Purple Knight - Community Edition v1.4

Getting Started Guide

January 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 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.

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. 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: • 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.
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 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**).

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.

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

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 - Community Edition. 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.