicates that there were no security exposures found for the security indicators that were assessed. To effectively enhance your security posture score, it's essential to focus on addressing the most critical indicators of exposure (IOEs). These IOEs carry the greatest weight in influencing your score. Indicators with lower severity will have a corresponding minor effect on the overall score. Focusing on remediating these critical items will significantly improve your score and overall security posture.

The Security Assessment report provides the following scores:

- **Security Indicator score**: Each individual security indicator evaluated is assigned a percentage and grade according to its internal logic and the results found. Each individual security indicator is assigned a weight (value between 1-10) according to the risk of the IOE found and the likelihood of compromise. This weighted value, together with the quantity and impact of detected issues and a general factor of the industry risk, affects the score assigned to the relevant category.
- **Category score**: The security indicators included in the tool cover a range of categories that represent different aspects of Active Directory's security posture. The primary factors influencing category scores are the severity of identified exposures and the quantity of indicators within that category that detect these exposures.

  It is important to note that category scores do not factor into the overall score's calculation. As such, there is no direct correlation between category scores and the overall score. Instead, each category score should be regarded as an

independent metric that can be compared to its future values, serving as a valuable tool for tracking progress in remediation efforts.

- **Overall security posture score**:The overall security posture score focuses solely on "failed" indicators. This adjustment aligns the overall score more accurately with the severity and impact of security exposures in your environment.

> ***NOTE**:*
> *When calculating the scores, only security indicators that resulted in IOEs found are included. Security indicators that were not selected, canceled, passed, or failed to run are not taken into account. For an accurate security posture assessment, it is recommended that you include all security indicators and all domains in the selected Active Directory forest.*

The scoring system places more emphasis on the severity of the indicators and the volume of objects found for each indicator. In essence, the overall score is now more influenced by the severity of the indicators and their respective impact on your environment. As mentioned above, critical IOEs have the most substantial impact on your score.

Letter grade

Each score is assigned a suitable letter grade as described in the following table.

Table 7: Scoring legend

Letter Grade	Percentage
A+	100
A	99
A-	98
B+	96-97
B	93-95
B-	90-92
C+	86-89

Letter Grade	Percentage
C	81-85
C-	75-80
D+	67-74
D	58-66
D-	44-57
F	0-43

Risk factors

To determine the risk level of a particular security indicator, the following factors are taken into consideration:

- Severity (Low, Medium, High, Critical)

> ***NOTE:***
> *Security indicators with a severity of "Informational" are not taken into account when calculating the security posture score.*

- Likelihood of compromise
- Number and impact of detected issues
- The *DREAD Threat Probability Matrix* , which is included in the appendix of the Security Assessment report.

DREAD Threat Probability Matrix

Table 8: DREAD Threat Probability Matrix

DREAD		High (3)	Medium (2)	Low(1)
Damage potential	How bad would the attack be?	Significant damage. The attacker can subvert the security system and gain full trust authorization.	Moderate damage. The attacker can access/leak sensitive information.	Minimal damage. The attacker can only access/leak trivial information.
Reproducibility	How easy would it be to recreate the attack?	The attack can be consistently reproduced and does not require a specific timing window.	The attack can be reproduced, but only within a specific timing window and in a particular sequence.	The attack is very difficult to reproduce, even with knowledge of the security weakness/vulnerability.
Exploitability	How easy would it be to launch the attack?	A novice programmer could perform the attack with minimal effort.	Requires a skilled programmer to launch the attack and be able to repeat the steps.	Requires an extremely skilled programmer with in-depth knowledge to launch an attack.
Affected users	How many users would be impacted?	A large percentage or all users are impacted; default configuration and key customers are impacted.	A moderate percentage of users are impacted; non-default configuration is impacted.	A very small percentage of users are impacted; anonymous users are affected.
Discoverability	How each would it be for the attacker to discover this exposure?	Easily discovered. Published information explains the vulnerability and attack technique.	Would require some effort to discover and successfully exploit.	Hard to discover. The issue is obscure, and it is unlikely that users would discover a way to cause damage.

DREAD		High (3)	Medium (2)	Low(1)
		The vulnerability is found in commonly used features and is very noticeable.	The vulnerability is found in a seldomly-used part of the product and only a few users should discover it.	

Hybrid Category Scoring and Placement

Hybrid indicators help you understand and mitigate the risks associated with a hybrid identity environment. Active Directory is a perimeter point for Entra ID and a popular attack vendor. So understanding where the Active Directory perimeter is connecting to Entra ID provides clarity for how to secure the Active Directory entry point.

A Hybrid indicator can have their score calculated into either the overall AD security posture score or the Entra ID score. In addition, the Hybrid category and indicators can appear either under the Active Directory Results or Entra ID Results section within the Security Assessment report. How a Hybrid indicator score is calculated and where it is included in the report depends on the target environment and the data source for the indicator:

- Hybrid indicators have both the AD and Entra ID target.
- If the data source for a hybrid indicator only includes AAD.GraphAPI, the indicator is included in the Entra ID score and the Entra ID Results section.
- If the data source for a hybrid indicator only includes AD.LDAP, the indicator is included in the overall AD security posture score and is included in the Active Directory Results section.
- If the data source includes both AAD.GraphAPI and AD.LDAP, the hybrid indicator will only appear if both the Active Directory forest and Entra tenant environment information are provided.

To explain this, the following table lists the Hybrid indicators included in Purple Knight, their target (environment), data source, score where it is included, and placement in the report.

Table 9: Hybrid category: Scoring and placement in report

Security Indicator	Target	Data Source	Score	Security Assessment Report
AD privileged users that are synced to Entra ID	AD; Entra ID	AD.LDAP AAD.GraphAPI	Entra ID	Entra ID Results
Entra ID privileged users that are also privileged in AD	AD; Entra ID	AD.LDAP AAD.GraphAPI	Entra ID	Entra ID Results
Password has synchronization is not enabled	Entra ID	AAD.GraphAPI	Entra ID	Entra ID Results
Resource Based Constrained Delegation applied to AZUREADSSOACC account	AD; Entra ID	AD.LDAP	AD	AD Results
SSO computer account with password last set over 90 days ago	AD; Entra ID	AD.LDAP	AD	AD Results

APPENDIX B

How to Add Company Branding

You can customize Purple Knight in the following ways:

- Add your company name to the header of the tool.
- Add your company logo to the Security Assessment report.
- Replace the introductory paragraph that appears at the beginning of the Security Assessment report.

To add your company name to the tool header:

> ***NOTE:***
> *Maximum characters allowed is 30. If you enter a company name that is longer than 30 characters, the first 30 characters will appear in the header at the top of the tool.*

1. Create a text file called "header.txt" that contains your company name.
2. Place this file in the **custom** folder under the **PurpleKnight** directory (for example, ***<drive/path>*\PurpleKnight\custom\header.txt**).

   Now when you run Purple Knight, (Community edition) will be replaced with (<*CompanyName*> edition) in the banner at the top of the tool.

To add your company logo to the report banner:

> ***NOTE:***
> *The company logo requirements include:*
>
> - *160 x 70 px*
> - *.png, .jpg, or .jpeg format*
> - *no larger than 250 KB*
> - *file name must be logo.png, logo.jpg, or logo.jpeg*

1. Place your company logo file (logo.<*extension*>) in a **custom** folder under the **PurpleKnight** directory. For example:

   <*drive/path*>\PurpleKnight\custom\logo.png

   Now when you run Purple Knight, your company logo will appear in the banner at the top of the Security Assessment report.

To replace the introductory text in the report:

> ***NOTE**:*
> *Maximum characters allowed is 800. If you enter more than 800 characters, the first 800 characters will appear in the report. Only plain text is supported; HTML tags are not supported.*

1. Create a text file called "IntroText.txt" that contains the text that is to replace the introductory paragraph at the beginning of the report.

   The txt file name (IntroText) is case-sensitive.

2. Place this file in the **custom** folder under the **PurpleKnight** directory. For example: **<*drive/path*>\PurpleKnight\custom\IntroText.txt**

   Now when you run Purple Knight, the content of this text file will appear at the beginning of the Security Assessment report.

APPENDIX C

How to Access the Debug Log Level

By default, no debug level or verbose logs are written to the PurpleKnight log.

NOTE:
Local admin rights are required to perform the following procedure.

To access the debug log level in Purple Knight:

1. Set a registry key named **LogLevel** in:

   HKEY_LOCAL_MACHINE\SOFTWARE\Semperis.

2. Set the value to 5.

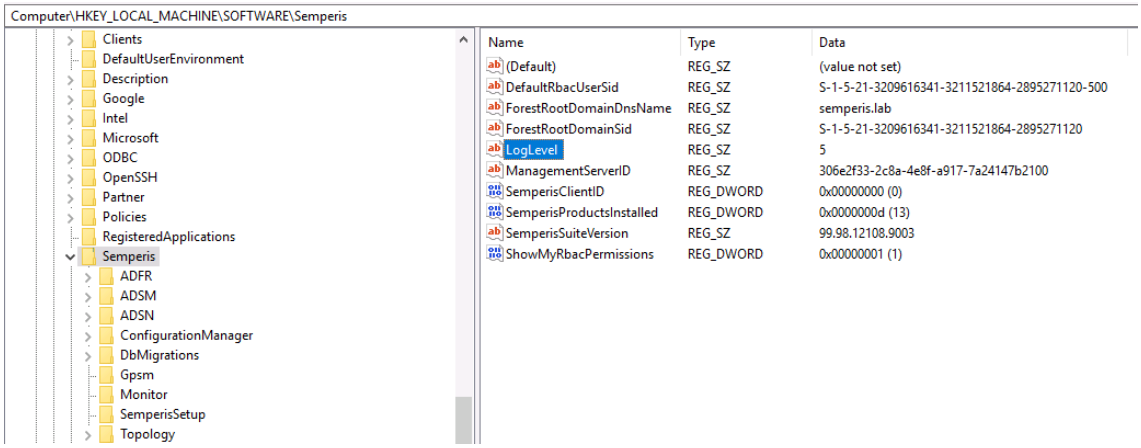


Figure 24: LogLevel registry key

APPENDIX D

Security Indicators: Ignore Lists

An ignore list can be used to "ignore" objects (for example, an account) for a particular indicator after evaluating that the results are considered "accepted" behavior, such as a false positive result or you accept that particular risk. By ignoring objects, you can more accurately assess the risk posed by the remaining objects that are still vulnerable, allowing you to prioritize remediation efforts more effectively to secure your hybrid identity environment.

Once an ignore list is applied, you will continue to see the results in the **Security Assessment Report**, but ignored objects will no longer be used when calculating the security posture scores.

In order to use an ignore list, there are three main steps:

- *Run Security Indicators to Create .json File*
- *Edit .json file*
- *Review Indicator Results*

Run Security Indicators to Create .json File

Prior to using the ignore list functionality, please ensure that you have the latest security indicators deployed.

To check if there is an updated security indicator package available, click the  (**More**) button in the top right corner of any page within Purple Knight, except the **Agreement** page.

When an indicator fails (returns an **IOE found** result), Purple Knight automatically creates the corresponding ignore list template (.json file), which can be found in a Config folder, which is created at the same location as the PurpleKnight executable file:

<*drive:path*>\PurpleKnight\Config

***NOTES**:*

- *The ignore list templates (.json files) use the same name as the indicator script (<ScriptName>.json), not the name displayed in the user interface. Do NOT change the name of the .json files. For a list of security indicators and their corresponding .json file name, see Security Indicator to Ignore List Template Map.*
- *In the .json file, the "Object" properties match the column names displayed in the **Results** pane when an IOE is found. There are different objects returned for each security indicator and therefore there is a specific ignore list template (.json file) for each indicator.*
  Each object property in the .json file includes options that can be edited to specify the criteria to be used to identify the objects to be added to the security indicator's ignore list. For a list of the options supported, see Ignore Options.
  Do NOT change the structure of the "exclude" section in the .json file. JSON files with an invalid format or invalid entry will return a "Failed to run" result.
- *Security indicators without an ignore list function as usual. This is also the case when an unedited ignore list template is created for an indicator.*

Edit .json file

Edit the corresponding ignore list template (.json file), which was automatically created when the security indicator returned an **IOE found** result. Use the options in the "exclude" section to specify the criteria to be used to identify the objects to be added to the security indicator's ignore list. For a list of supported options, see *Ignore Options*.

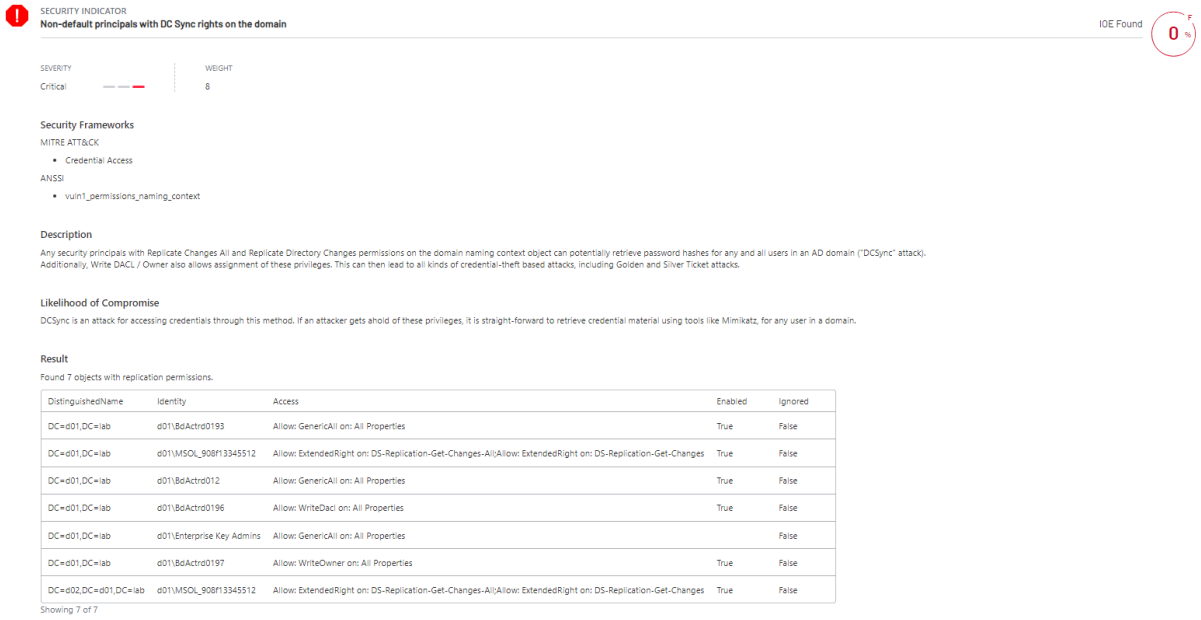
***NOTE**:*
Ensure you are using the correct format and syntax when editing an ignore list template (.json file).

In .json format, the backslash (\) is regarded as an escape character, therefore, you must use a double backslash (\\) when specifying the full name of an object that contains a backslash.

If multiple values are specified, the OR operator applies where only one condition needs to be met.

Example 1: Ignore objects using the "like" option:

In the following example, the "Non-default principals with DC Sync rights on the domain" indicator is returning 7 objects.



SECURITY INDICATOR
Non-default principals with DC Sync rights on the domain

IOE Found 0

SEVERITY: Critical
WEIGHT: 8

Security Frameworks

MITRE ATT&CK
- Credential Access

ANSSI
- vuln1_permissions_naming_context

Description

Any security principals with Replicate Changes All and Replicate Directory Changes permissions on the domain naming context object can potentially retrieve password hashes for any and all users in an AD domain ("DCSync" attack). Additionally, Write DACL / Owner also allows assignment of these privileges. This can then lead to all kinds of credential-theft based attacks, including Golden and Silver Ticket attacks.

Likelihood of Compromise

DCSync is an attack for accessing credentials through this method. If an attacker gets ahold of these privileges, it is straight-forward to retrieve credential material using tools like Mimikatz, for any user in a domain.

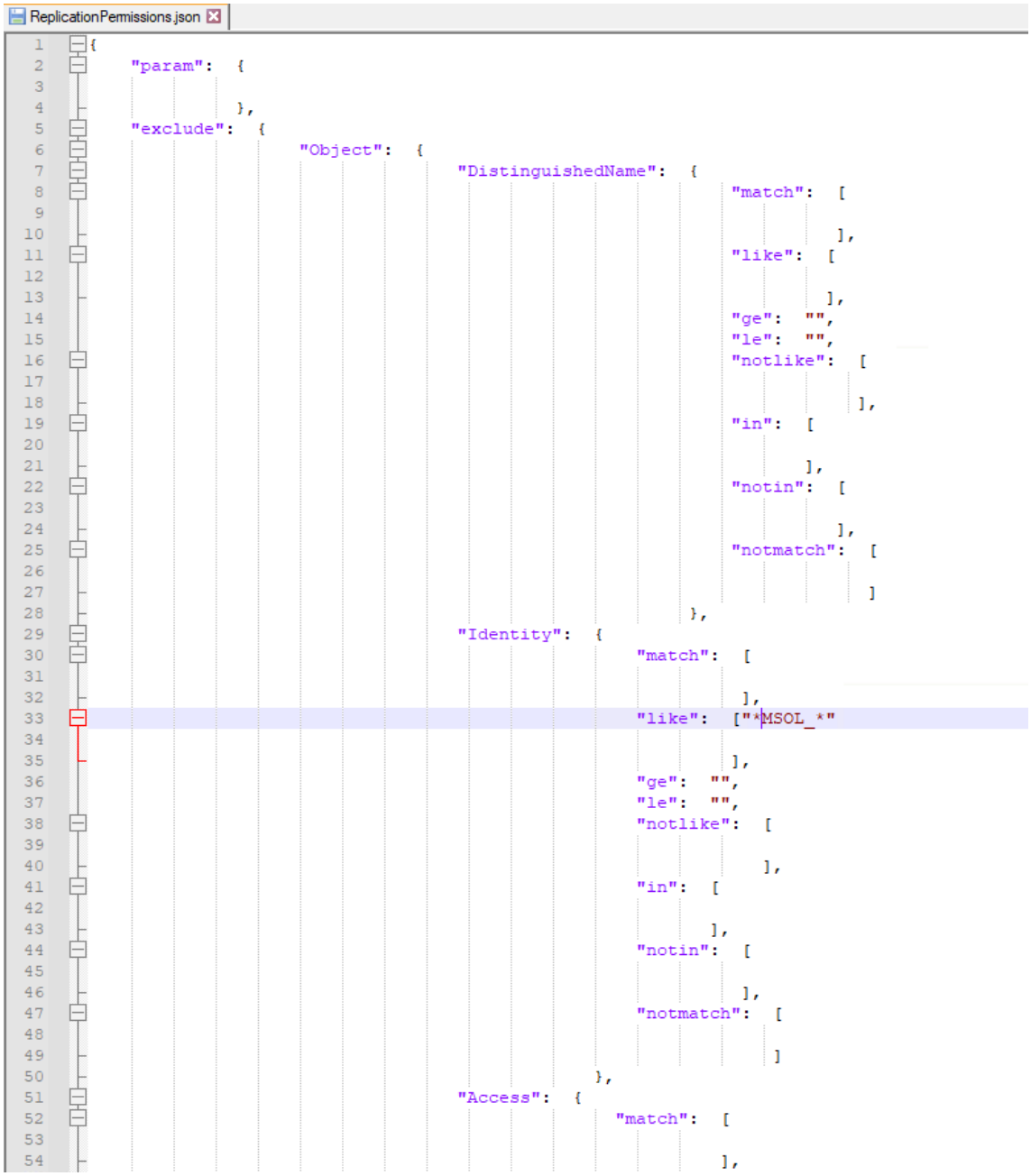
Result

Found 7 objects with replication permissions.

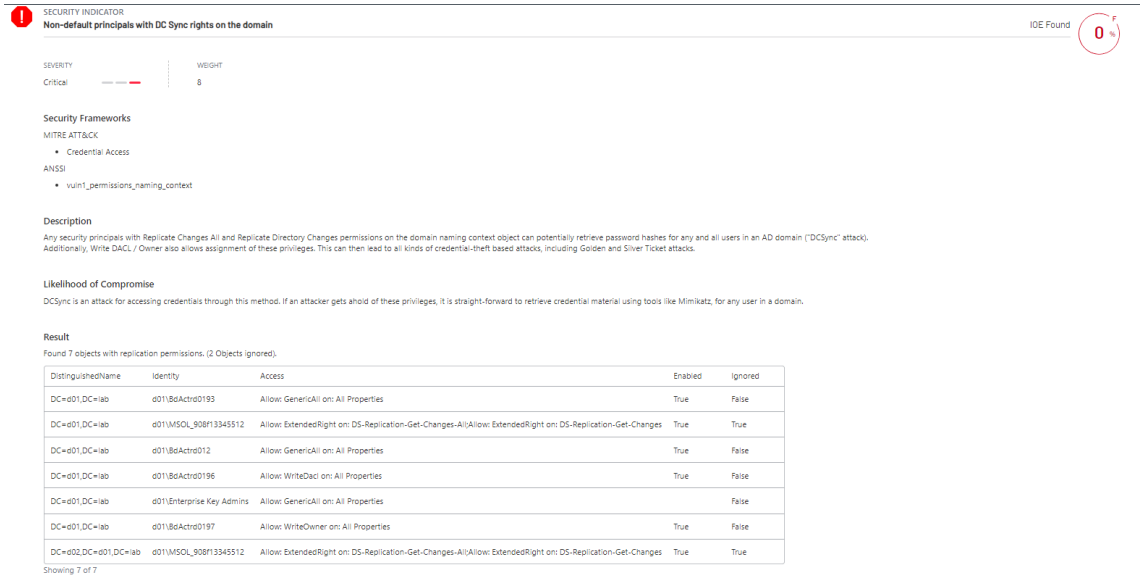
DistinguishedName	Identity	Access	Enabled	Ignored
DC=d01,DC=lab	d01\BdActrd0193	Allow: GenericAll on: All Properties	True	False
DC=d01,DC=lab	d01\MSQL_908f13345512	Allow: ExtendedRight on: DS-Replication-Get-Changes-All\Allow: ExtendedRight on: DS-Replication-Get-Changes	True	False
DC=d01,DC=lab	d01\BdActrd012	Allow: GenericAll on: All Properties	True	False
DC=d01,DC=lab	d01\BdActrd0196	Allow: WriteDacl on: All Properties	True	False
DC=d01,DC=lab	d01\Enterprise Key Admins	Allow: GenericAll on: All Properties		False
DC=d01,DC=lab	d01\BdActrd0197	Allow: WriteOwner on: All Properties	True	False
DC=d02,DC=d01,DC=lab	d01\MSQL_908f13345512	Allow: ExtendedRight on: DS-Replication-Get-Changes-All\Allow: ExtendedRight on: DS-Replication-Get-Changes	True	False

Showing 7 of 7

1. Open the ignore list template file ("ReplicationPermissions.json").
2. To ignore objects that contain "MSQL" in their name, edit the **Identity** parameter using the "like" option.



3. Save the changes made to the .json file.
4. Rerun Purple Knight and ensure this security indicator is included in the assessment. Notice that objects with "MSQL" in their name (**Identity** field) are now being ignored (**Ignored = True**).



SECURITY INDICATOR
Non-default principals with DC Sync rights on the domain

IOE Found 0 %

SEVERITY	WEIGHT
Critical	8

Security Frameworks

MITRE ATT&CK
- Credential Access

ANSSI
- vuln1_permissions_naming_context

Description

Any security principals with Replicate Changes All and Replicate Directory Changes permissions on the domain naming context object can potentially retrieve password hashes for any and all users in an AD domain ("DCSync" attack). Additionally, Write DACL / Owner also allows assignment of these privileges. This can then lead to all kinds of credential-theft based attacks, including Golden and Silver Ticket attacks.

Likelihood of Compromise

DCSync is an attack for accessing credentials through this method. If an attacker gets ahold of these privileges, it is straight-forward to retrieve credential material using tools like Mimikatz, for any user in a domain.

Result

Found 7 objects with replication permissions. (2 Objects ignored).

DistinguishedName	Identity	Access	Enabled	Ignored
DC=d01,DC=lab	d01\BdActrd0193	Allow: GenericAll on: All Properties	True	False
DC=d01,DC=lab	d01\MSOL_908f13345512	Allow: ExtendedRight on: DS-Replication-Get-Changes-All;Allow: ExtendedRight on: DS-Replication-Get-Changes	True	True
DC=d01,DC=lab	d01\BdActrd012	Allow: GenericAll on: All Properties	True	False
DC=d01,DC=lab	d01\BdActrd0196	Allow: WriteDacl on: All Properties	True	False
DC=d01,DC=lab	d01\Enterprise Key Admins	Allow: GenericAll on: All Properties		False
DC=d01,DC=lab	d01\BdActrd0197	Allow: WriteOwner on: All Properties	True	False
DC=d02,DC=d01,DC=lab	d01\MSOL_908f13345512	Allow: ExtendedRight on: DS-Replication-Get-Changes-All;Allow: ExtendedRight on: DS-Replication-Get-Changes	True	True

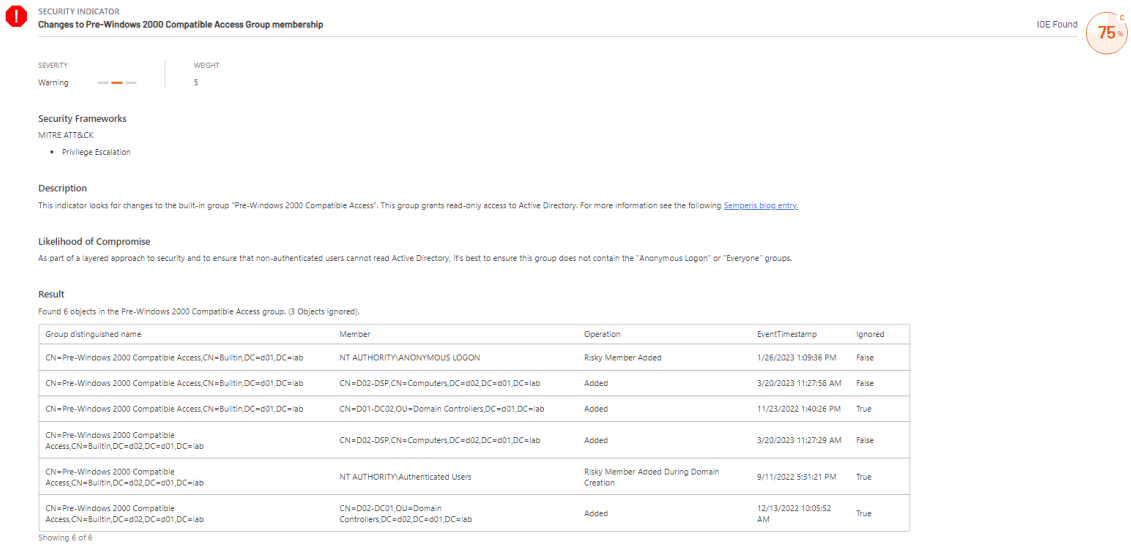
Showing 7 of 7

Example 2: Ignore events using the "le" option

In the following example, we want to ignore any event triggered by the "Changes to Pre-Windows 2000 Compatible Access Group membership" security indicator that occurred on or before January 01, 2023.

1. Open the ignore list template file ("PreWin2KGroup.json").
2. To ignore events that occurred on or before a specific date, edit the **EventTimestamp** parameter using the "le" option.

3. Save the changes made to the .json file.
4. Rerun Purple Knight and ensure this security indicator is included in the assessment. Notice that events that occurred before the specified date are now being ignored (**Ignored = True**).



SECURITY INDICATOR
Changes to Pre-Windows 2000 Compatible Access Group membership

IOE Found 75 C

SEVERITY
Warning

WEIGHT
5

Security Frameworks

MITRE ATT&CK

- Privilege Escalation

Description

This indicator looks for changes to the built-in group "Pre-Windows 2000 Compatible Access". This group grants read-only access to Active Directory. For more information see the following Semperis blog entry.

Likelihood of Compromise

As part of a layered approach to security and to ensure that non-authenticated users cannot read Active Directory, it's best to ensure this group does not contain the "Anonymous Logon" or "Everyone" groups.

Result

Found 6 objects in the Pre-Windows 2000 Compatible Access group. (3 Objects ignored).

Group distinguished name	Member	Operation	EventTimestamp	Ignored
CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=d01,DC=lab	NT AUTHORITY\ANONYMOUS LOGON	Risky Member Added	1/26/2023 1:09:36 PM	False
CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=d01,DC=lab	CN=D02-DSP,CN=Computers,DC=d02,DC=d01,DC=lab	Added	3/20/2023 11:27:58 AM	False
CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=d01,DC=lab	CN=D01-DC02,OU=Domain Controllers,DC=d01,DC=lab	Added	11/23/2022 1:40:26 PM	True
CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=d02,DC=d01,DC=lab	CN=D02-DSP,CN=Computers,DC=d02,DC=d01,DC=lab	Added	3/20/2023 11:27:29 AM	False
CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=d02,DC=d01,DC=lab	NT AUTHORITY\Authenticated Users	Risky Member Added During Domain Creation	9/11/2022 5:31:21 PM	True
CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=d02,DC=d01,DC=lab	CN=D02-DC01,OU=Domain Controllers,DC=d02,DC=d01,DC=lab	Added	12/13/2022 10:05:52 AM	True

Showing 6 of 6

Ignore Options

To ignore specific events for objects that meet the criteria defined, the "exclude" section of your .json file must be formatted correctly. That is, you must ensure that each option is paired with the appropriate list of values, ranges, regular expression patterns, or wildcard patterns, as described below. The ignore list feature will then apply the specified logic to exclude the relevant events from affecting the final score of the security indicator.

"match"

This option allows you to specify a regular expression where the indicator's result must match at least one pattern in the list in order for it to be ignored. It follows an "OR" logic, meaning if the result matches any one of the options in the list, it will be ignored immediately. To use this option, provide a list of regular expression patterns.

Syntax:

```
"match": ["pattern1", "pattern2", ...]
```

Example:

In this example, events from systems that use one of the specified naming standards (host_sys1_<*xxx*> and "host_sys2_<*xxx*>) will be added to the ignore list.

```
"match": [".*_sys1_.*", ".*_sys2_.*"]
```

"notmatch"

This option allows you to specify a regular expression where the indicator's result must not match any of the options in the list for it to be ignored. To use this option, provide a list of regular expression patterns.

Syntax:

```
"notmatch": ["pattern1", "pattern2", ...]
```

Example:

In this example, events for users that do not belong to a group with the specified prefixes ("A1" or "A2") will be added to the ignore list:

```
"notmatch": ["A1*", "A2*"]
```

"in"

This option allows you to specify a range or value. If the indicator's result falls within the specified range or value, it will be ignored. It follows an "OR" logic, meaning if the result matches any one of the options in the list, it will be ignored immediately. To use this option, provide a list of ranges or individual values.

Syntax:

```
"in": ["range1", "range2", ...]
```

Example:

In this example, events for objects with the specified GUID will be added to the ignore list.

```
"in": ["4e25afc3-f7e1-4c1f-b092-eb7287c0f2d1", "a4a97716-bca9-498e-
844b-eef6ac402efa"]
```

"notin"

With this option, the indicator's result must not fall within any of the specified ranges or values in the list for it to be ignored. To use this option, provide a list of ranges or individual values.

Syntax:

```
"notin": ["range1", "range2", ...]
```

Example:

In this example, events from all users expect those in domain A or domain B will be added to the ignore list.

```
"notin": ["A", "B"]
```

"like"

This option allows you to use wildcard patterns to match the indicator's result. If the result matches any of the wildcard patterns in the list, it will be ignored. It follows an "OR" logic, meaning if the result matches any one of the options in the list, it will be ignored immediately.

To use this option, provide a list of wildcard patterns. For more information on supported PowerShell wildcard patterns, see the Microsoft documentation: about_Comparison_Operators.

Syntax:

```
"like": ["*pattern1*", "*pattern2*", ...]
```

Example:

In the following example, all events with objects in domains "d01" or "d02" will be added to the ignore list.

```
"like": ["*d01*", "*d02*"]
```

"notlike"

With this option, the indicator's result must not match any of the wildcard patterns in the list for it to be ignored. To use this option, provide a list of wildcard patterns.

Syntax:

```
"notlike": ["*pattern1*", "*pattern2*", ...]
```

Example:

In the following example, all events with objects that do not contain the domains "d01" and "d02" will be added to the ignore list.

```
"notlike": ["*d01*", "*d02*"]
```

"ge" (Greater than or equal)

This option allows you to specify a date. Any event that occurred on or after the specified date will be ignored.

> ***NOTE**:*
> *This option is specifically designed for dates and can only accept a single date value in the correct format ("YYYY-MM-DD"). If both "ge" and "le" options are provided, the "ge" option will take precedence. It is recommended to use either the "ge" or "le" option to avoid contradictions between the specified dates.*

Syntax:

```
"ge": "YYYY-MM-DD"
```

Example:

In this example, any event that occurred on or after January 1, 2023, will be ignored.

```
"ge": "2023-01-01"
```

"le" (Less than or equal to)

This option allows you to specify a date. Any event that occurred on or before the specified date will be ignored.

> ***NOTE**:*
> *This option is specifically designed for dates and can only accept a single date value in the correct format ("YYYY-MM-DD"). If both "ge" and "le" options are provided, the "ge" option will take precedence. It is recommended to use either the "ge" or "le" option to avoid contradictions between the specified dates.*

Syntax:

```
"le": "YYYY-MM-DD"
```

Example:

In this example, any event that occurred on or before December 31, 2023, will be ignored.

```
"le": "2023-12-31"
```

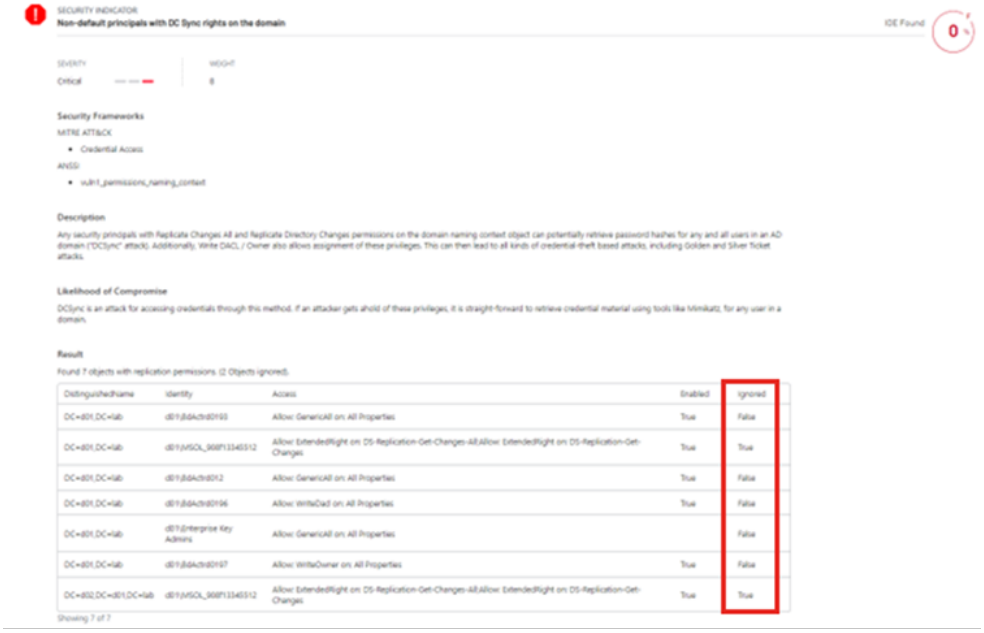
Review Indicator Results

To ensure you are not ignoring more than you intended, it is recommended that you review the security indicator results and adjust the ignore list if necessary.

1. Rerun Purple Knight.

   After an ignore list is applied, you will see the following in the **Security Assessment report** when the security indicator now runs:

   - **Security Posture Overview**: Recalculated security posture score where ignored objects are no longer included.
   - The test result details for the individual security indicator shows the objects that are being ignored.
     - The **Result** pane shows how many objects are being ignored and a new **Ignored** column displays "True" for the objects being ignored.



     - If all results are ignored, the status indicator displays "Passed" instead of "IOE found" and the **Result** pane displays "True" for all the objects being ignored.

   If the security indicator returns a "Failed to run" results, review the message in the **Result** pane for information as to why the indicator failed to run.

APPENDIX E

Security Indicator to Ignore List Template Map

The ignore list templates (.json files) use the same name as the indicator script (<*ScriptName*>.json), not the name displayed in the user interface. The following table maps each security indicator to its corresponding ignore list template (.json file). Please note that some indicators do not support ignore lists; this is noted in the **Ignore list template name** column.

Table 10: Security Indicator to Ignore List Template Map

Indicator name	Ignore list template name (.json file name)
Abnormal Password Refresh	AbnormalPasswordRefresh
Accounts with altSecurityIdentities configured	altSecurityIdentitiesConfigured
Accounts with Constrained Delegation configured to ghost SPN	DelegateToGhostSPN
Accounts with Constrained Delegation configured to krbtgt	ConstrainedDelegationToKRBTGT
AD Certificate Authority with Web Enrollment - PetitPotam and ESC8	EnterpriseCAs
AD objects created within the last 10 days	***NOTE**: This indicator does not support ignore lists.*
AD privileged users that are synced to Entra ID	AAD_PrivilegedOnPremiseSyncedToAAD

Indicator name	Ignore list template name (.json file name)
Administrative units are not being used	***NOTE**: This indicator does not support ignore lists.*
Admins with old passwords	OldPwdLastSetAdmin
Anonymous access to Active Directory enabled	AnonAccessonAD
Anonymous NSPI access to AD enabled	AnonNSPIAccess
Application expired secrets and certificates	AAD_ExpiredSecretsAndCertificates
Application Name and Geographic Location additional contexts are disabled on MFA	***NOTE**: This indicator does not support ignore lists.*
Built-in domain Administrator account used within the last two weeks	AdminUsedRecently
Built-in domain Administrator account with old password (180 days)	AdminPWNotChanged
Built-in guest account is enabled	GuestAccountEnabled
Certificate-Based Authentication Persistence	AAD_CBAPersistence
Certificate templates that allow requesters to specify a subjectAltName	CertificateTemplatesWithSANAllowed
Certificate templates with 3 or more insecure configurations	CertificateTemplatesAreVulnerable
Changes to AD Display Specifiers in the past 90 days	ChangesToAdminContextMenuPK

Indicator name	Ignore list template name (.json file name)
Changes to default security descriptor schema in the last 90 days	ChangesToDefaultSD
Changes to MS LAPS read permissions	ObjectsWithLapsRead
Changes to Pre-Windows 2000 Compatible Access Group membership	PreWin2KGroup
Changes to privileged group membership in the last 7 days	PrivilegedGroupChanges
Changes to unprivileged group membership in the last 7 days	MemberChangesToUnprivilegedGroups
Check for guests having permission to invite other guests	***NOTE**: This indicator does not support ignore lists.*
Check for risky API permissions granted to application service principals	AAD_CheckRiskyRoles
Check for users with weak or no MFA	AAD_CheckSecureMFA
Check if legacy authentication is allowed	***NOTE**: This indicator does not support ignore lists.*
Computer account takeover through Kerberos Resource-Based Constrained Delegation (RBCD)	RBCD
Computer Accounts in Privileged Groups	ComputersInPrivilegedGroup

Indicator name	Ignore list template name (.json file name)
Computer or user accounts with SPN that have unconstrained delegation	ComputerUserWithSPNUnconstrainedDelegation
Computers with older OS versions	CompObsoleteOS
Computers with password last set over 90 days ago	CompOldPwdLastSet
Conditional Access policies contain private IP addresses	AAD_CheckConditionalPrivateAddress
Conditional Access policies that contain MFA Trusted IPs	AAD_CheckLegacyMFA
Conditional Access Policy does not require MFA on privileged accounts	AAD_RequiredMFAOnPrivilegedAccounts
Conditional Access Policy that disable admin token persistence	***NOTE**: This indicator does not support ignore lists.*
Conditional Access Policy that does not require a password change from high risk users	***NOTE**: This indicator does not support ignore lists.*
Conditional Access Policy that does not require MFA when sign-in risk has been identified	***NOTE**: This indicator does not support ignore lists.*
Conditional Access policy with Continuous Access Evaluation disabled	AAD_CAEDisabled
Custom banned password protection not in use	***NOTE**: This indicator does not support ignore lists.*

Indicator name	Ignore list template name (.json file name)
Dangerous control paths expose certificate containers	CertificatesNTAuthPermissions
Dangerous control paths expose certificate templates	CertificateTemplatesPermissions
Dangerous GPO logon script path	GPOLogonScripts
Dangerous Trust Attribute Set	DangerousTrustAttributeSet
Dangerous user rights granted by GPO	GPOUserRights
Distributed COM Users group or Performance Log Users group are not empty	NonEmptyDcomAndPerformanceLogGroups
Domain Controller owner is not an administrator	DomainControllerOwnerPermissions
Domain Controllers in inconsistent state	DomainControllerInconsistent
Domain controllers that have not authenticated to the domain for more than 45 days	InactiveDCs
Domain controllers with old passwords	CompOldPwdLastSetDC
Domain controllers with Resource-Based Constrained Delegation (RBCD) enabled	RBCDOnDC
Domain trust to a third-party domain without quarantine	OutboundTrustWithoutQuarantine
Domains with obsolete functional levels	DomainObsoleteFunctionalLevel

Indicator name	Ignore list template name (.json file name)
Enabled admin accounts that are inactive	EnabledAdminsNotInUse
Enterprise Key Admins with full access to domain	EnterpriseKeyAdminsFullControl
Entra Connect sync account password reset	AAD_GetResetAADSyncUsers
Entra custom roles with risky permissions	AAD_RiskyCustomRolesPermissions
Entra ID privileged users that are also privileged in AD	AAD_PrivilegedOnPremiseAndAAD
Entra tenant is susceptible to Hidden Consent Grant attack	AAD_HiddenConsentGrant
Ephemeral Admins	EphemeralAdmins
Ensure all non-privileged users can complete MFA	AAD_UserCapableMFA
Evidence of Mimikatz DCShadow attack	DCShadowInUse
FGPP not applied to Group	FGPPNotAppliedToAGroup
FIDO2 Attestation is not enforced	***NOTE**: This indicator does not support ignore lists.*
Foreign Security Principals in Privileged Group	FSPInPrivilegedGroup
Forest contains more than 50 privileged accounts	ManyAdministratorsInForest
gMSA not in use	GMSANotInUse
gMSA objects with old passwords	GMSAOldPwdLastSet
GPO linking delegation at the AD Site level	WeakGPOLinkingADSite

Indicator name	Ignore list template name (.json file name)
GPO linking delegation at the domain controller OU level	WeakGPOLinkingOnDCOU
GPO linking delegation at the domain level	WeakGPOLinkingOnDomain
GPO Weak LM Hash storage enabled	GPOWeakLMHashStorageEnabled
GPO with scheduled tasks configured	GPOScheduledTasks
Guest accounts that were inactive for more than 30 days	AAD_InactiveGuests
Guest invites not accepted in last 30 day	AAD_StaleGuestsInvites
Guest users are not restricted	***NOTE**: This indicator does not support ignore lists.*
High-privileged custom roles (Okta)	***NOTE**: This indicator does not support ignore lists.*
Inheritance enabled on AdminSDHolder object	AdminSDHolderInheritance
Kerberos krbtgt account with old password	KerberosGoldenTicket
Kerberos protocol transition delegation configured	ObjectsWithProtocolTranistion
krbtgt account with Resource-Based Constrained Delegation (RBCD) enabled	RBCDOnkrbtgt
LDAP signing is not required on Domain Controllers	LdapSigningIsNotRequired
Less than 2 Global Administrators exist	AAD_LessThan2GAs

Indicator name	Ignore list template name (.json file name)
List of risky users (medium and high level)	AAD_RiskyUsers
MFA bombing attack occurred in the past day	AAD_MFABombingOnPrivilegedAccounts
MFA not configured for privileged accounts	AAD_CheckPrivilegedMFA
More than 5 Global Administrators exist	AAD_MoreThan5GlobalAdministrators
More than 10 Privileged Administrators exist	AAD_MoreThan10PrivilegedRoles
New API token was created (Okta)	***NOTE**: This indicator does not support ignore lists.*
New permission has been granted to a group (Okta)	***NOTE**: This indicator does not support ignore lists.*
New permission has been granted to a user (Okta)	***NOTE**: This indicator does not support ignore lists.*
New Super Admin permission has been granted to a group (Okta)	***NOTE**: This indicator does not support ignore lists.*
New Super Admin permission has been granted to a user (Okta)	***NOTE**: This indicator does not support ignore lists.*
Non-admin users can create tenants	***NOTE**: This indicator does not support ignore lists.*
Non-admin users can register custom applications	***NOTE**: This indicator does not support ignore lists.*
Non-default access to DPAPI key	DPAPIKeysPermissions
Non-default principals with DC Sync rights on the domain	ReplicationPermissions

Indicator name	Ignore list template name (.json file name)
Non default value on ms-Mcs-AdmPwd SearchFlags	LapsSearchFlagsNonDefault
Non-privileged users with access to gMSA passwords	GMSAPasswordPermissions
Non-standard schema permissions	NonStandardSchemaPermissions
Non-synced AAD user that is eligible for a privileged role	AAD_CheckSMTPMatch
Non default value on ms-Mcs-AdmPwd SearchFlags	LapsSearchFlagsNonDefault
Non-standard schema permissions	NonStandardSchemaPermissions
Non-synced Entra user that is eligible for a privileged role	AAD_CheckSMTPMatch
NTFRS SYSVOL Replication	NTFRSSysvolReplication
Objects in privileged groups without adminCount=1 (SDProp)	ObjectsInPrivilegedGroupWithoutAdmincount
Objects with constrained delegation configured	ObjectsWithConstrainedDelegation
Objects with Reanimated-Tombsontes extended rights	ObjectsCanReanimateTombstones
Operator groups no longer protected by AdminSDHolder and SDProp	DwAdminSDExMaskSet
Operators Groups that are not empty	OperatorsGroupsAreNotEmpty
OU permissions enabling BadSuccessor dMSA escalation	BadSuccessorAttackOUPermissions

Indicator name	Ignore list template name (.json file name)
Outbound forest trust with SID History enabled	OutboundForestTrustWithSIDHistory
Password hash synchronization is not enabled	AAD_PasswordHashSync
Password policy check (Okta)	***NOTE**: This indicator does not support ignore lists.*
Permanent Active Privileged Role Assignment	AAD_PermanentActivePrivilegedRoleAssignment
Permission changes on AdminSDHolder object	AdminSDHolderPermissionChange
Primary users with SPN not supporting AES encryption on Kerberos	PrimaryUsersWithSPNNotSupportingAES
Principals with constrained authentication delegation enabled for a DC service	ObjectsWithConstrainedDelegationDC
Principals with constrained delegation using protocol transition enabled for a DC service	ObjectsWithProtocolTransitionDC
Print spooler service is enabled on a DC	DCPrintSpooler
Privileged accounts with a password that never expires	UsersPwdNeverExpiresAdmin
Privileged accounts with mailbox	PrivilegedMailbox
Privileged group contains guest account	AAD_CheckPrivigedGuests
Privileged objects with unprivileged owners	UnprivilegedOwner

Indicator name	Ignore list template name (.json file name)
Privileged user credentials cached on RODC	RODCPrivilegedCreds
Privileged users that are disabled	DisabledPrivilegedUsers
Privileged users with SPN defined	PrivilegedSPN
Privileged Users with Weak Password Policy	PrivilegedUsersWeakPasswordPolicy
Prohibited Entra ID roles assigned	AAD_ProhibitedPrivilegedRoles
Protected Users group not in use	ProtectedUsersNotUsed
RC4 or DES encryption type are supported by Domain Controllers	RC4EnabledOnDC
Recent privileged account creation activity	NewPrivilegedUsers
Recent sIDHistory changes on objects	RecentSIDHistoryChanges
Report suspicious MFA activity disabled	***NOTE**: This indicator does not support ignore lists.*
Resource Based Constrained Delegation applied to AZUREADSSOACC account	AAD_RBCDOnSSOUser
Reversible passwords found in GPOs	GPPrefPasswords
Risky RODC credential caching	RiskyRODCCreds
Security defaults not enabled	***NOTE**: This indicator does not support ignore lists.*

Indicator name	Ignore list template name (.json file name)
Security questions are in use	***NOTE**: This indicator does not support ignore lists.*
Self-service password reset enabled for privileged roles	***NOTE**: This indicator does not support ignore lists.*
Shadow Credentials on privileged objects	ShadowCredentials
Smart card password rotation disabled	ExpirePasswordOnSmartCard
SMB Signing is not required on Domain Controllers	SmbSigningIsNotRequired
SMBv1 is enabled on Domain Controllers	SMBv1EnabledOnDCs
SSO computer account with password last set over 90 days ago	AAD_SSOOldPwdLastSet
Suspicious credentials on Microsoft service principals	EID_SuspiciousMSSPCreds
Suspicious Directory Synchronization Accounts role member	AAD_ SuspiciousDirectorySynchronizationAccountRoleMember
SYSVOL Executable Changes	SYSVOLExecutableChanges
Trust accounts with old passwords	TrustPwdLastSet
Unexpected accounts in Cert Publishers Group	***NOTE**: This indicator does not support ignore lists.*
Unprivileged accounts with adminCount=1	NonPrivilegedObjectsWithAdminCount
Unprivileged owner of a privileged group	AAD_UnprivilegedGroupOwner
Unprivileged principals as DNS Admins	UnprivilegedDNSAdmin

Indicator name	Ignore list template name (.json file name)
Unprivileged users can add computer accounts to the domain	UsersCanAddComputers
Unresolved Entra ID privileged role members	EID_UnresolvedPrivilegedUsers
Unrestricted user consent allowed	***NOTE**: This indicator does not support ignore lists.*
Unsecured DNS configuration	DnsZonesWithUnsecureUpdate
User accounts that store passwords with reversible encryption	UsersReversiblePWD
User accounts that use DES encryption	UsersDESPWD
User accounts with password not required	UsersPWDNotReq
User activation in the last 7 days (Otka)	***NOTE**: This indicator does not support ignore lists.*
User consent is allowed for risky applications	***NOTE**: This indicator does not support ignore lists.*
User deactivation in the last 7 days (Otka)	***NOTE**: This indicator does not support ignore lists.*
Users and computers with non-default Primary Group IDs	NonStandardPGID
Users and computers without readable PGID	NoPGID
Users are not using their privileged roles	AAD_UnusedEligibleRole
Users can create security groups	***NOTE**: This indicator does not support ignore lists.*

Indicator name	Ignore list template name (.json file name)
Users or devices inactive for at least 90 days	AAD_CheckInactivePrincipals
Users with Kerberos pre-authentication disabled	UsersWithPreAuth
Users with old passwords	OldPwdLastSet
Users with Password Never Expires flag set	UsersPwdNeverExpires
Users with permissions to set Server Trust Account	InstallReplicaPermissions
Users with SPN defined	PrimaryUsersWithSPN
Users with the attribute userPassword assigned	UserPasswordAttributeIsSet
Users without Multi-Factor Authentication (MFA) (Okta)	***NOTE**: This indicator does not support ignore lists.*
Weak certificate cipher	WeakCertificateCipher
Well-known privileged SIDs in sIDHistory	SIDHistoryPrivilegedSID
Write access to RBCD on DC	RBCDWriteOnDC
Write access to RBCD on krbtgt account	RBCDWriteOnkrbtgt
Zerologon vulnerability	ZeroLogonPK