

Purple Knight
Version: 2.2
User Guide
November 2022 (6.4)

Legal Notice

Copyright © 2022 Semperis. All rights reserved.

All information included in this document, such as text, graphics, photos, logos, and images, is the exclusive property and contains confidential information of Semperis or its licensors and is protected by copyright and trademark laws and various other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions and international conventions. The information included in this document regarding processes, systems, and technological mechanisms is proprietary to Semperis and constitutes trade secrets of Semperis. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, translated into any language or computer language, distributed, or made available to others, in any form or by any means, whether electronic, mechanical, or otherwise, without prior written permission of Semperis.

Semperis is a registered trademark of Semperis Inc. All other company or product names are trademarks or registered trademarks of their respective holders.

This document is provided strictly on an "AS IS" basis without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Semperis and its staff assume no responsibility for any errors that may have been included in this document and reserve the right to make changes to the document without notice. Semperis and its staff disclaim any responsibility for incidental or consequential damages in connection with the furnishing, performance, use of, or reliance on this document or its content.

Contents

| | |
|---|----|
| Preface | v |
| Document Revisions | v |
| Styles and conventions used in this document | vi |
| Contacting Semperis | vi |
| Purple Knight Overview | 1 |
| What's New in Purple Knight v2.2 | 2 |
| Getting Started | 4 |
| System Requirements | 4 |
| Create and Configure Application Registration | 6 |
| Installing Purple Knight | 11 |
| Viewing Version Information | 13 |
| Checking for New Version | 14 |
| Running a Security Assessment Report | 15 |
| Agreement page | 16 |
| Environment page | 17 |
| Environment page: Azure Active Directory | 18 |
| Environment page: Active Directory | 20 |
| Indicators page | 24 |
| Progress page | 28 |
| Report Summary page | 31 |
| Security Assessment Report | 35 |
| Security Posture Overview | 37 |
| Indicators of Exposure | 38 |
| Critical IOEs Found | 39 |
| Additional IOEs Found | 40 |
| Indicators Failed To Run | 41 |
| Active Directory Results | 41 |
| Categories: Active Directory | 42 |
| Test Result Details: Active Directory | 43 |
| Azure AD Results | 47 |
| Categories: Azure AD | 47 |

| | |
|--|----|
| Test Result Details: Azure AD | 48 |
| Report Appendices | 51 |
| Scoring method | 53 |
| Letter grade | 54 |
| Risk factors | 54 |
| DREAD Threat Probability Matrix | 55 |
| Hybrid Category Scoring and Placement | 56 |
| How to Add Company Branding | 58 |
| How to Access the Debug Log Level | 60 |

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 Active Directory environment. 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 and Azure Active Directory. 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

Table 1: Document Revisions

| Document Edition | Date | Product Version | Comments |
|------------------|---------------|-----------------|--|
| 1.0 | March 2021 | 1.2 | Initial release; Partner edition |
| 1.1 | March 2021 | 1.2 | Updated system requirements and contact information |
| 2.0 | April 2021 | 1.2 SP1 | Updated for SP1 release |
| 3.0 | August 2021 | 1.3 | Updated for 1.3 release |
| 3.1 | November 2021 | 1.3.1 | Updated security indicator list (What's New topic), updated ports list, and correction to registry key location for debug log level. |
| 4.0 | January 2022 | 1.4 | Updated for 1.4 release; combined Partner and Community editions |
| 5.0 | July 2022 | 1.5 | Updated for 1.5 release; Azure AD indicators |
| 6.0 | August 2022 | 2.0 | Updated for 2.0 release |
| 6.1 | August 2022 | 2.0 | Minor edits for 2.0 release |
| 6.2 | October 2022 | 2.1 | Updated for 2.1 release |

| Document Edition | Date | Product Version | Comments |
|------------------|---------------|-----------------|---|
| 6.3 | October 2022 | 2.1 | Updated permissions list; republished for 2.1.1 |
| 6.4 | November 2022 | 2.2 | Updated for 2.2 release; new Hybrid category |

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. |
| <i>Italics</i> | Used for references to documents that are not hyperlinks to other documents or topics. Also used for dialog names and to introduce new terms. |
| 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. |

In addition, 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 Azure Active Directory (Azure AD) environment focusing on some of the most common attack vectors that threat actors use to gain access to the Azure AD environment.

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 or Azure AD. 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 Active Directory or Azure AD 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 or Azure AD 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.

What's New in Purple Knight v2.2

With this release of Purple Knight, the following enhancements are available in Purple Knight Community edition.

Hybrid Security Indicators Category

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

For more information on how the hybrid indicator score is calculated (that is, within the overall AD score or Azure AD score) and where this category and indicators may appear in your Security Assessment report, see [Hybrid Category Scoring and Placement](#).

New Erase Outputs Script

A new script, Erase_PK_Output, has been included that allows you to remove the output files generated by Purple Knight runs. The files that are removed using this script include:

- PurpleKnight\Output (folder and all its contents)
If you have PDF or CSV files saved to another location (other than the PurpleKnight\Output folder) these files will NOT be removed.
- PurpleKnight\custom (folder and all its contents)
- ProgramData\Semperis\Logs (all logs with "PurpleKnight" in their names)

New Security Indicators

Purple Knight includes the following new security indicators:

Active Directory

- Privileged user credentials cached on RODC

Azure Active Directory

**NOTE:**

*There is a new permission required for some of the new Azure AD indicators:
`AuditLog.Read.All`.*

- AAD Connect sync account password reset
Permissions: AuditLog.Read.All; Directory.Read.All; User.Read.All;
RoleManagement.Read.Directory
- Conditional Access policy with Continuous Access Evaluation disabled
Permissions: Policy.Read.All
- Guest accounts that were inactive for more than 30 days
Permissions: User.Read.All; AuditLog.Read.All

Hybrid

- Resource Based Constrained Delegation applied to AZUREADSSOACC account

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

Table 3: System requirements

| Software/Hardware | Requirement |
|---------------------------|---|
| Operating system | Supported operating systems include: <ul style="list-style-type: none">• Windows 8.1• Windows 10• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019 |
| .NET Framework | .NET Framework version 4.6.2 or later |
| Windows PowerShell | Windows PowerShell version 4.0 or later |
| Network Access | The following ports are required to run Purple Knight: <ul style="list-style-type: none">• 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 |

Table 3: System requirements

| Software/Hardware | Requirement |
|---------------------------|---|
| | <ul style="list-style-type: none">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 <p>Purple Knight does NOT support running from an untrusted network location.</p> |
| Supported browsers | The latest versions of the following browsers are supported: <ul style="list-style-type: none">Google ChromeMicrosoft Edge |
| Display resolution | Minimum: 1024 x 768 |
| Logo size | Company logo requirements include: <ul style="list-style-type: none">160 x 70 px.jpg or .pngno larger than 250 KB <p>For more information on how to add your company logo to the Security Assessment report, see How to Add Company Branding.</p> |

In addition, for those wanting to run the Azure AD security indicators, the following system requirements also apply.

Table 4: Microsoft Azure AD connection requirements

| Azure Component | Requirement |
|--------------------------------|---|
| Azure AD tenant | Supports only one Azure AD tenant per Purple Knight instance. |
| Azure application registration | <p>Before you can configure the Azure AD connection in Purple Knight, you must create and configure an application registration that has the ability to generate a client secret.</p> <p>Required permissions (API permissions > Microsoft Graph > Application permissions):</p> <ul style="list-style-type: none">User.Read.AllGroup.Read.All |

Table 4: Microsoft Azure AD connection requirements

| Azure Component | Requirement |
|-----------------|---|
| | <ul style="list-style-type: none"> Application.Read.All <p>In addition, the following permissions must be granted to the application in order to run the Azure AD security indicators:</p> <ul style="list-style-type: none"> AdministrativeUnit.Read.All Application.Read.All * AuditLog.Read.All Directory.Read.All Policy.Read.All PrivilegedAccess.Read.AzureAD Reports.Read.All RoleManagement.Read.Directory User.Read.All * UserAuthenticationMethod.Read.All <p>* The Application.Read.All and User.Read.All permissions are required for both the application itself and to run some of the Azure AD security indicators.</p> |

Create and Configure Application Registration



NOTE:

These configuration instructions apply to those wanting to run the Azure AD security indicators available in Purple Knight. If you have no intention of running a security scan of an Azure AD tenant, you can skip these configuration steps and proceed to [Installing Purple Knight](#).

Before you can configure the Azure AD 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 Azure AD connection in Purple Knight to run the Azure AD security indicators:

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

**TIP:**

To run Purple Knight in your Azure AD environment, you need to create and update the app registration in Azure AD 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](#).

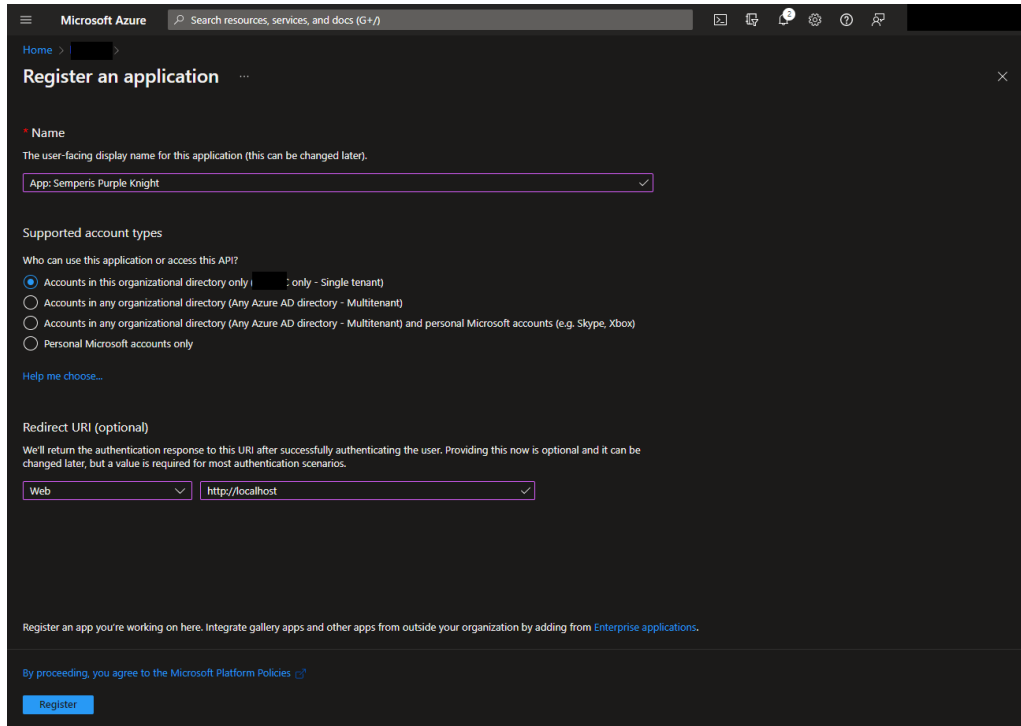
In summary, the script supports the following:

- *Create and update the application registration in Azure AD in order for Purple Knight to be able to scan for vulnerabilities in Azure AD.*
 - *Delete the application registration from Azure AD*
 - *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 Azure AD.*
 - *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, select the **Azure Active Directory** service.
2. In the Azure AD 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 Azure AD, the page for the newly registered application is displayed.

To add permissions to the Purple Knight application:

1. In the Azure AD 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
- Directory.Read.All
- Group.Read.All
- Policy.Read.All
- PrivilegedAccess.Read.AzureAD
- Reports.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 <Azure AD tenant>**.

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 <Azure AD tenant>" status message for the above permissions.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for zkq61

| API / Permissions name | Type | Description | Admin consent requ... | Status |
|---|-------------|--|-----------------------|-------------------------|
| ▼ Microsoft Graph (11) ... | | | | |
| AdministrativeUnit.Read.All | Application | Read all administrative units | Yes | ✓ Granted for zkq61 ... |
| Application.Read.All | Application | Read all applications | Yes | ✓ Granted for zkq61 ... |
| AuditLog.Read.All | Application | Read all audit log data | Yes | ✓ Granted for zkq61 ... |
| Directory.Read.All | Application | Read directory data | Yes | ✓ Granted for zkq61 ... |
| Policy.Read.All | Application | Read your organization's policies | Yes | ✓ Granted for zkq61 ... |
| PrivilegedAccess.Read.AzureAD | Application | Read privileged access to Azure AD roles | Yes | ✓ Granted for zkq61 ... |
| Reports.Read.All | Application | Read all usage reports | Yes | ✓ Granted for zkq61 ... |
| RoleManagement.Read.Directory | Application | Read all directory RBAC settings | Yes | ✓ Granted for zkq61 ... |
| User.Read | Delegated | Sign in and read user profile | No | ✓ Granted for zkq61 ... |
| User.Read.All | Application | Read all users' full profiles | Yes | ✓ Granted for zkq61 ... |
| UserAuthenticationMethod.Read.All | Application | Read all users' authentication methods | Yes | ✓ Granted for zkq61 ... |

To create a client secret for the Purple Knight application:**IMPORTANT!**

In the Azure AD 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 Azure AD 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 Azure AD 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 Azure AD 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 value that is accessible by authorized persons only.

1. In the Azure AD 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 Azure AD 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 Azure AD Environment page in Purple Knight.
2. In the Azure AD 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 Azure AD Environment page in Purple Knight.

Installing Purple Knight

To install 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 install 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.



TIP:

You can also unblock all files using the following PowerShell cmdlet:

`dir -Path e:\PK -Recurse | Unblock-File`

Where: e:\PK is the folder where the files are to be extracted.

3. Extract the contents of the PurpleKnight.zip file to a folder with write permissions on a domain-joined computer (Windows workstation or server).
4. Ensure that your PowerShell Execution Policy is not blocking scripts from running on your machine.
 - To check your current execution policy, run the following PowerShell cmdlet:
`Get-ExecutionPolicy -list`
 - 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, it is recommended to run the following PowerShell cmdlet:
`Set-ExecutionPolicy -Scope LocalMachine RemoteSigned`
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.)

%ProgramData%\Semperis

\Logs

PurpleKnight.Log


PurpleKnightResults.Log

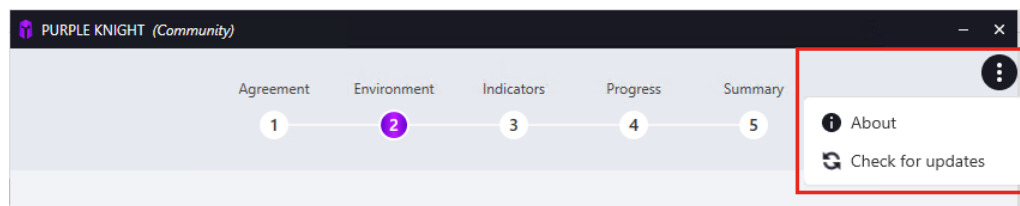
Viewing Version Information

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

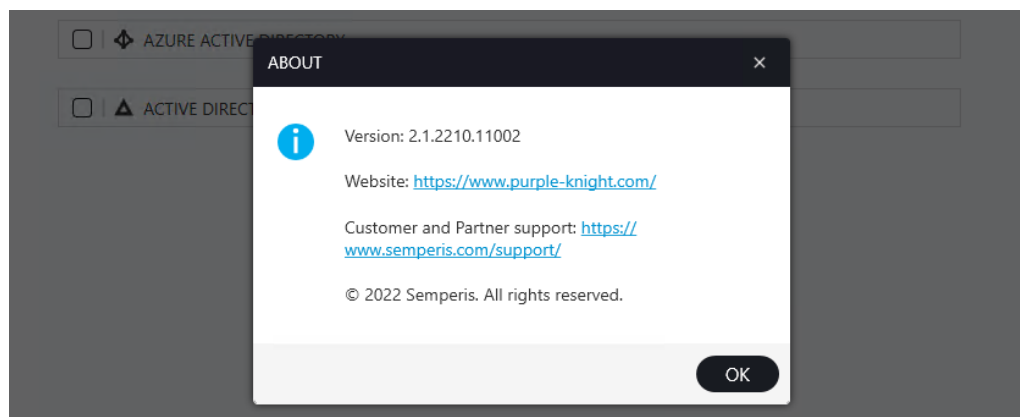
The **About** box can be viewed from all pages in the product except the **Agreement** page.

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.




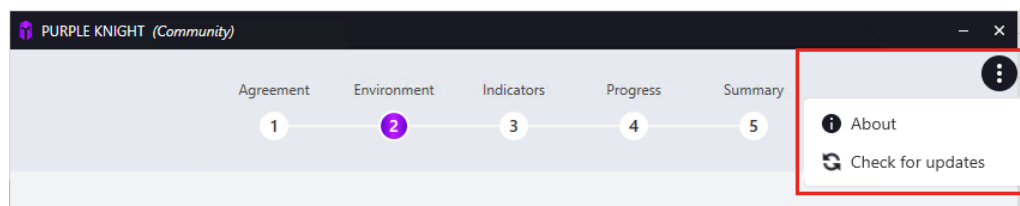
3. Click **OK** to close the **About** box.

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 update* dialog displays. Once the check is completed you will be presented with the results:

- If you are using the latest version, a message displays stating you are using the latest version. Click **OK** to close the *Check for update* 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 **OK** to close the *Check for update* dialog and use the currently installed version.

CHAPTER 3

Running a Security Assessment Report

Purple Knight is a stand alone utility that runs Windows PowerShell scripts to assess Active Directory and Azure AD 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.

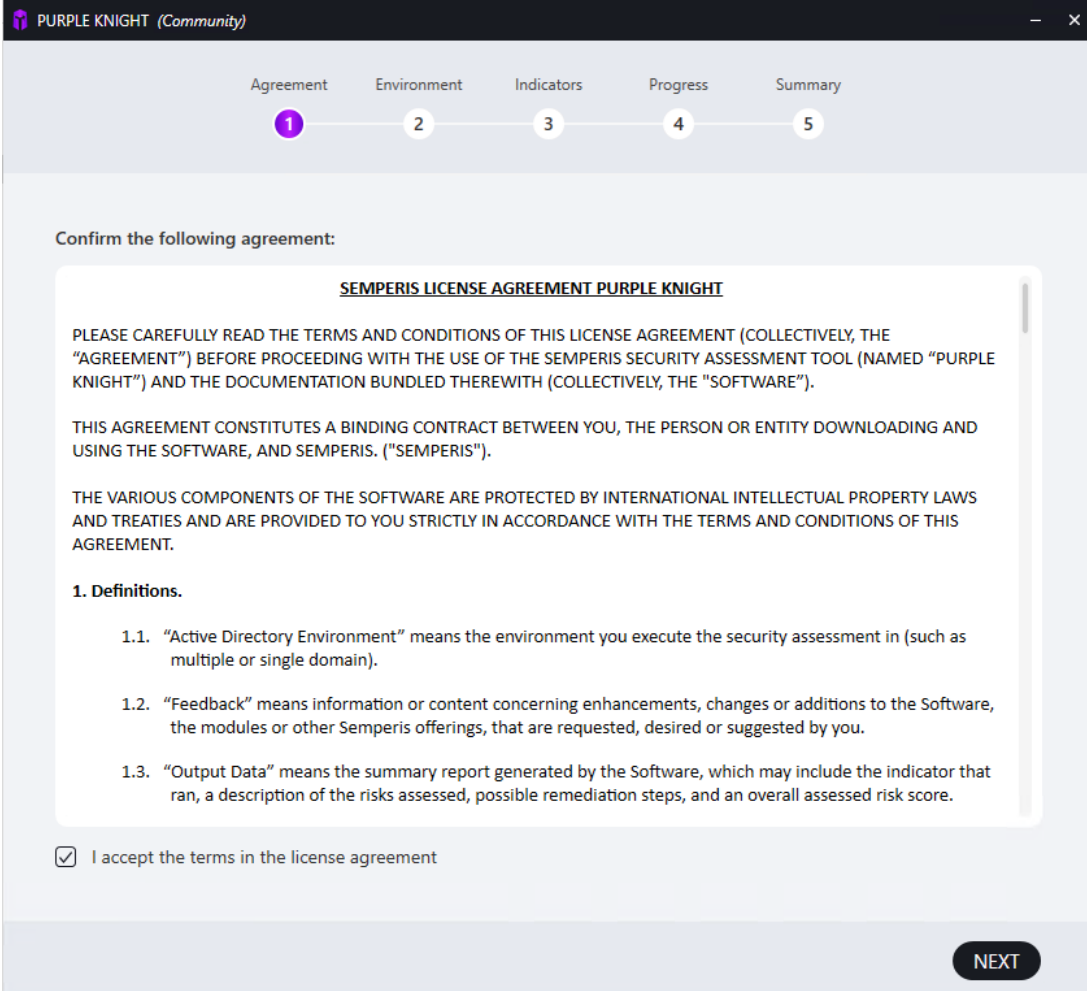
To run a security assessment report:

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, Azure AD, or both 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, and the forest and domains to be used in the new Active Directory 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 **Close** button (X) 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.



PURPLE KNIGHT (Community)

Agreement Environment Indicators Progress Summary

1 2 3 4 5

Confirm the following agreement:

SEMPERIS LICENSE AGREEMENT PURPLE KNIGHT

PLEASE CAREFULLY READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT (COLLECTIVELY, THE "AGREEMENT") BEFORE PROCEEDING WITH THE USE OF THE SEMPERIS SECURITY ASSESSMENT TOOL (NAMED "PURPLE KNIGHT") AND THE DOCUMENTATION BUNDLED THEREWITH (COLLECTIVELY, THE "SOFTWARE").

THIS AGREEMENT CONSTITUTES A BINDING CONTRACT BETWEEN YOU, THE PERSON OR ENTITY DOWNLOADING AND USING THE SOFTWARE, AND SEMPERIS. ("SEMPERIS").

THE VARIOUS COMPONENTS OF THE SOFTWARE ARE PROTECTED BY INTERNATIONAL INTELLECTUAL PROPERTY LAWS AND TREATIES AND ARE PROVIDED TO YOU STRICTLY IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions.

1.1. "Active Directory Environment" means the environment you execute the security assessment in (such as multiple or single domain).

1.2. "Feedback" means information or content concerning enhancements, changes or additions to the Software, the modules or other Semperis offerings, that are requested, desired or suggested by you.

1.3. "Output Data" means the summary report generated by the Software, which may include the indicator that ran, a description of the risks assessed, possible remediation steps, and an overall assessed risk score.

☒ I accept the terms in the license agreement

NEXT

Figure 1: Agreement page

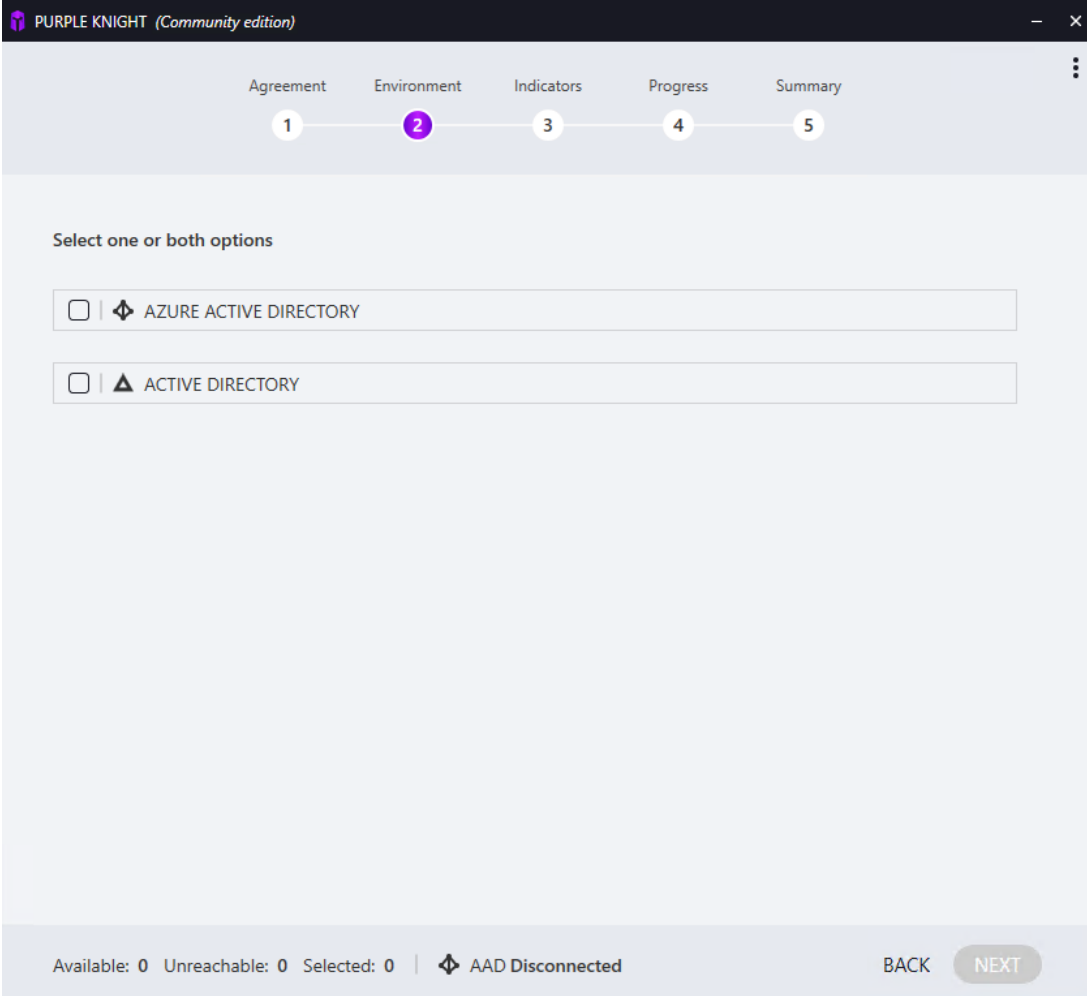
To confirm and continue:

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, Azure AD, or both if you want to see the overall security posture across your hybrid identity environment.



PURPLE KNIGHT (Community edition)

Agreement Environment Indicators Progress Summary

1 2 3 4 5

Select one or both options

☐ AZURE ACTIVE DIRECTORY

☐ ACTIVE DIRECTORY

Available: 0 Unreachable: 0 Selected: 0 | AAD Disconnected

BACK NEXT

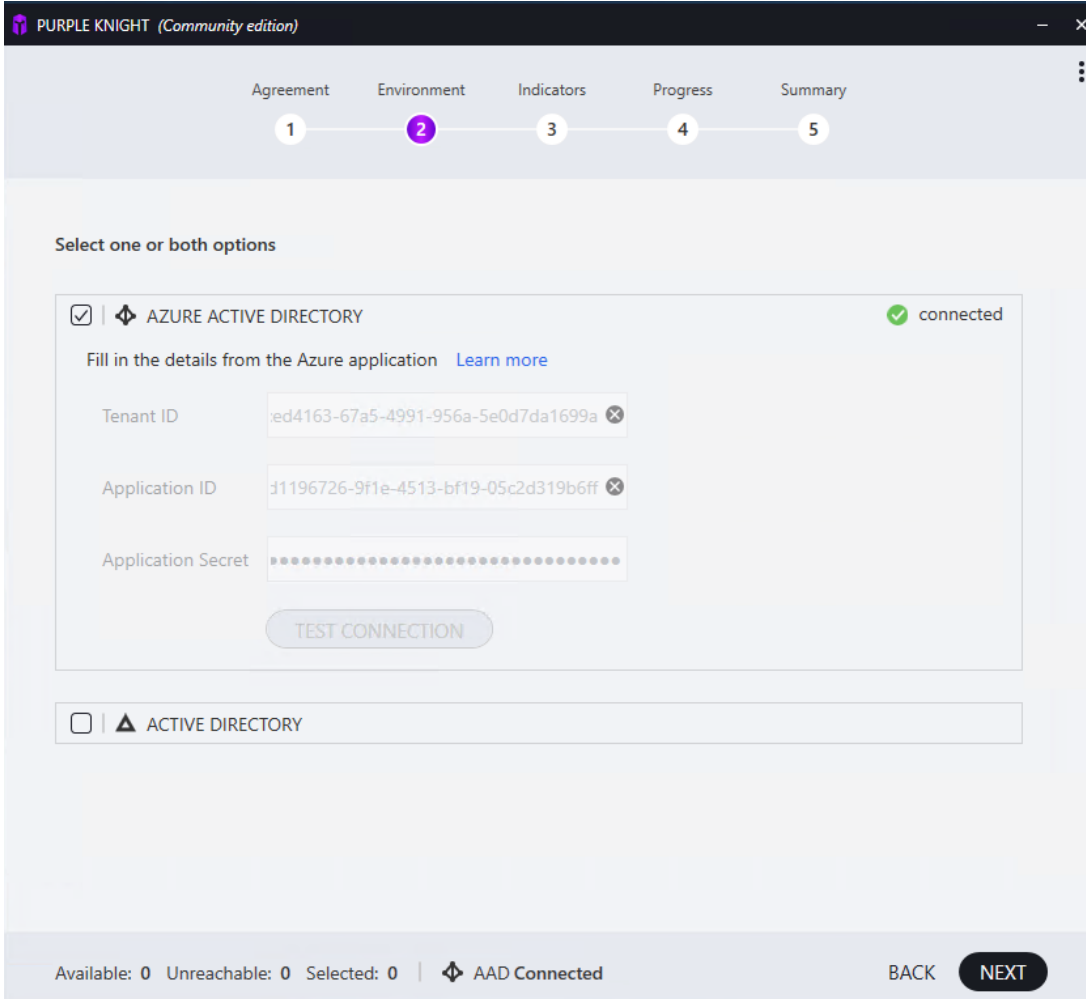
Figure 2: Environment page

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 environment (s).

- [Environment page: Azure Active Directory](#)
- [Environment page: Active Directory](#)

Environment page: Azure Active Directory

Use the **Azure Active Directory** pane on the **Environment** page to establish an Azure AD tenant connection. All of the information you need can be copied from the Azure portal and pasted into the designated fields in this pane.



The screenshot shows the 'Environment' page of the Purple Knight (Community edition) interface. At the top, a progress bar indicates five steps: Agreement (1), Environment (2, highlighted), Indicators (3), Progress (4), and Summary (5). Below the progress bar, the heading 'Select one or both options' is followed by two selection boxes. The first box, 'AZURE ACTIVE DIRECTORY', is checked and marked as 'connected' with a green checkmark. It contains fields for 'Tenant ID' (ed4163-67a5-4991-956a-5e0d7da1699a), 'Application ID' (d1196726-9f1e-4513-bf19-05c2d319b6ff), and 'Application Secret' (masked with dots). A 'TEST CONNECTION' button is below these fields. The second box, 'ACTIVE DIRECTORY', is unchecked. At the bottom, a status bar shows 'Available: 0 Unreachable: 0 Selected: 0' and 'AAD Connected' with a checkmark icon. 'BACK' and 'NEXT' buttons are on the right.

Figure 3: Environment page: Azure Active Directory



NOTE:

Only one Azure AD tenant can be registered per Purple Knight instance. The time it takes to create the initial connection to Azure AD could take several minutes to complete.

Before you begin:

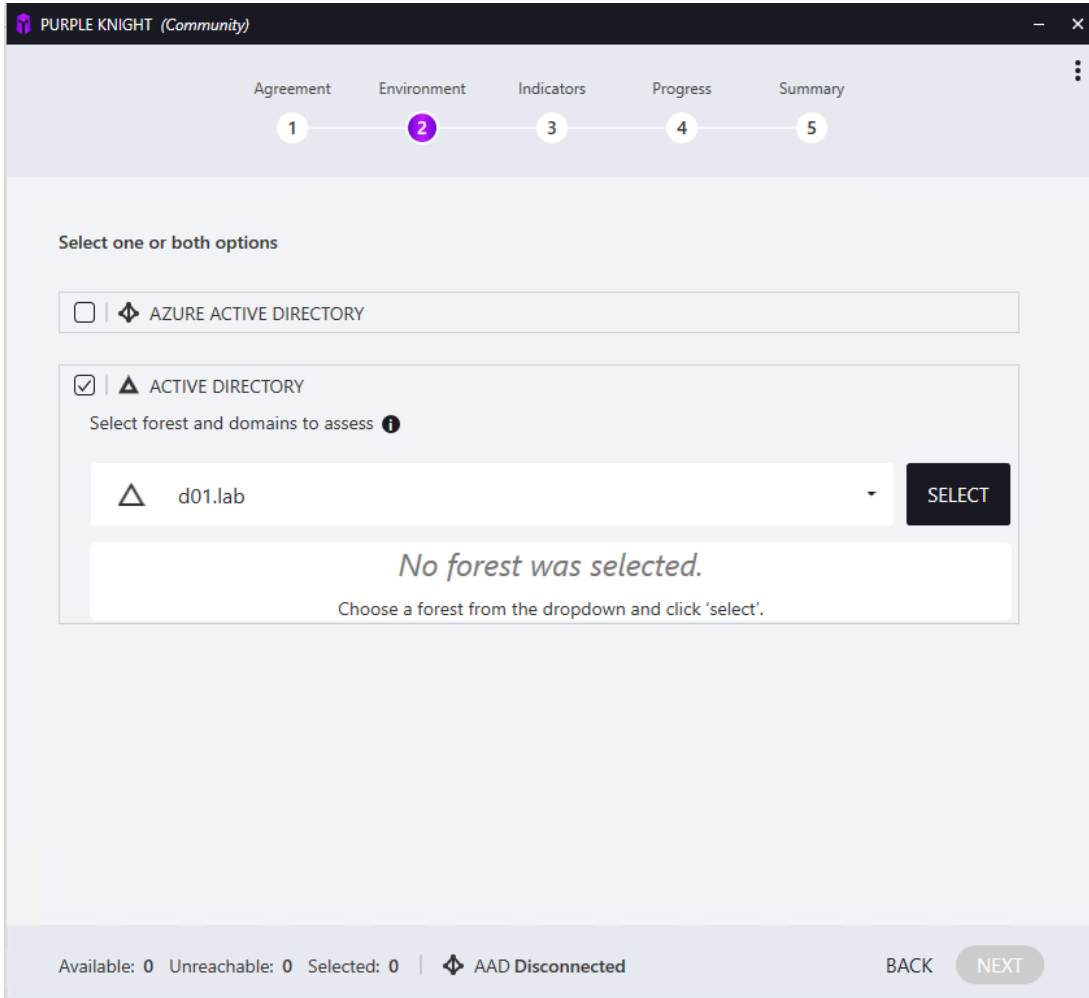
Ensure the Azure AD tenant is configured. This includes registering the Purple Knight application, setting the appropriate permissions, and creating a client secret for the application. For more information, see [Create and Configure Application Registration](#).

To configure an Azure AD tenant connection:

1. On the **Environment** page, select **Azure Active Directory**.
2. In the expanded **Azure Active Directory** pane, enter the following information from your Azure AD portal:
 - **Tenant ID:** The unique tenant identifier assigned to the Azure AD tenant where the Purple Knight application is registered.
(Azure AD portal: The **Tenant ID** can be found in the *Basic Information* pane at the top of the **Overview** page for the Azure tenant.)
 - **Application ID:** The unique application identifier assigned to the Purple Knight application.
(Azure AD 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.
(Azure AD 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 Azure AD pane. In addition, "**AAD Connected**" displays across the bottom of the page. (The domain counts (Available, Unreachable, and Selected) do not apply to your Azure AD connection.)
4. If you want to see the overall security posture across your hybrid identity environment, click 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](#).
5. Click **NEXT**.

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.



The screenshot shows the 'Environment' page in the Purple Knight (Community) interface. At the top, a progress bar indicates five steps: 1. Agreement, 2. Environment (current), 3. Indicators, 4. Progress, and 5. Summary. Below the progress bar, the instruction 'Select one or both options' is displayed. There are two main selection options: 'AZURE ACTIVE DIRECTORY' (unchecked) and 'ACTIVE DIRECTORY' (checked). Under the 'ACTIVE DIRECTORY' section, there is a dropdown menu labeled 'Select forest and domains to assess' with a tree icon and the text 'd01.lab'. To the right of the dropdown is a 'SELECT' button. Below the dropdown, a message states 'No forest was selected.' with a sub-instruction 'Choose a forest from the dropdown and click 'select'.' At the bottom of the page, a status bar shows 'Available: 0 Unreachable: 0 Selected: 0' and a connection status 'AAD Disconnected'. Navigation buttons 'BACK' and 'NEXT' are located at the bottom right.

Figure 4: 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.

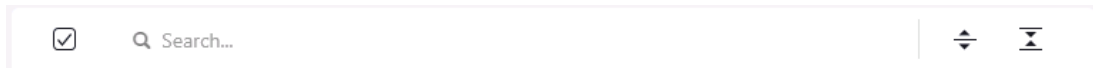


Figure 5: Domain selection tool bar

Use the domain selection controls as described below:



Select all check box.

- A check mark indicates that all domains and child domains are selected.
- 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.

Click to expand the domain list to display all child domains.



Click to collapse the domain list to hide all child domains.

To select the forest and domains:



BEST PRACTICE:

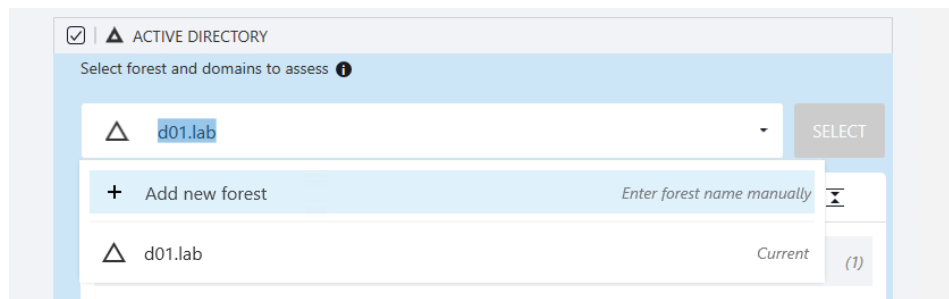
For an accurate assessment, select all of the domains in the selected forest.



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 AAD connection status does not apply to your Active Directory connect.)

4. If you want to see the overall security posture across your hybrid identity environment, click the **Azure Active Directory** check box to specify the Azure AD tenant to be included in the assessment. For more information, see [Environment page: Azure Active Directory](#).
5. 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.

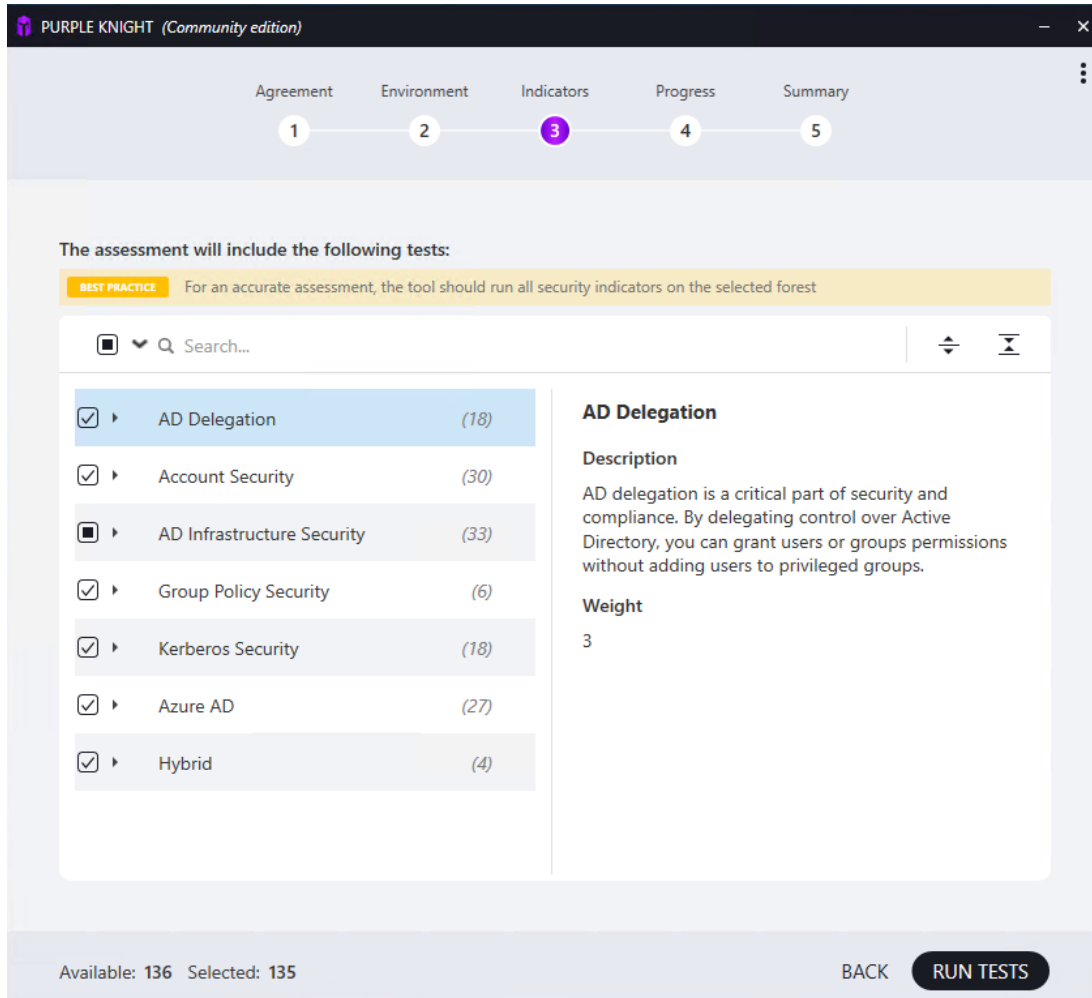


Figure 6: Indicators page

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.

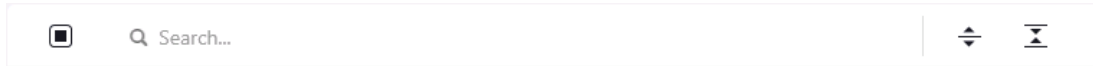


Figure 7: Security Indicator selection tool bar

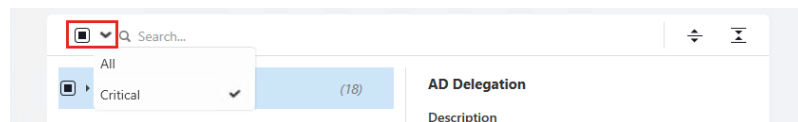
Use the security indicator selection controls as described below:



Select all check box.

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

You can filter the selection list to display and select only critical security indicators by clicking this check box and selecting **Critical**.



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.
Click to expand the list to display all relevant security indicators per category.



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 or Azure AD)
- Security Frameworks
- Description
- Likelihood of Compromise

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

To select a security indicator:



BEST PRACTICE:

For an accurate assessment, select all of the security indicators.




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.

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**.

Azure AD: If you do not have sufficient permissions to run a selected security indicator, an error message displays explaining which Azure AD application permissions are not granted.

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.

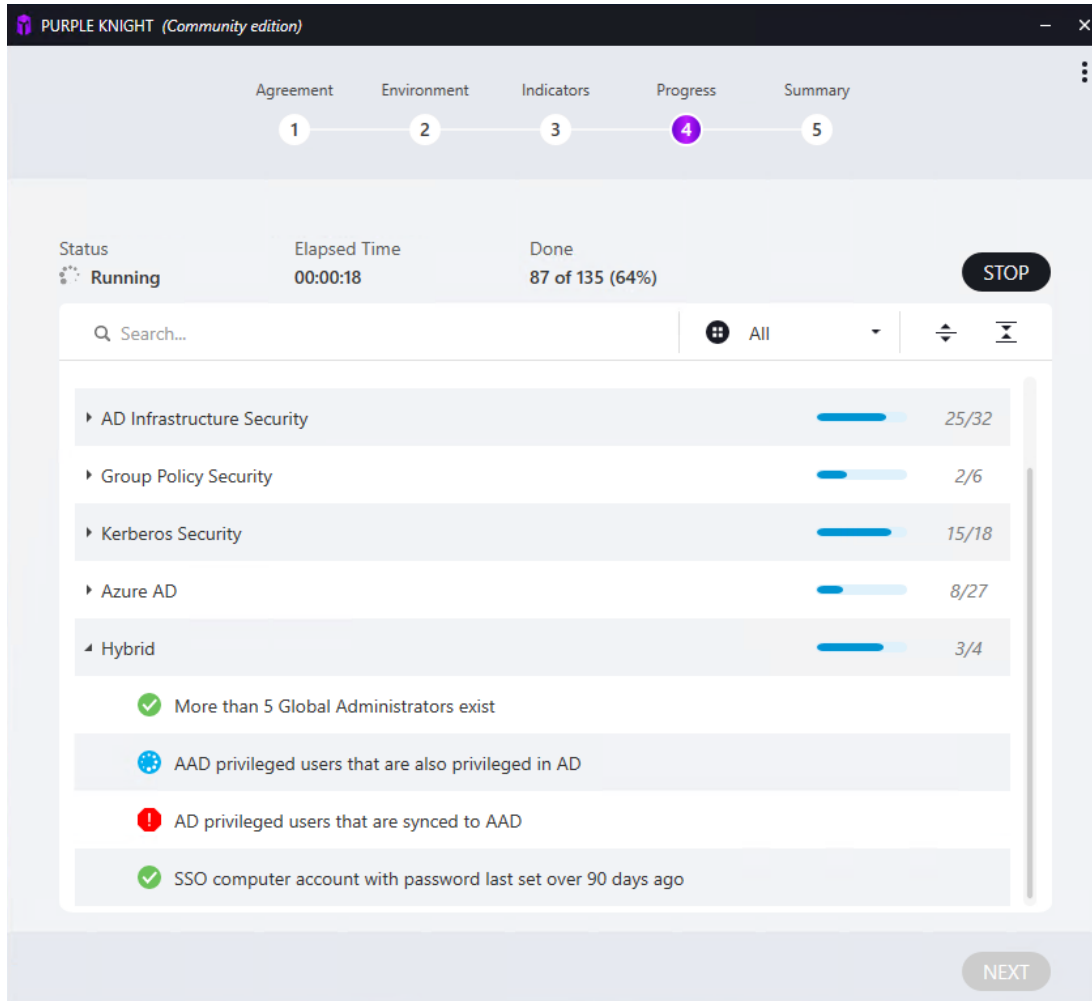


Figure 8: Progress page

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 9: Progress page tool bar

Use the Progress page controls as described below:

 Search...

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.



Click to expand the category list to display all relevant security indicators per category.



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.

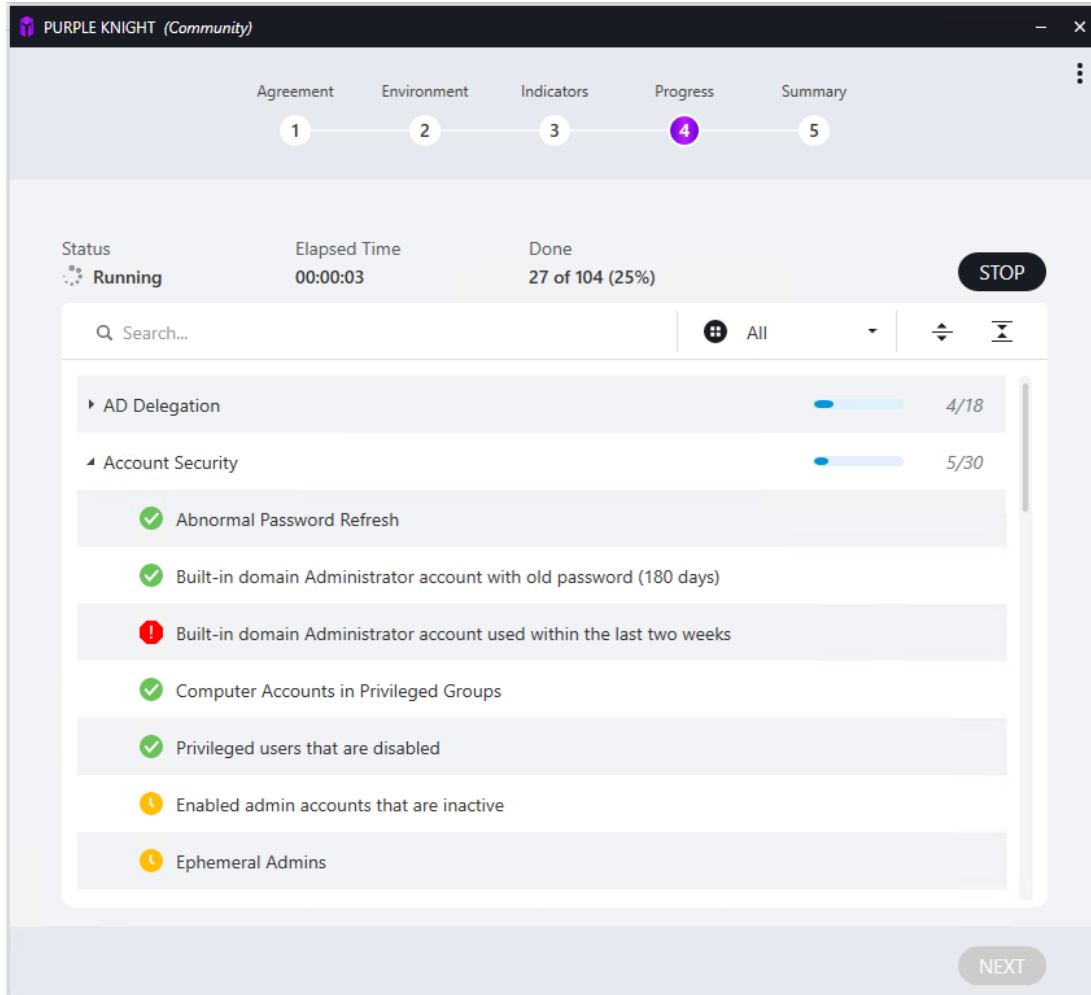


Figure 10: Progress page with category expanded

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), environment details, run details, and evaluation results summary for each environment included in the security assessment.

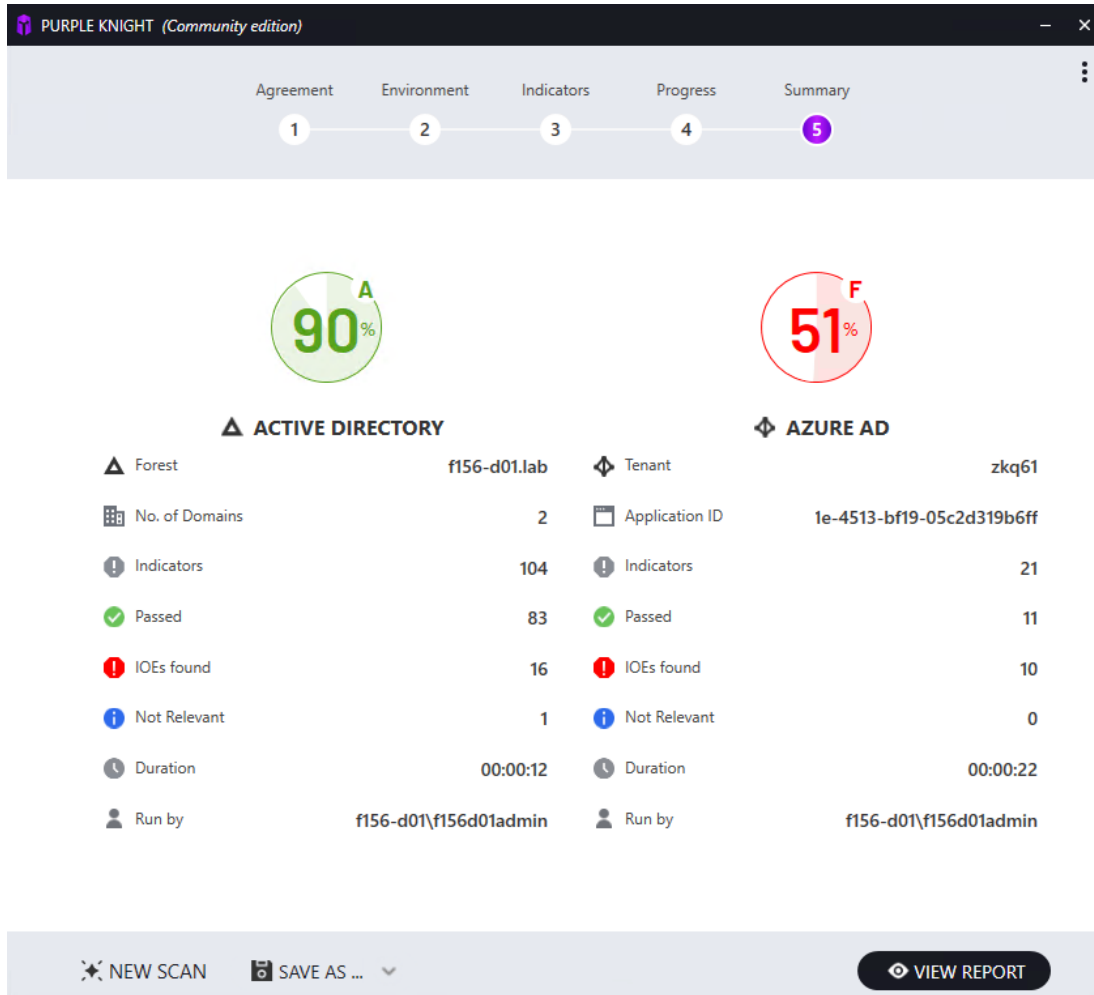


Figure 11: Report Summary page

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.
- **No. of Domains:** The number of domains that were evaluated.
- **Indicators:** Number of Active Directory security indicator tests that successfully completed (passed or IOE found)
- **Passed:** Total number of Active Directory tests that passed without finding any Indicators of Exposure (IOEs).

- **IOEs found:** Total number of IOEs found across all selected Active Directory security indicators.
- **Not Relevant:** Total number of Active Directory security indicator tests that did not run because they do not apply to the selected environment.
- **Duration:** The amount of time (hh:mm:ss) it took to generate the assessment report for the Active Directory environment.
- **Run by:** The name of the account that ran the assessment report.

Azure AD

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

- **Tenant:** The name of the Azure AD tenant that was evaluated.
- **Application ID:** The identifier assigned to the Purple Knight application when it was created in Azure.
- **Indicators:** Number of Azure AD security indicator tests that successfully completed (passed or IOE found)
- **Passed:** Total number of Azure AD tests that passed without finding any IOEs.
- **IOEs found:** Total number of Indicators of Exposure (IOEs) found across all selected Azure AD security indicators.
- **Not Relevant:** Total number of Azure AD security indicator tests that did not run because they do not apply to the selected environment.
- **Duration:** The amount of time (hh:mm:ss) it took to generate the assessment report for the Azure AD environment.
- **Run by:** The name of the account that ran the assessment report.

The report, in HTML format, is 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.
- Security_Assessment_Report_<forest-name>_<date/time stamp>.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: Active Directory](#) in order to select the 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.

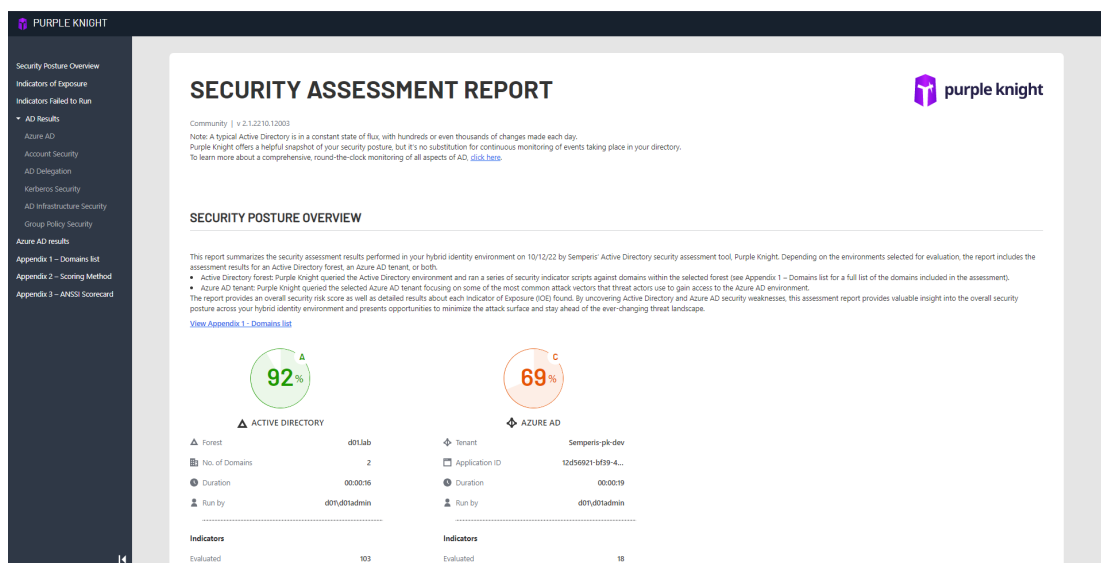


Figure 12: Security Assessment Report

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 Active Directory and Azure AD 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.
- *Azure AD Results:* Provides a recap of the Azure AD category score and details about the individual Azure AD security indicators.
 - *Categories: Azure AD:* 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: Azure AD:* For each Azure AD 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 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 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 10/12/22 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 Azure AD tenant, or both.

- 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).
- Azure AD tenant: Purple Knight queried the selected Azure AD tenant focusing on some of the most common attack vectors that threat actors use to gain access to the Azure AD environment.

The report provides an overall security risk score as well as detailed results about each Indicator of Exposure (IOE) found. By uncovering Active Directory and Azure AD 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](#)

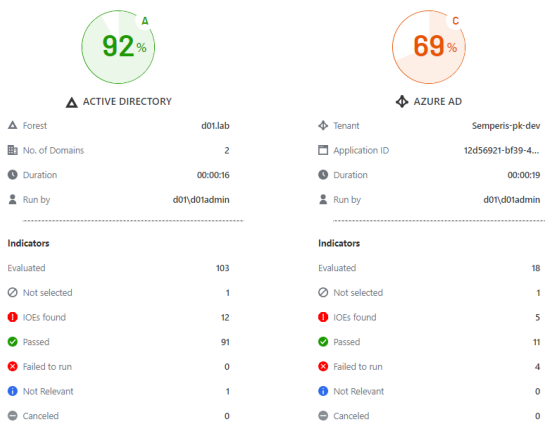


Figure 13: Security Assessment Report > Security Posture Overview

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.

Azure AD

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

- **Tenant:** The name of the Azure AD tenant that was evaluated.
- **Application ID:** The identifier assigned to the Purple Knight application when it was created in Azure.
- **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 Active Directory and Azure AD configurations that could be exploited by an attacker:

- **Critical IOEs Found:** Lists the security indicator tests that found critical IOEs in your Active Directory or Azure AD 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 Active Directory or Azure AD 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.

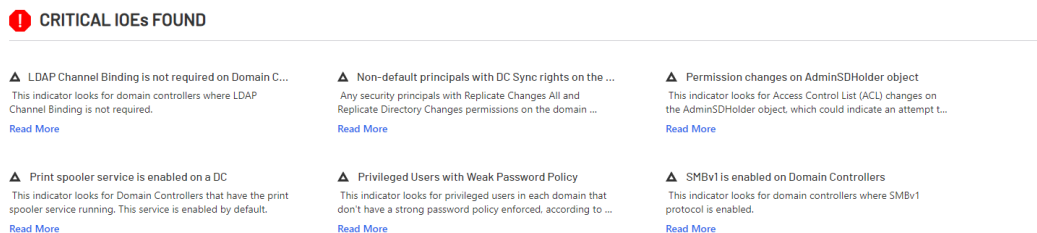


Figure 14: Security Assessment report: Critical IOEs Found

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

- Indicator representing the environment to which the indicator belongs:
 - ▲ Active Directory
 - ◆ Azure AD
- 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.

| ADDITIONAL IOEs FOUND | | | |
|--|------------|--|---------------------------|
| NAME | PLATFORM | SEVERITY LEVEL | ACTION |
| Built-in domain Administrator account used within the last two weeks | ▲ AD | Warning <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Changes to Pre-Windows 2000 Compatible Access Group membership | ▲ AD | Warning <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Changes to privileged group membership in the last 7 days | ▲ AD | Warning <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Check for guests having permission to invite other guests | ◆ Azure AD | Warning <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| LDAP signing is not required on Domain Controllers | ▲ AD | Warning <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Non-admin users can register custom applications | ◆ Azure AD | Warning <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| RC4 or DES encryption type are supported by Domain Controllers | ▲ AD | Warning <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Unrestricted user consent allowed | ◆ Azure AD | Warning <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Administrative units are not being used | ◆ Azure AD | Informational <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Changes to Default Domain Policy or Default Domain Controllers Policy in the last 7 days | ▲ AD | Informational <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| gMSA not in use | ▲ AD | Informational <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Guest users are not restricted | ◆ Azure AD | Informational <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Protected Users group not in use | ▲ AD | Informational <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Recent privileged account creation activity | ▲ AD | Informational <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |
| Unprivileged users can add computer accounts to the domain | ▲ AD | Informational <div><div></div><div></div><div></div><div></div><div></div></div> | Read More |

Figure 15: Security Assessment report: Additional IOEs Found

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

- **Name:** The name of the security indicator.
- **Platform:** The environment evaluated: AD or Azure AD.
- **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.









| INDICATORS FAILED TO RUN | | | |
|---|---|---|---------------------------|
| NAME | PLATFORM | SEVERITY LEVEL | ACTION |
| • AAD privileged users that are also privileged in AD | △ AD  Azure AD | Critical  | Read More |
| • Check for users with weak or no MFA |  Azure AD | Warning  | Read More |
| • MFA not configured for privileged accounts |  Azure AD | Warning  | Read More |
| • More than 5 Global Administrators exist | △ AD  Azure AD | Warning  | Read More |

Figure 16: Security Assessment report: Indicators Failed to Run

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 or Azure AD.
- **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.

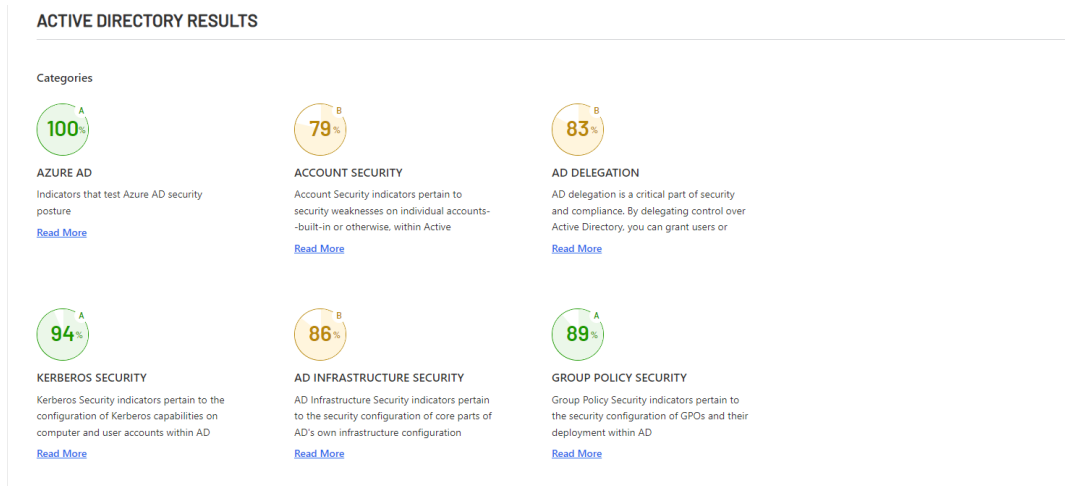


Figure 17: Security Assessment report: AD Results > Categories

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 18: 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, based on the importance of each category to the overall Active Directory security posture.
- **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.

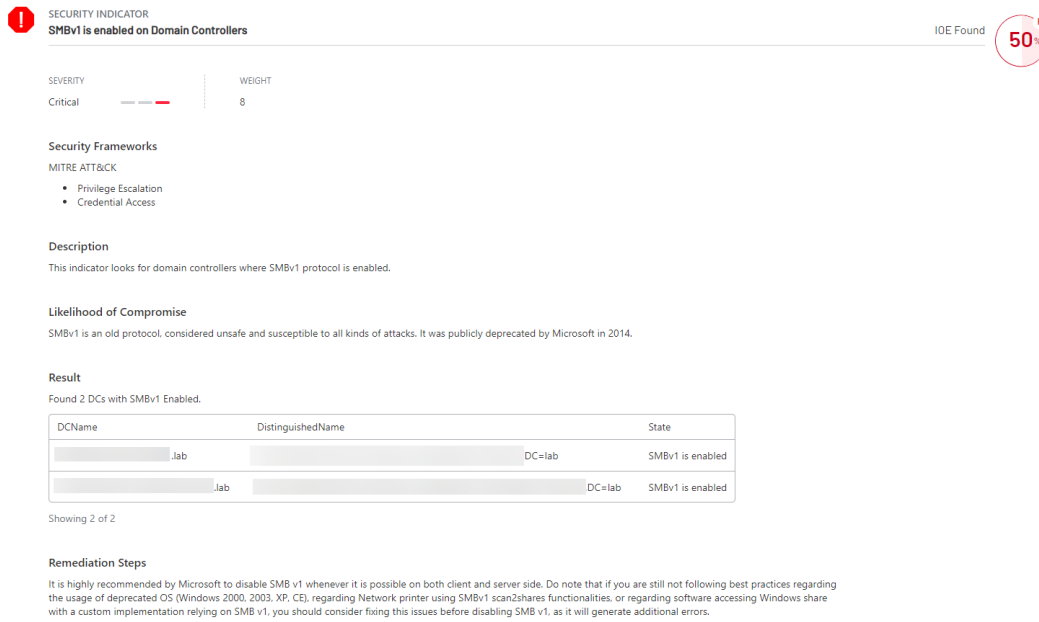








Figure 19: Security Assessment report: **IOE Found** results for an AD indicator

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, Warning, and Critical.
- **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 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 are 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.

Azure AD Results

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

- [Categories: Azure AD](#)
- [Test Result Details: Azure AD](#)

Categories: Azure AD

The **Categories** subsection in the **Azure AD Results** section provides a recap of the category scores.

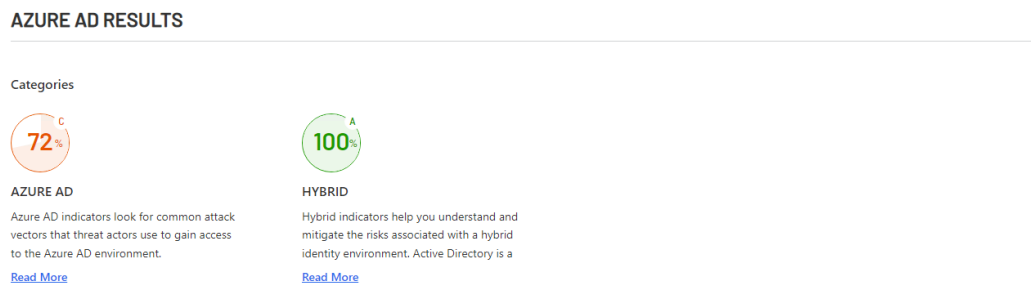


Figure 20: Security Assessment report: AAD Results > Categories

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: Azure AD

For each Azure AD 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 Azure AD security indicators.

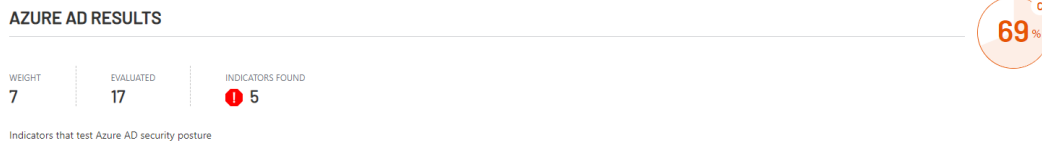


Figure 21: Security Assessment Report: Azure AD category results

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

- **Category name:** The name of the category (Azure AD or Hybrid).
- **Category score:** A percentage and letter grade for the Azure AD 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, based on the importance of the category to the overall Active Directory security posture.
- **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 Azure AD category.

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

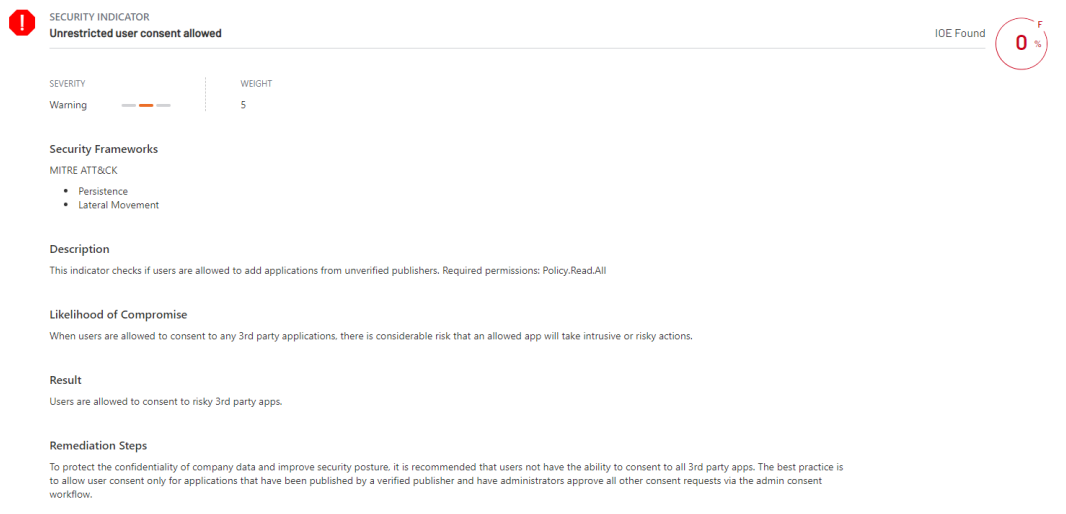








Figure 22: Security Assessment Report: **IOE Found** results for an Azure AD indicator

The following details are provided for each Azure AD 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, Warning, and Critical.
- **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 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 Azure AD 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 appendices provide the results for security indicators that returned more results (more than 10 objects) than can be displayed within the body of the report. The maximum number of objects included in the results appendix for a security indicator is 30 objects. A note is added to the end of the list indicating the name of the tab within the Excel spreadsheet where the results are saved.

**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 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 Active Directory and Azure AD environments that were assessed. Scores are represented by percentage and letter grade. It is recommended to aim for the highest score possible; a 100% (A) score indicates that there were no Indicators of Exposure (IOEs) found for the security indicators that were assessed. The following explanation is intended to help you understand the scoring methodology and factors used to calculate the scores presented in this report.

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 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 category score is based on the test results and weight of each individual security indicator that was evaluated within the relevant category.
- **Overall security posture score:** For Active Directory, the overall security posture score represents the weighted average of the individual AD category scores. For Azure AD, the overall security posture score represents the Azure AD category score, which is based on the test results and weight of each individual security indicator that was evaluated within that category.

**NOTE:**

When calculating the scores, only security indicators and categories included in the assessment are included (for example, security indicators that passed and resulting in IOEs found). Security indicators that were not selected, canceled, 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 forest.

To calculate the scores presented in the Security Assessment report, the following scoring methods and factors are used.

Letter grade

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

Table 5: Scoring legend

| Letter Grade | Percentage |
|--------------|------------|
| A | 90-100% |
| B | 80-89% |
| C | 70-79% |
| D | 60-69% |
| F | 0-59% |

Risk factors

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

- Severity (Informational, Warning, Critical)
- Likelihood of compromise
- The [DREAD Threat Probability Matrix](#), which is included in the appendix of the Security Assessment report.

DREAD Threat Probability Matrix

Table 6: 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 easy 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 Azure AD and a popular attack vector. So understanding where the Active Directory perimeter is connecting to Azure AD 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 Azure AD score. In addition, the Hybrid category and indicators can appear either under the Active Directory Results or Azure AD 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 AAD target.
- If the data source for a hybrid indicator includes AAD.GraphAPI, the indicator is included in the Azure AD score and the Azure AD 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 Azure AD tenant environment information are provided.

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

Table 7: Hybrid category: Scoring and placement in report

| Security Indicator | Target | Data Source | Score | Security Assessment Report |
|--|------------|-------------------------|-------|----------------------------|
| AAD privileged users that are also privileged in AD | AD; AAD | AD.LDAP AAD.GraphAPI | AAD | AAD Results |
| AD privileged users that are synced to AAD | AD; AAD | AD.LDAP AAD.GraphAPI | AAD | AAD Results |
| More than 5 Global Administrators exist | AD; AAD | AD.LDAP AAD.GraphAPI | AAD | AAD Results |
| Resource Based Constrained Delegation applied to AZUREADSSOACC account | AD; AAD | AD.LDAP | AD | AD Results |
| SSO computer account with password last set over 90 days ago | AD; AAD | 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 or .jpg format
- no larger than 250 KB

1. Place your company logo file 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.

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.

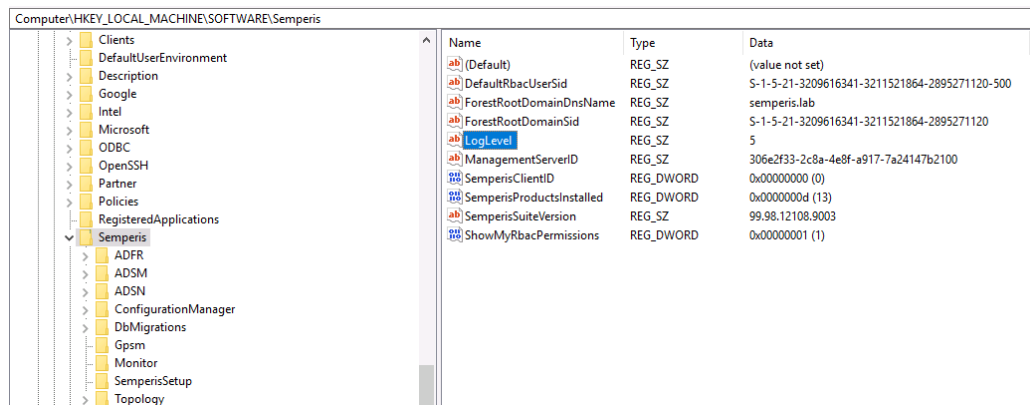


Figure 23: LogLevel registry key