

Purple Knight - Community Edition v4.2

Getting Started Guide

December 2023

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 a hybrid Active Directory environment that includes Active Directory, Azure AD, and/or Okta. 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. 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 unauthorized access or your Okta environment checking for activities that may indicate unauthorized access attempts, suspicious behavior, or potential threats within the Okta infrastructure.

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, Azure AD, or Okta environment 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.

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

1. Run the following command from the directory where the PurpleKnight.exe file is located:
`runas/env/netonly/user:<domainname>\<username> PurpleKnight.exe`
2. You may need to manually enter the forest name in the forest enumeration screen.

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

Table 1: 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 5.0 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• 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.
Supported browsers	The latest versions of the following browsers are supported: <ul style="list-style-type: none">• Google Chrome• Microsoft Edge

Table 1: System requirements

Software/Hardware	Requirement
Display resolution	Minimum: 1024 x 768
Logo size	<p>Company logo requirements include:</p> <ul style="list-style-type: none"> • 160 x 70 px • .jpg, .png, pr .jpeg format • no larger than 250 KB • file name must be logo.png, logo.jpg, or logo.jpeg <p>To add a company logo to the header in the Security Assessment report, place your company logo file (logo.<extension>) in a custom folder under the PurpleKnight directory. For example, C:\PurpleKnight\custom\logo.png</p>

In addition, for those wanting to run the Azure AD security indicators, the following system requirements also apply. For more information on configuring Azure AD to run Purple Knight security indicators, see [Create and Configure Application Registration](#).

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	<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.All • 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 • Device.Read.All • Directory.Read.All • Policy.Read.All • PrivilegedAccess.Read.AzureAD

Table 2: Microsoft Azure AD connection requirements

Azure Component	Requirement
	<ul style="list-style-type: none">• Reports.Read.All• RoleManagement.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>

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

Table 3: Okta connection requirements

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

Additional Permission Requirements

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

Privileged Users with Weak Password Policy

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

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

**NOTE:**

Further details can be found in the Microsoft document [AD DS: Fine-Grained Password Policies](#).

Unsecured DNS Configuration

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

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:**

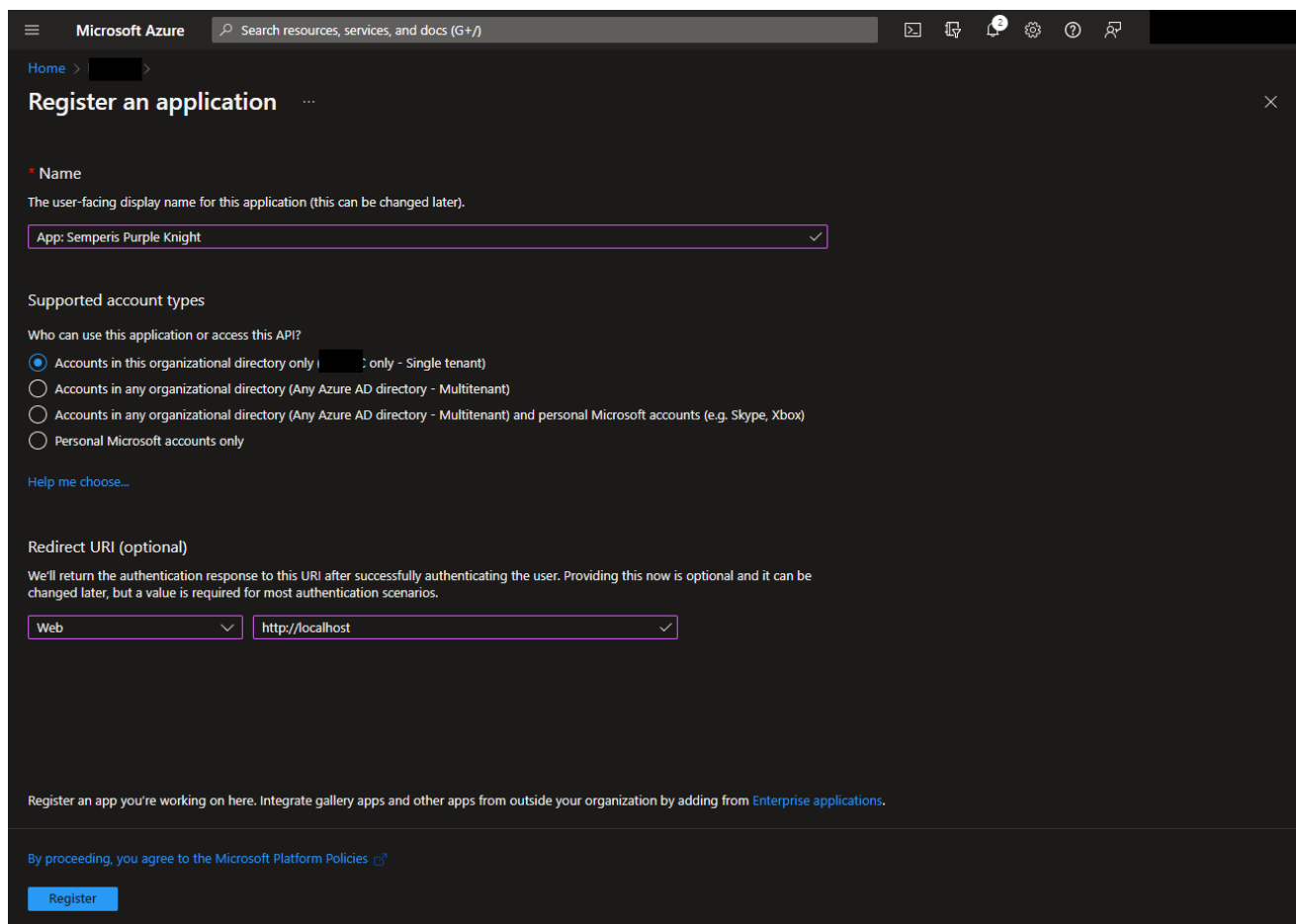
To run Purple Knight in your Azure AD environment, you need to create and update the app registration in Azure AD with a defined and consented set of application permissions for the Microsoft Graph. To automate this step, Semperis provides a [PowerShell script](#), which is available in GitHub.

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).



Microsoft Azure Search resources, services, and docs (G+/)

Home > [redacted]

Register an application

Name

The user-facing display name for this application (this can be changed later).

App: Semperis Purple Knight ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only ([redacted] only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ✓ http://localhost ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

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
- Device.Read.All
- Directory.Read.All
- Policy.Read.All
- PrivilegedAccess.Read.AzureAD
- Reports.Read.All
- RoleManagement.Read.All
- RoleManagement.Read.Directory
- User.Read.All
- UserAuthenticationMethod.Read.All

Click the **Add permissions** button.

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

API / Permissions name	Type	Description	Admin consent requ...	Status	
▼ Microsoft Graph (12)					...
AdministrativeUnit.Read.All	Application	Read all administrative units	Yes	✓ Granted for	...
Application.Read.All	Application	Read all applications	Yes	✓ Granted for	...
AuditLog.Read.All	Application	Read all audit log data	Yes	✓ Granted for	...
Device.Read.All	Application	Read all devices	Yes	✓ Granted for	...
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for	...
Policy.Read.All	Application	Read your organization's policies	Yes	✓ Granted for	...
PrivilegedAccess.Read.AzureAD	Application	Read privileged access to Azure AD roles	Yes	✓ Granted for	...
Reports.Read.All	Application	Read all usage reports	Yes	✓ Granted for	...
RoleManagement.Read.All	Application	Read role management data for all RBAC providers	Yes	✓ Granted for	...
RoleManagement.Read.Directory	Application	Read all directory RBAC settings	Yes	✓ Granted for	...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for	...
UserAuthenticationMethod.Read.All	Application	Read all users' authentication methods	Yes	✓ Granted for	...

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 vault 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. Purple Knight runs with the following execution permissions:
 - RemoteSigned
 - Unrestricted
 - Bypass

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 to set the execution permission on the "CurrentUser" scope:

```
Set-ExecutionPolicy -Scope CurrentUser 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.

Information included in this document is confidential and/or proprietary to Semperis, is protected by copyright and trademark laws and subject to other intellectual property rights and unfair competition laws of the United States, foreign jurisdictions and international conventions. 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 disclaims any responsibility for incidental or consequential damages in connection with the furnishing, performance, use of, or reliance on this document or its content.