semperis

Purple Knight

Version: 1.4

User Guide

January 2022 (4.0)

Legal Notice

semperis

Contents

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 an Active Directory environment. It explains how to run the tool as well as how to generate an Active Directory Security Assessment report that provides details about potential vulnerabilities found. 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

Styles and conventions used in this document

The following styles are used in this document.

Table 2: Document conventions and styles

Typeface	Description
Bold	Used for names of UI elements, such as buttons, pages, menus, options, fields, and columns.
Italics	Used for references to documents that are not hyperlinks to other documents or topics. Also used for dialog names and to introduce new terms.
`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.
Settings Link	Denotes a link within the web portal, usually found on a Settings page.

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 your Active Directory security posture. 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, and Kerberos security.

Each security indicator is mapped to security frameworks such as MITRE ATT&CK® tactic categories 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. The output of the utility is a comprehensive Active Directory Security Assessment report that provides an overall security posture score as well as detailed results about each Indicator of Exposure (IOE) found. Each IOE found highlights weak Active Directory 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 Active Directory environment by detecting software and configuration weaknesses using Indicators of Exposure (IOEs). IOEs help you understand how your Active Directory 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 v1.4

With this release of Purple Knight, the following features and enhancements are available to all Purple Knight users:

- Scan results are automatically saved to an Excel file.
- Ability to export the full report to .PDF or the scan result data to a series of .CSV files. The **SAVE AS** button on the **Report Summary** pages gives you these additional options for saving the assessment report details.

- Active Directory Security Assessment report includes an ANSSI appendix, which displays a breakdown of security indicators within the French National Agency for the Security of Information systems (ANSSI) framework.
- Ability to start a new scan without having to rerun the Purple Knight executable. Clicking the **NEW SCAN** button on the **Report Summary** page returns you to the **Environment** page to select the forest and domains to be assessed.
- Ability to view Purple Knight version and Semperis contact information. Click the **More** button in the top right corner of the screen to check for updates and view version information.
- Ability to customize the assessment report or Purple Knight tool. That is, you can add your company logo to the heading of the report and your company name to the header of the tool.

In addition, the following security indicators were added since the last major release of Purple Knight:

Account Security:

- Abnormal Password Refresh
- Changes to Pre-Windows 2000 Compatible Access Group membership
- Ephemeral Admins
- Users and computers without readable PGID

AD Delegation:

- Foreign Security Principals in Privileged Group
- Users with permissions to set Server Trust Account

AD Infrastructure Security:

- Dangerous Trust Attribute Set
- gMSA not used

Group Policy Security

- SYSVOL Executable Changes

Kerberos Security

- Write access to RBCD on DC
- Write access to RBCD on krbtgt account

For a list of bug fixes, improvements, and known issues, please see the ReleaseNotes.<*version*>.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: • 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: • Local client -> DC (TCP 389): Used for domain discovery; Also used by scans that use LDAP queries • Local client -> DC (TCP 445): Used for domain discovery; Also used by scans that attempt RPC calls, such as ZeroLogon and PrintSpooler • Local client -> Any server running AD CS web enrollment endpoint (HTTPS 443): Used by AD Certificate Authority security indicator; attempts authentication to CS web servers Purple Knight does NOT support running from an untrusted network location.

Table 3: System requirements

Software/Hardware	Requirement
Supported browsers	The latest versions of the following browsers are supported: • Google Chrome • Microsoft Edge • Microsoft Internet Explorer (IE)
Display resolution	Minimum: 1024 x 768
Logo size	Company logo requirements include: • 160 x 70 px • .jpg or .png • no larger than 250 KB For more information on how to add your company logo to the Security Assessment report, see *How to Add Company Branding*.

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.

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)

ReleaseNotes.<version>.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

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

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 heading and select **About**.

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

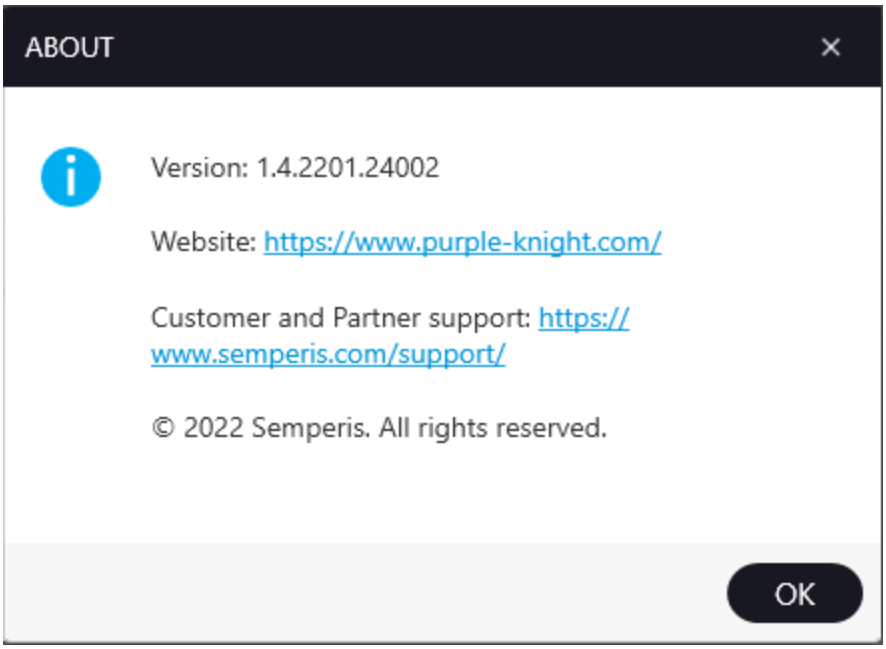

Figure 1: Purple Knight About box

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 heading and select **Check for update**.

   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 view the release notes and 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 environments and produce an Active Directory 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 a forest and domains to be evaluated.
    - *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 score and category scores 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 forest and domains to be used in the new scan.
    - **SAVE AS**: Click to save the full assessment report in .PDF format or the scan results data in a series of .CSV files.
    - **VIEW REPORT**: Click to view the full detailed Active Directory 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.

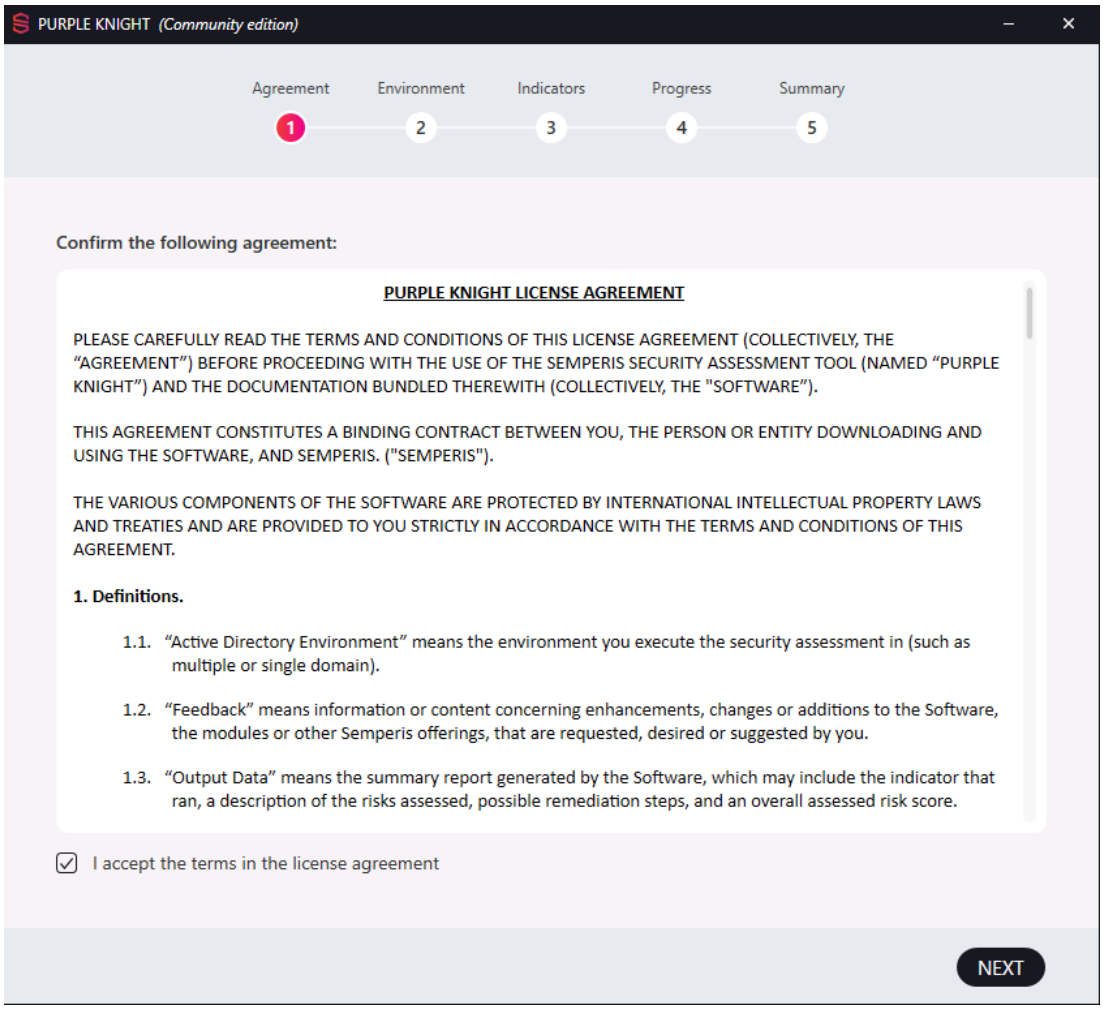

Figure 2: Agreement page

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 forest and domains to be assessed.

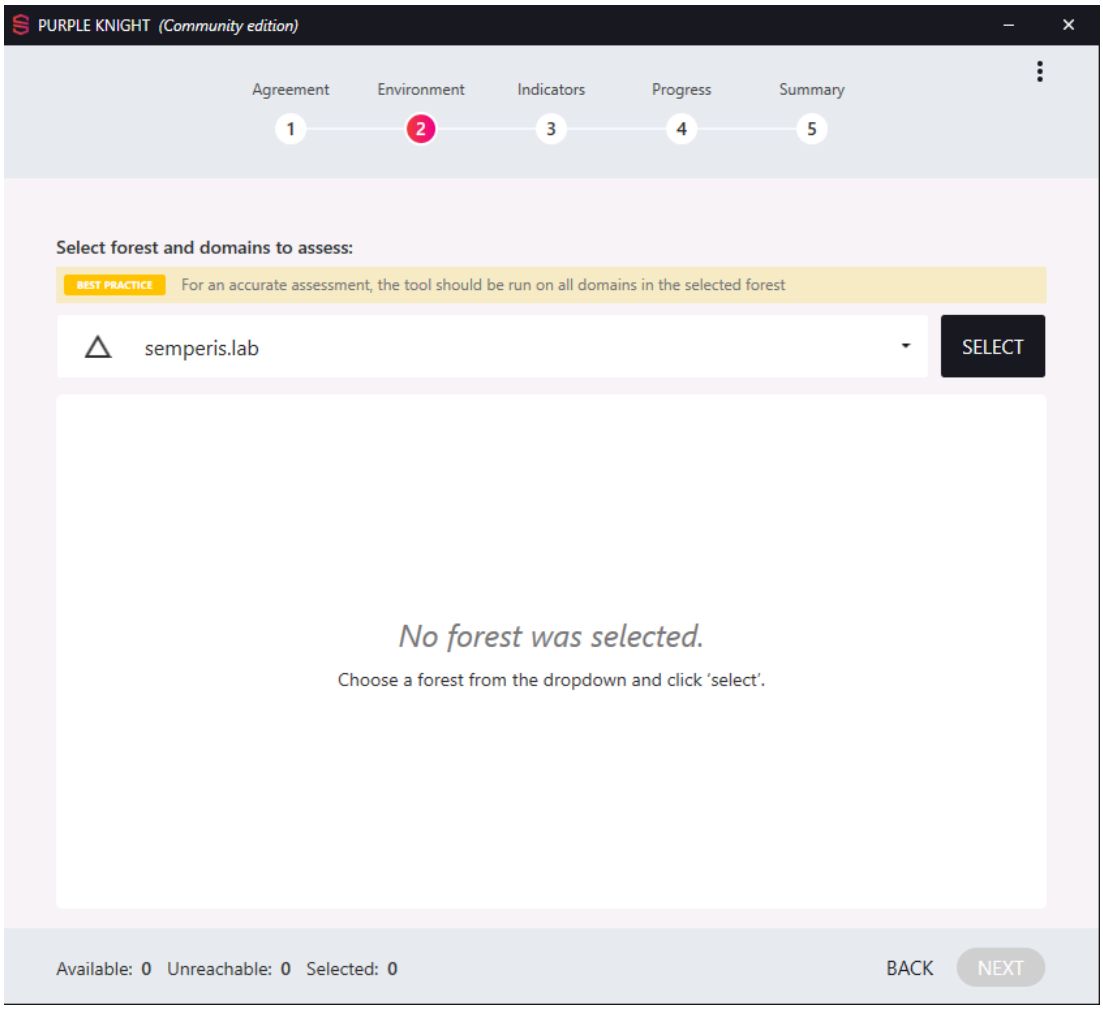

Figure 3: Environment page

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, the tool 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, the tool returns a list of available domains.

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

Figure 4: Domain selection tool bar

Use the domain selection controls as described below:

☑	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.
Search...	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. 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.

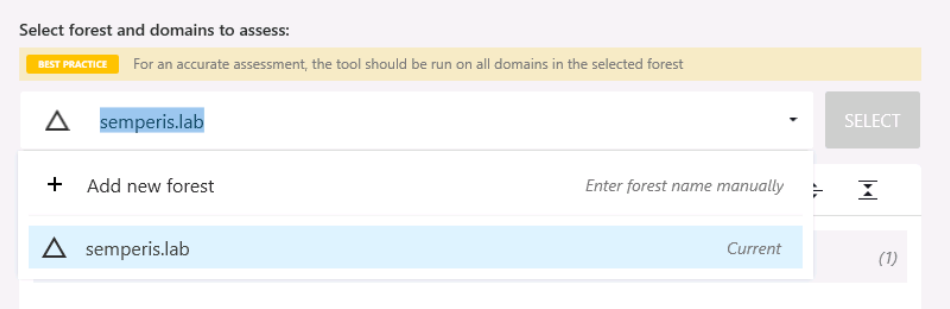

*Figure 5: Forest drop-down - **Add new forest** option*

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.

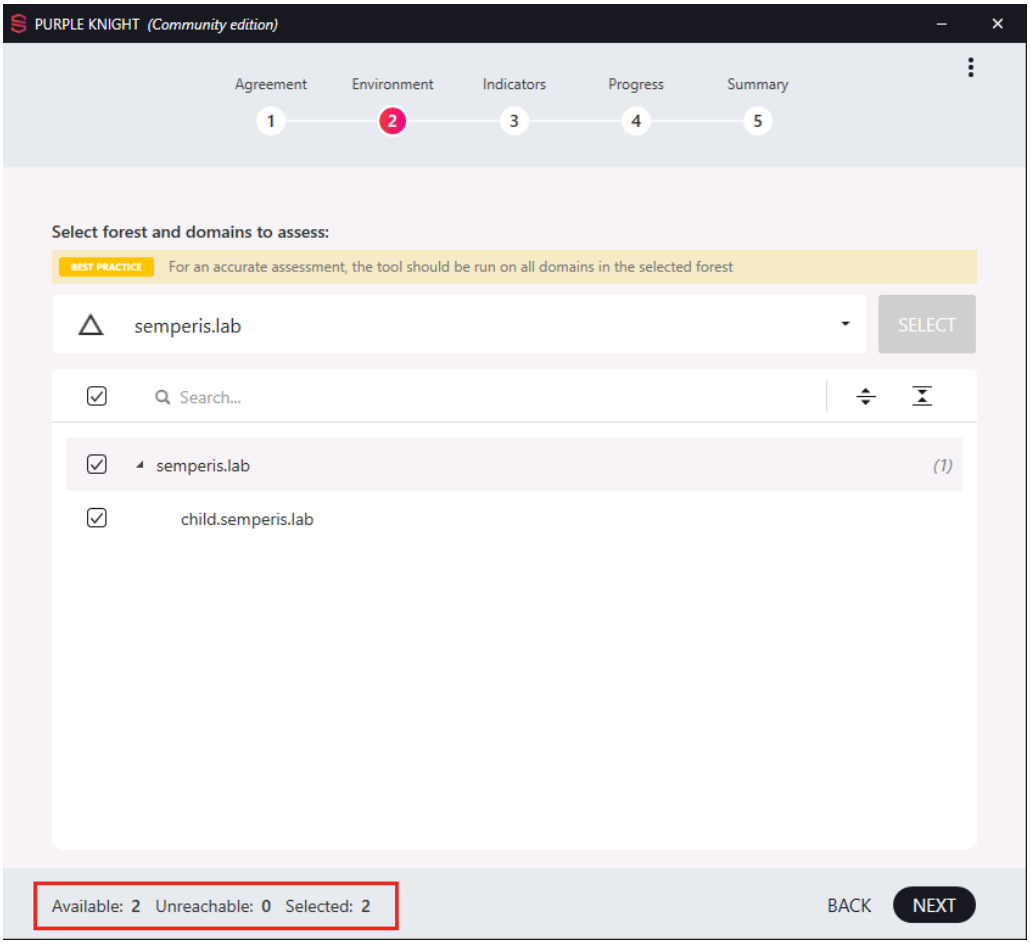

Figure 6: Environment Page with domains selected

4. After selecting the domains to be included, click **NEXT**.

Indicators page

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

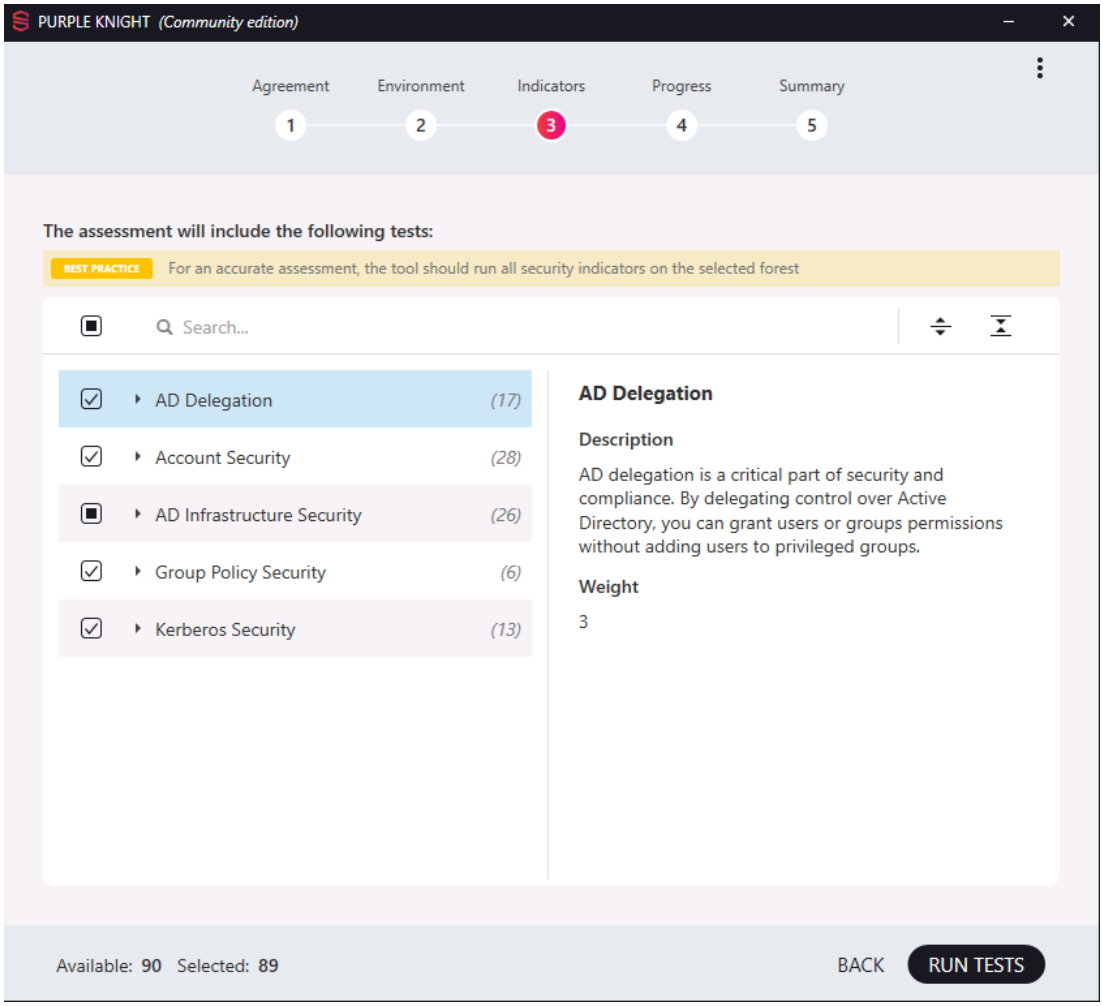

Figure 7: Indicators page

Security indicator selection

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

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

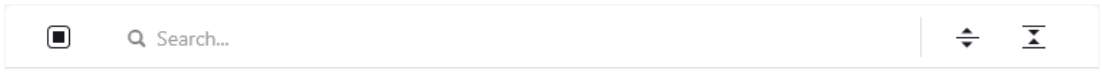

Figure 8: Security Indicator selection tool bar

Use the security indicator selection controls as described below:

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.

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
- Security Frameworks
- Description
- Likelihood of Compromise

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**.

Progress page

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

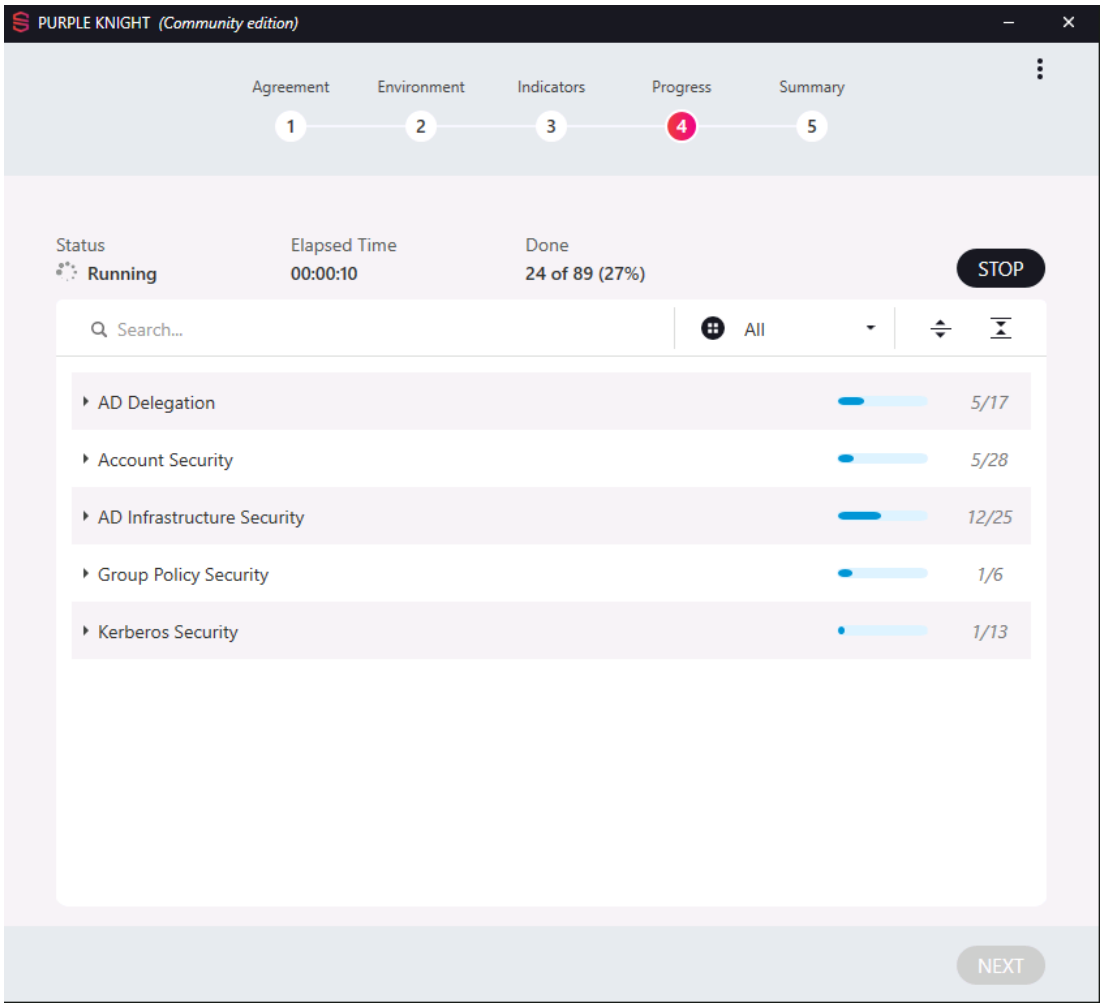

Figure 9: Progress page

Overall report progress

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

- **Status**: The current overall status of the tests being run.
- **Elapsed Time**: The amount of time it is taking to run the assessment report.
- **Done**: How many tests have completed against the total number of selected tests to be run. The completed test count includes security indicators that passed without

finding any IOE and those that found an IOE. It does not include security indicators that failed to run.

Individual security indicator progress

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

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

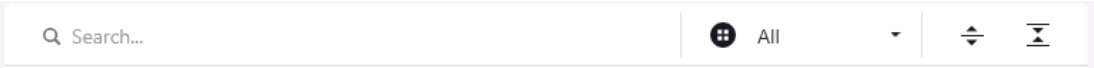

Figure 10: Progress page tool bar

Use the Progress page controls as described below:

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.
All	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.

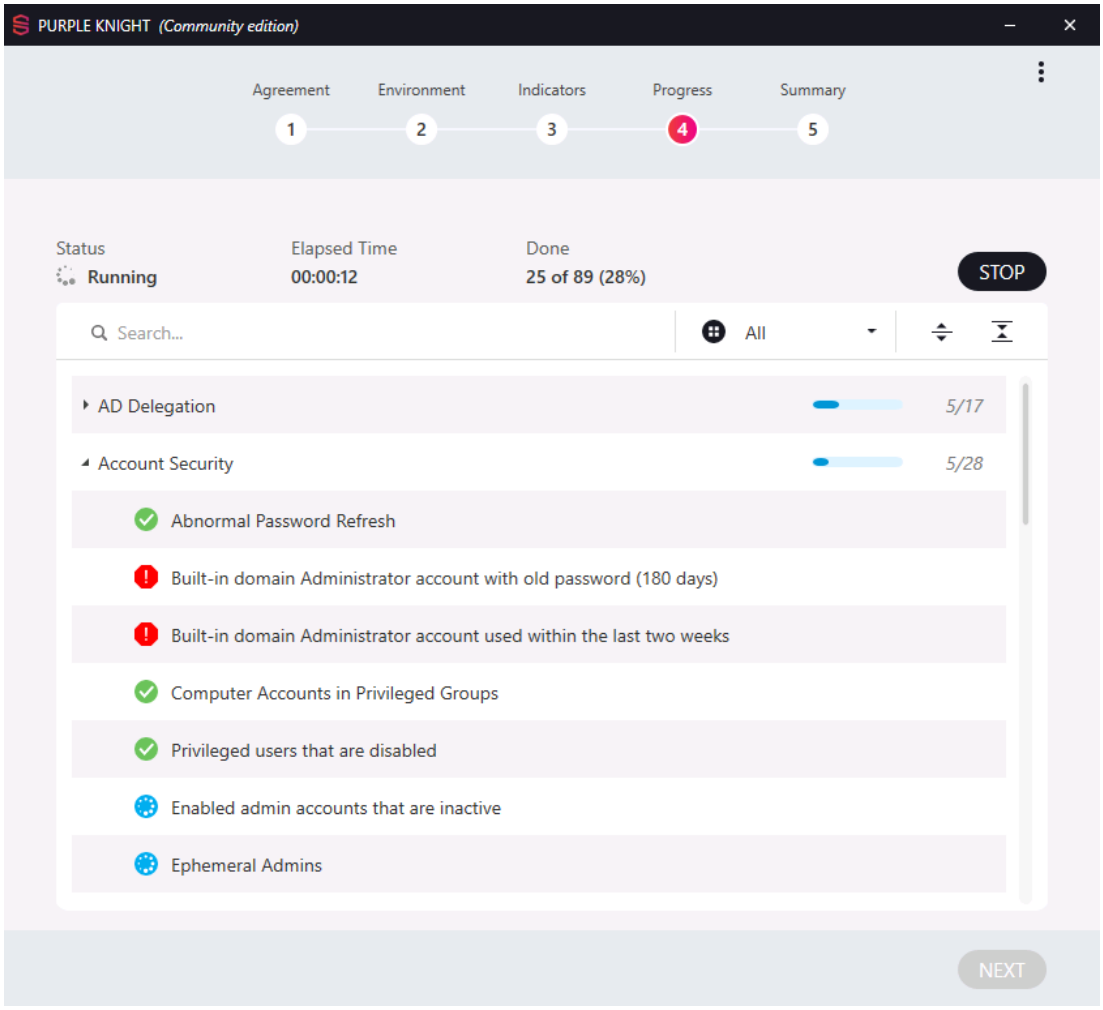

Figure 11: Progress page with category expanded

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

To stop running the tests in progress:

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

NOTE:

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

Report Summary page

The **Report Summary** page summarizes the results of the Active Directory security assessment, including an overall security posture score, which is based on the category scores. The first five category scores are also displayed, which are based on the test results and weight of individual security indicators evaluated within the selected category.

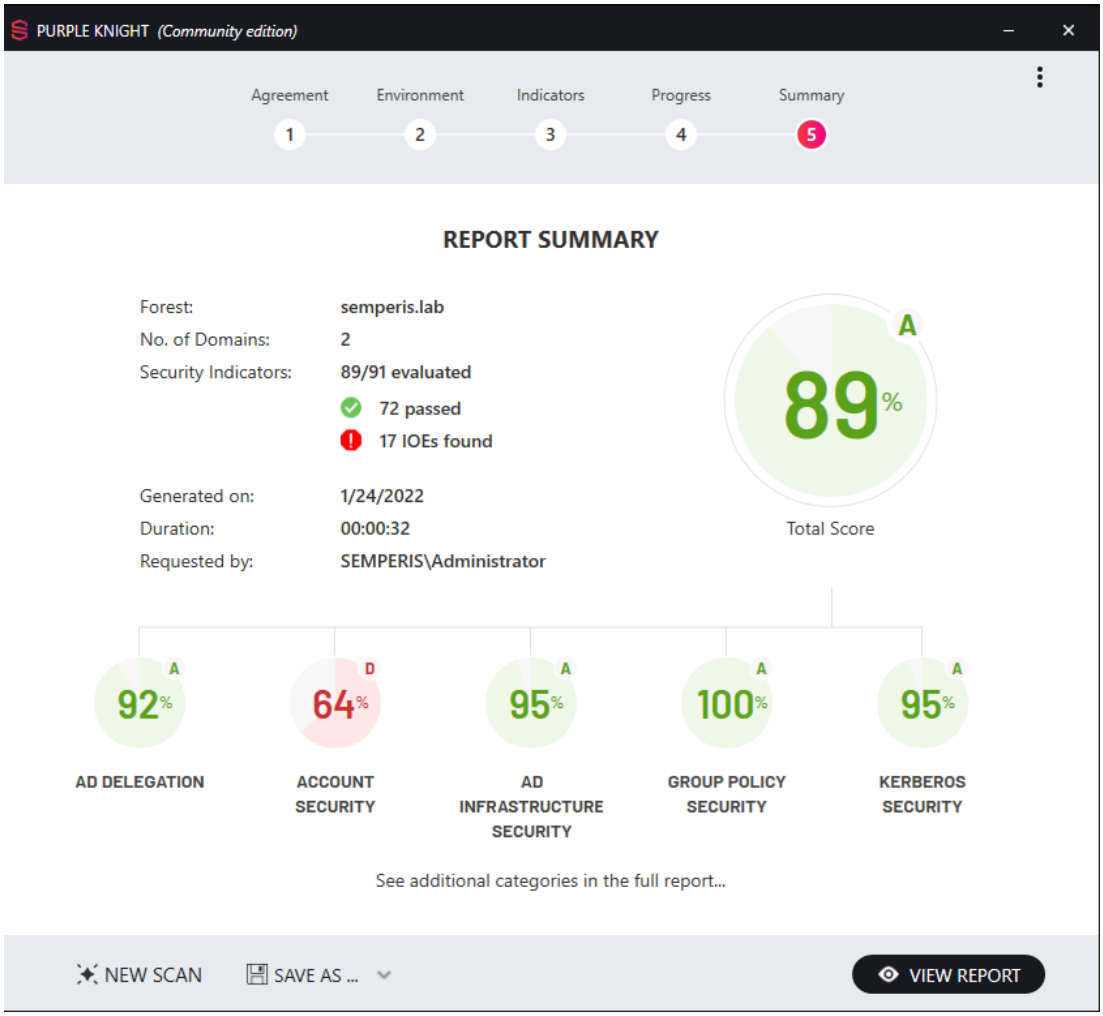

Figure 12: Report Summary page

The report summary includes the following information:

- **Forest**: The name of the forest that was evaluated.
- **No. of Domains**: The number of domains that were evaluated.
- **Security Indicators**: Summarizes the results of the security indicators included in the current assessment.
  - Evaluated: Number of security indicator tests that successfully completed (passed or IOE found) against the total number of security indicators selected for inclusion.
  - Passed: Total number of tests that passed without finding any IOEs.
  - IOEs Found: Total number of Indicators of Exposure (IOEs) found across all selected security indicators.
- **Generated on**: The date the assessment report was generated.
- **Duration**: The amount of time (hh:mm:ss) it took to generate the assessment report.

- **Requested by**: The name of the account that ran the assessment report.
- **Total Score**: Overall security posture score for all security indicators that successfully ran (passed or IOE found).
- **Category Scores**: Score for the first five categories based on the test results and weight of each security indicator that was evaluated within the selected category.

  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 indicators completed.

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 the utility.

NEW SCAN Click to start a new scan. Clicking this button returns you to the *Environment page* 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 Active Directory Security Assessment report in your default browser.

CHAPTER 4

AD Security Assessment Report

The **Report Summary** page in the Purple Knight tool displays the overall security posture score and scores for the first five categories. Whereas, the full Active Directory Security Assessment report provides the overall security posture score (percentage and letter score), detailed findings for each security indicator test, and recommended actions that can be taken to address any weaknesses or risky configurations that are found.

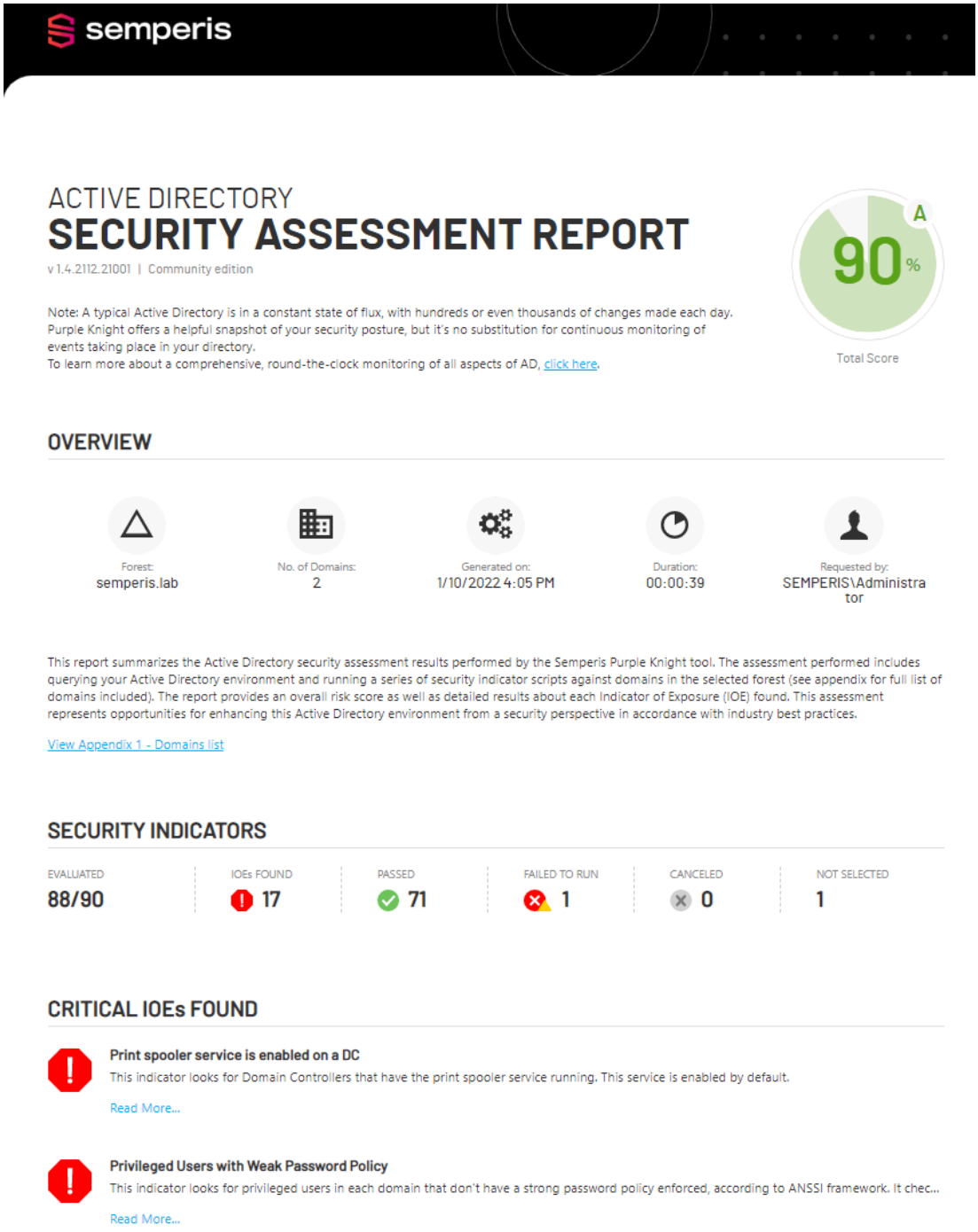

Figure 13: AD Security Assessment Report

The report is divided into the following sections:

- *Overview*: Provides environment and run details.
- *Security Indicators*: Summarizes the results of the security indicators included in the current assessment.
- *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.
- *Categories*: 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*: This section is organized by category and includes details about each security indicator within each category. For each 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 to the header. For more information on adding or replacing your company logo, see How to Add Company Branding.

Overview

An **Overview** containing the following information is provided at the top of each Active Directory Security Assessment report:

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

The **Overview** also provides a general description for the Security Assessment report and a link to the Domains list appendix.

Security Indicators

The **SECURITY INDICATORS** section of the report summarizes the results of the security indicators included in the current assessment.

Figure 14: Security Assessment report: Security Indicators

This summary includes the following information:

- **Evaluated**: Number of security indicator tests that successfully completed (returned a result of **Passed** or **IOE Found**) against the total number of security indicators selected for inclusion.
- **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.
- **Canceled**: Number of tests that were canceled before they finished.
- **Not Selected**: Number of security indicators that were not included in the current assessment.

Critical IOEs Found

The **CRITICAL IOEs FOUND** section lists the security indicator tests that found critical IOEs in your Active Directory 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.

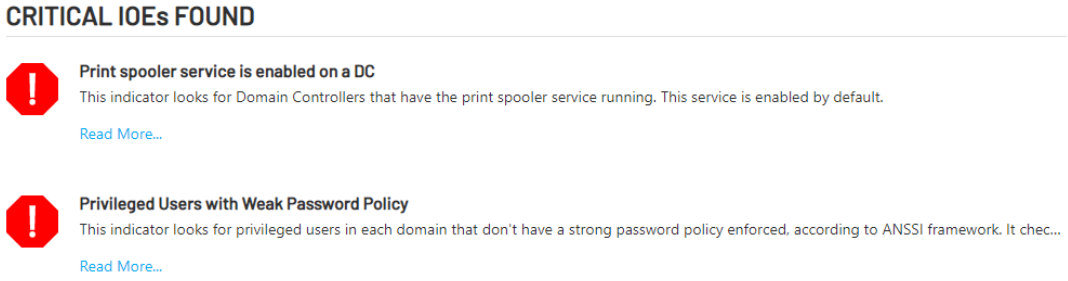

Figure 15: Security Assessment report: Critical IOEs Found

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

- 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.

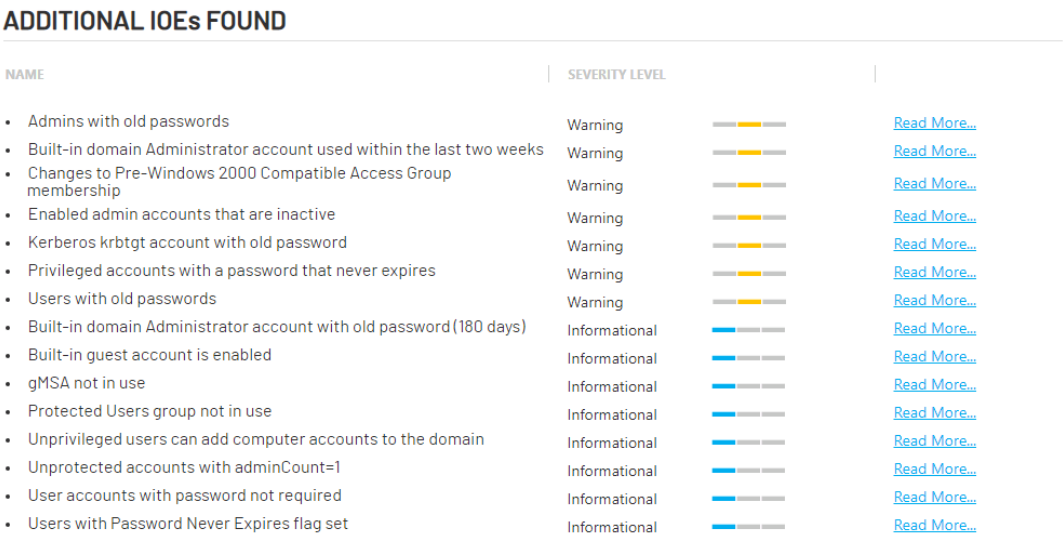

Figure 16: Security Assessment report: Additional IOEs Found

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

- **Name**: The name of the security indicator.
- **Severity Level**: The severity level assigned to the security indicator.
- ***Read More***: A link to view the full 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. For example, an indicator will return "Failed to Run" when it is not applicable to the selected forest. Note that indicators that fail to run do NOT affect the security posture scores.

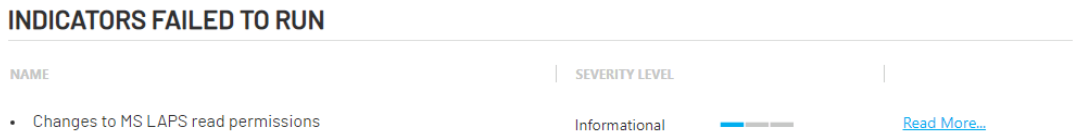

Figure 17: Security Assessment report: Indicators Failed to Run

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

- **Name**: The name of the security indicator.
- **Severity Level**: The severity level assigned to the security indicator.
- ***Read More***: A link to view the full description of the security indicator including a message as to why the security indicator test did not run.

Categories

The **CATEGORIES** section in the Security Assessment report provides a recap of the category scores.

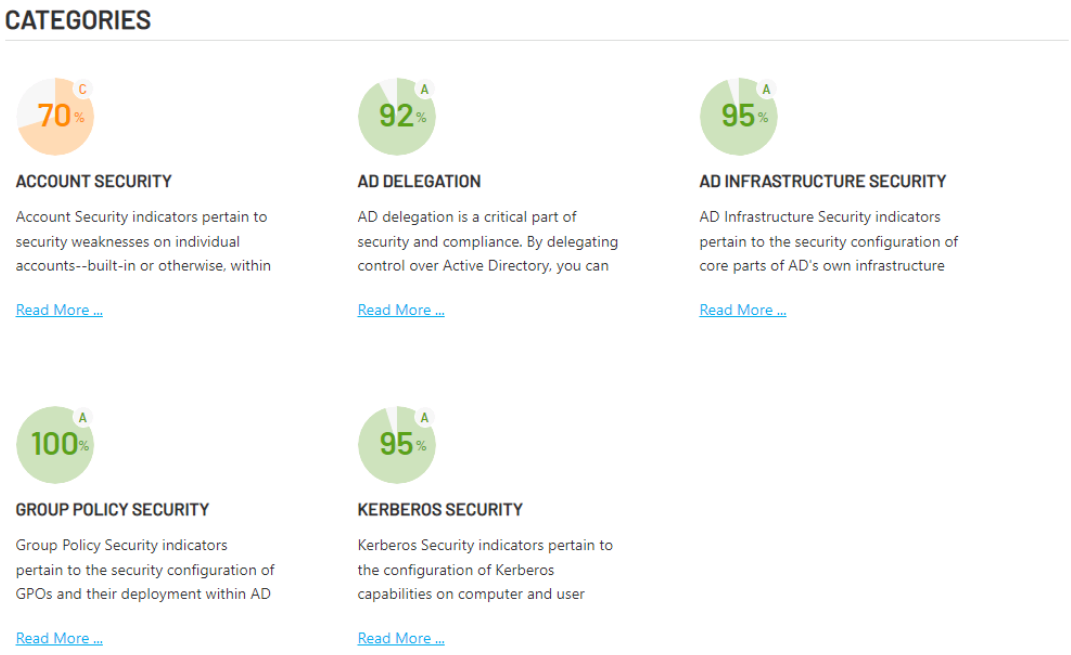

Figure 18: Security Assessment report: Categories

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

For each 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.

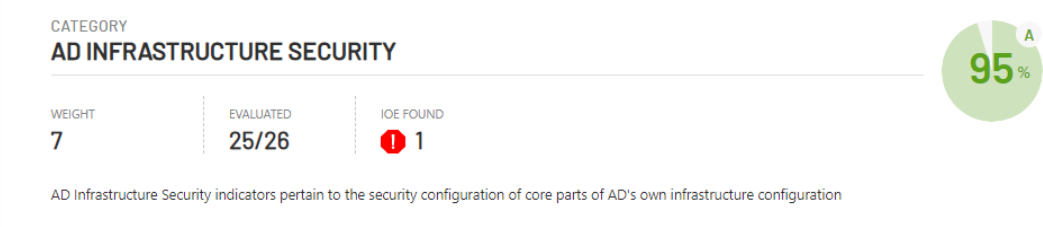

Figure 19: Security Assessment report: AD Infrastructure Security category results

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.
- **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 evaluated against the total number of security indicators in the category selected for evaluation.

- **IOE 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.

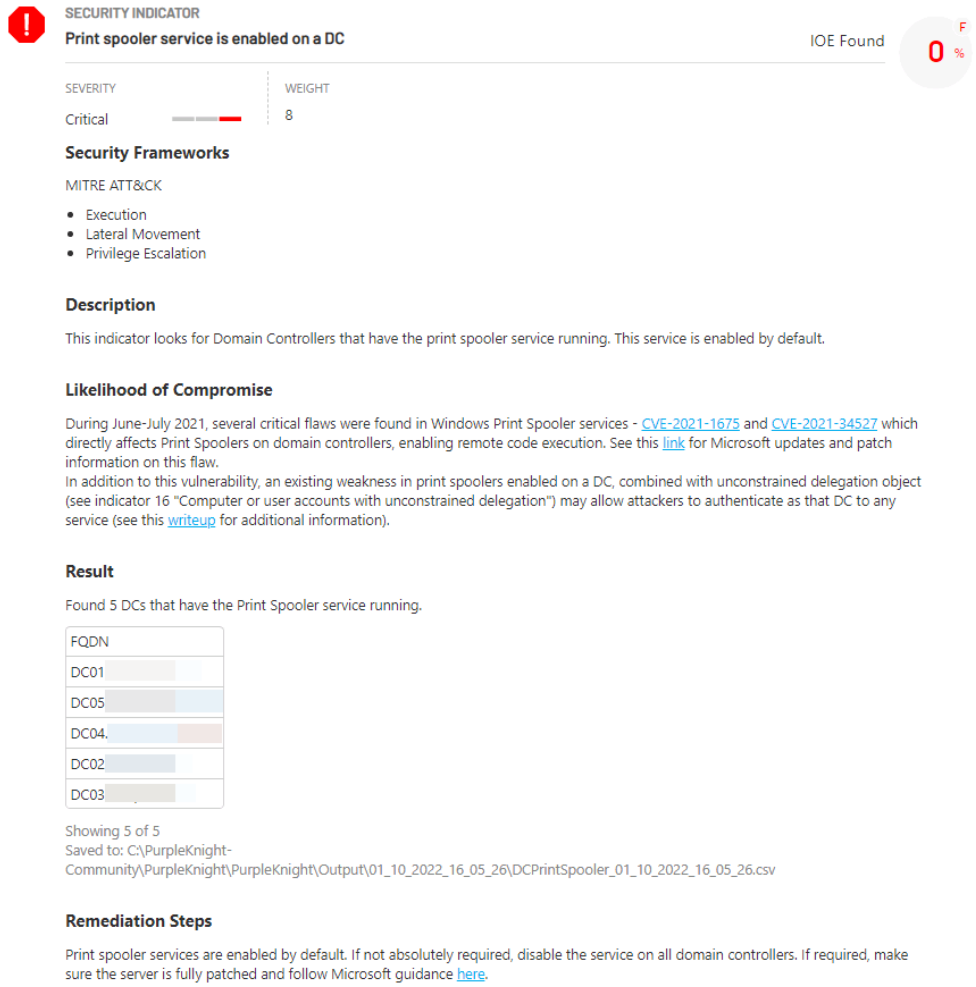

Figure 20: Security Assessment report: Print spooler service is enabled on a DC test result details

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.

   Passed without triggering an indicator.

   Failed to run.

   Canceled before test completed.

  No icon 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).
  - **Passed**: 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 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 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.

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 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.
- 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 environment that was 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**: The overall security posture score represents the weighted average of the category scores.

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 4: 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 5: 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.

DREAD		High (3)	Medium (2)	Low(1)
Exploitability	How easy would it be to launch the attack?	A novice programmer could perform the attack with minimal effort.	Requires a skilled programmer to launch the attack and be able to repeat the steps.	Requires an extremely skilled programmer with in-depth knowledge to launch an attack.
Affected users	How many users would be impacted?	A large percentage or all users are impacted; default configuration and key customers are impacted.	A moderate percentage of users are impacted; non-default configuration is impacted.	A very small percentage of users are impacted; anonymous users are affected.
Discoverability	How each would it be for the attacker to discover this exposure?	Easily discovered. Published information explains the vulnerability and attack technique. The vulnerability is found in commonly used features and is very noticeable.	Would require some effort to discover and successfully exploit. The vulnerability is found in a seldomly-used part of the product and only a few users should discover it.	Hard to discover. The issue is obscure, and it is unlikely that users would discover a way to cause damage.

APPENDIX B

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.

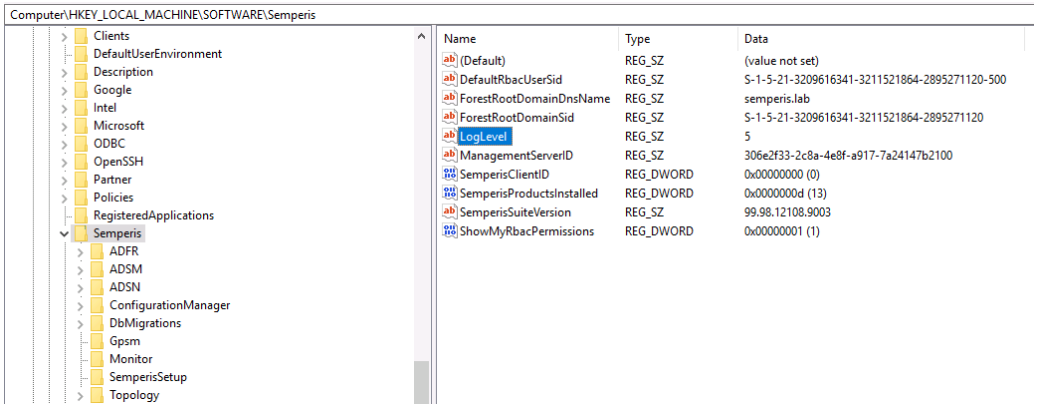

Figure 21: LogLevel registry key

APPENDIX C

How to Add Company Branding

You can customize Purple Knight in the following ways:

- Add your company logo to the header (top right corner) of the report.
- Add your company name to the header 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 a Security Assessment report, your company logo will appear in the banner at the top of the 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 and 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.