# Purple Knight - Community Edition v2.0

## Getting Started Guide

## August 2022

Welcome to the *Purple Knight Community Edition Getting Started Guide*. This document is intended for Security and IT professionals interested in performing a security posture assessment on an Active Directory environment. It 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.

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.

## 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. In this latest version, 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.

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. For more information, see the *Purple Knight User Guide*.

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.

# 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 1: System requirements*

| Software/Hardware | Requirement |
|---|---|
| **Operating system** | Supported operating systems include:<br>• Windows 8.1<br>• Windows 10<br>• Windows Server 2012 R2<br>• Windows Server 2016<br>• Windows Server 2019 |
| **.NET Framework** | .NET Framework version 4.6.2 or later |
| **Windows PowerShell** | Windows PowerShell version 4.0 or later<br>Semperis-built scripts require the "RemoteSigned" execution policy (default execution policy for Windows server computers). For custom indicators, see the *Custom Indicators* requirements. |
| **Network Access** | The following ports are required to run Purple Knight:<br>• Local client -> DC (TCP 389): Used for domain discovery; Also used by scans that use LDAP queries<br>• Local client -> DC (TCP 445): Used for domain discovery; Also used by scans that attempt RPC calls, such as ZeroLogon and PrintSpooler<br>• 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<br>Purple Knight does NOT support running from an untrusted network location. |
| **Supported browsers** | The latest versions of the following browsers are supported:<br>• Google Chrome<br>• Microsoft Edge |
| **Display resolution** | Minimum: 1024 x 768 |
| **Logo size** | Company logo requirements include: |

*Table 1: System requirements*

| Software/Hardware | Requirement |
|---|---|
| | • 160 x 70 px<br>• .jpg or .png<br>• no larger than 250 KB<br>To add a company logo to the header in the Security Assessment report, place your company logo file in a **custom** folder under the **PurpleKnight** directory (for example, **C:\PurpleKnight\custom\logo.png**). |
| **Custom Indicators** | Since custom scripts are not signed, they require the "Unrestricted" or "Bypass" PowerShell execution policy; therefore when opting in to include custom indicators, Purple Knight must be run as local Admin to enable the "Bypass" execution policy.<br>Custom scripts must follow specific structure for metadata and output. For more information, see the *Purple Knight Custom Indicators Integration Guide*. |

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

*Table 2: Microsoft Azure AD connection requirements*

| Azure Component | Requirement |
|---|---|
| Azure AD tenant | Supports only one Azure AD tenant per Purple Knight instance. |
| Azure application registration | 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.<br>Required permissions (API permissions > Microsoft Graph > Application permissions):<br>• User.Read.All<br>• Group.Read.All<br>• Application.Read.All<br>In addition, the following permissions must be granted to the application in order to run the Azure AD security indicators:<br>• AdministrativeUnit.Read.All<br>• Application.Read.All *<br>• Directory.Read.All<br>• Policy.Read.All<br>• PrivilegedAccess.Read.AzureAD<br>• Reports.Read.All |

*Table 2: Microsoft Azure AD connection requirements*

| Azure Component | Requirement |
|---|---|
| | • RoleManagement.Read.Directory<br>• User.Read.All *<br>* 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. |

# 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.*

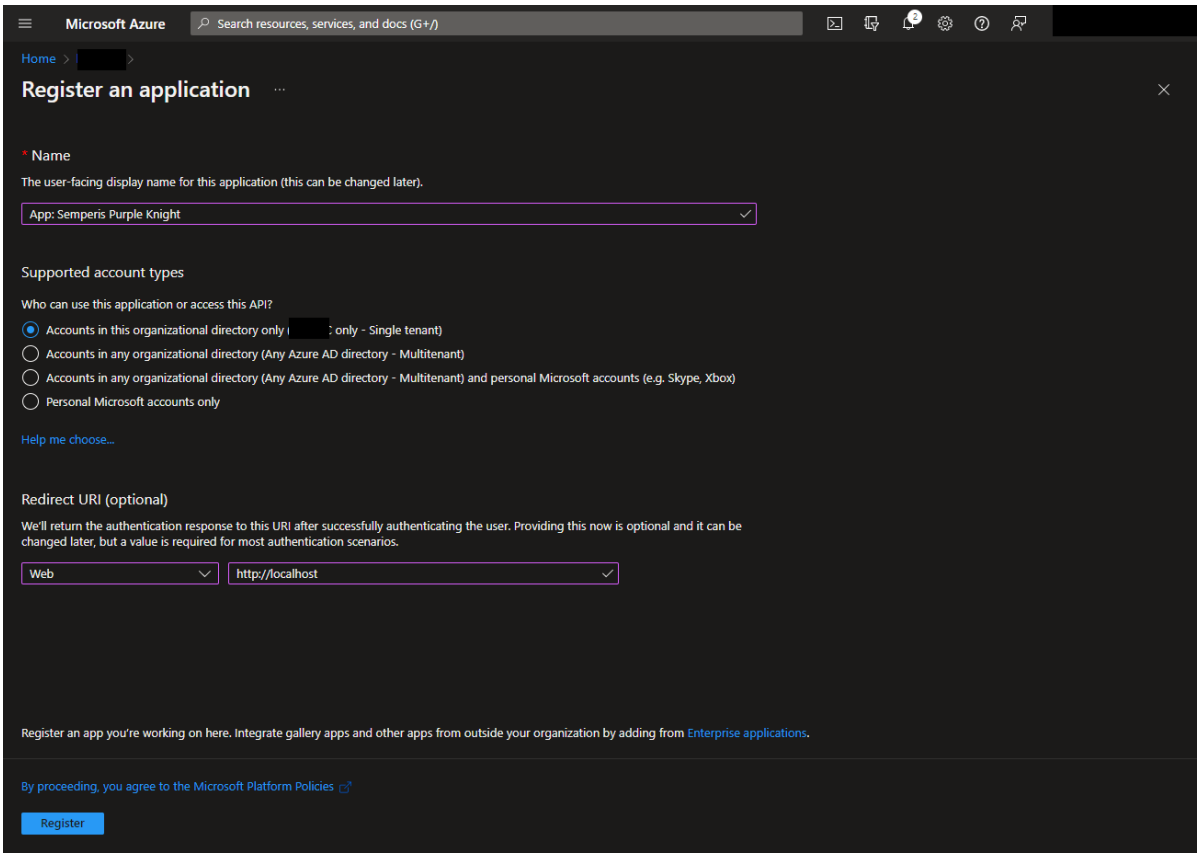
Before you can configure the Azure AD connection in Purple Knight, you must create and configure an application registration that has the ability to generate a client secret (referred to here as the Purple Knight application).

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.

***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 Read permissions:

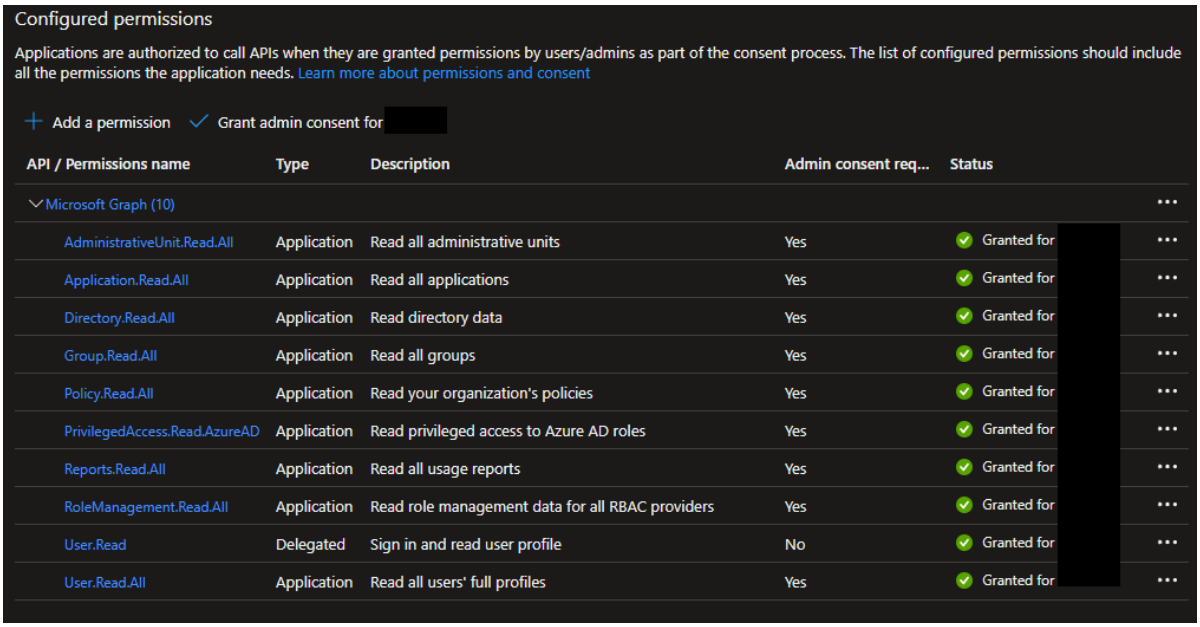
   - AdministrativeUnit.Read.All
   - Application.Read.All

- Directory.Read.All
- Group.Read.All
- Policy.Read.All
- PrivilegedAccess.Read.AzureAD
- Reports.Read.All
- RoleManagement.Read.Directory
- User.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.




***NOTE:***
*The User.Read permission (basic metadata about yourself) is added automatically to new applications. This permission can be removed; it is not used for Purple Knight.*

***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.

> ***NOTE:***
> *When running Purple Knight in large enterprise environments, you may want to consider the following:*
>
> ***Environment page: Domain Selection***
>
> *It may be beneficial to run Purple Knight in stages; excluding very large domains or those connecting across the WAN at first.*
>
> ***Indicators page: Indicator Selection***
>
> *If you are interested in 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.*

# 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.