Gold Finger

Active Directory Privileged Access Assessor

User's Guide

Gold Finger

Active Directory Privileged Access Assessor

Contents

Active Directory Privileged Access Assessor

Introduction

In organizations that operate on the Microsoft Windows Server platform, the entirety of their building blocks of cyber security i.e. all organizational domain user accounts, computer accounts, and security groups are stored, managed and secured in Active Directory.

Each one of these building blocks is represented as an object within Active Directory and is protected by an access control list (ACL), which contains access control entries (ACEs) that specify who is allowed and denied what security permissions on the object.

Together, there exist hundreds of thousands of security permissions in the ACLs of thousands of Active Directory objects, granted to a large number of users and groups, and it is the net resulting cumulative i.e. effective permissions that actually govern exactly who has what privileged access on thousands of objects in and across an Active Directory domain.

To secure Active Directory, accurately identify privileged users, control access to privileged users and groups, maintain security and fulfill various GRC driven audit needs, organizations need to be able to accurately assess privileged access domain-wide in Active Directory.

The *Active Directory Privileged Access Assessor* is unique in its ability to accurately and automatically assess privileged access domain-wide in Active Directory. It can uniquely –

- ✓ Accurately assess privileged access on thousands of objects in an Active Directory domain, based on the accurate determination of effective permissions/access domain-wide.
- ✓ Assess privileged access in terms of who can enact which administrative tasks in Active Directory, as well as identify the underlying permissions that entitle a user to a task.

It thus uniquely enables and empowers organizations to perform mission-critical assessments that are paramount for accurately controlling privileged access and maintaining cyber security.

1. Installation

Gold Finger can be installed on any computer running a Windows operating system.

To install Gold Finger, please download the Gold Finger installer from your custom download page, unzip it, verify that its digital signature is valid, and then proceed to install Gold Finger.

Once you have installed Gold Finger, please download your custom Gold Finger license from your custom download page, unzip it and install your custom Gold Finger license by following the installation instructions contained in the unzipped license package.

> Note: Gold Finger's use only requires that the computer on which it is installed have network access to the Active Directory environment in which you wish to use it, and that its user have standard domain-user credentials to be able to access and query Active Directory.

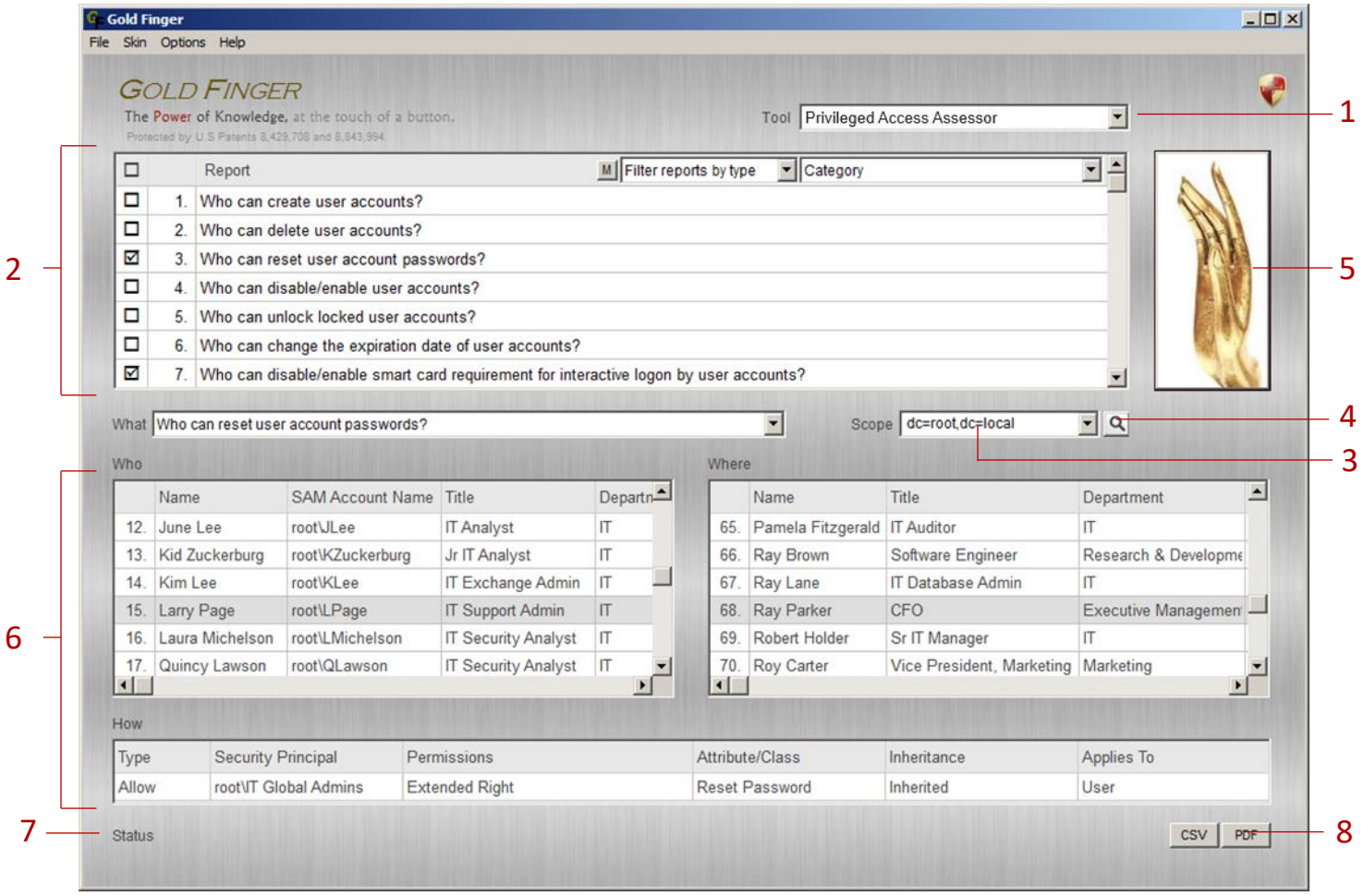
2. Getting Started

To begin, launch **Gold Finger**. To do so, click the *Start* menu, then locate the *Paramount Defenses* folder, and within it, select *Gold Finger* i.e. click on it to launch the application.

Gold Finger should be up and running in a few moments.

3. Becoming Familiar with Gold Finger's User-Interface

Gold Finger's sheer simplicity is reflected in its minimalist user-interface.



Gold Finger's user-interface is primarily comprised of 8 simple elements –

1. **Tool** Selector – The tool selector is used to select a specific tool
2. **Reports** pane – The reports pane lists all the reports available in a tool
3. **Scope** field – The scope field is used to specify the report's scope/target
4. **Search** utility – The inbuilt search utility is used to locate and specify targets
5. **Gold Finger** (**Run**) button – The *Gold Finger* button is used to generate a report
6. **Results** pane(s) – The results of a generated report are displayed in the results pane(s)
7. **Status** indicator – The status indicator provides an indication of the report's status
8. **CSV** and **PDF** buttons – The CSV and PDF buttons are used to export the report's results

4. Assessing Privileged Access Domain/OU-wide in Active Directory

Gold Finger can accurately, automatically and instantly assess privileged access provisioned on all (i.e. thousands of) objects in an Active Directory domain at the touch of a single button.

To assess privileged access in a specific Active Directory domain or organizational unit (OU) –

1. Use the Tool selector to select the **Active Directory Privileged Access Assessor** tool.

2. In the *Reports* pane, select the report(s) you wish to generate from amongst 100+ reports.

   Note: You can select multiple reports in the "Multiple" Reporting mode, which can be activated and deactivated by clicking the "S" ("Single") toggle button located in the *Reports* pane, to the immediate left of the "*Filter reports by type*" drop-down.

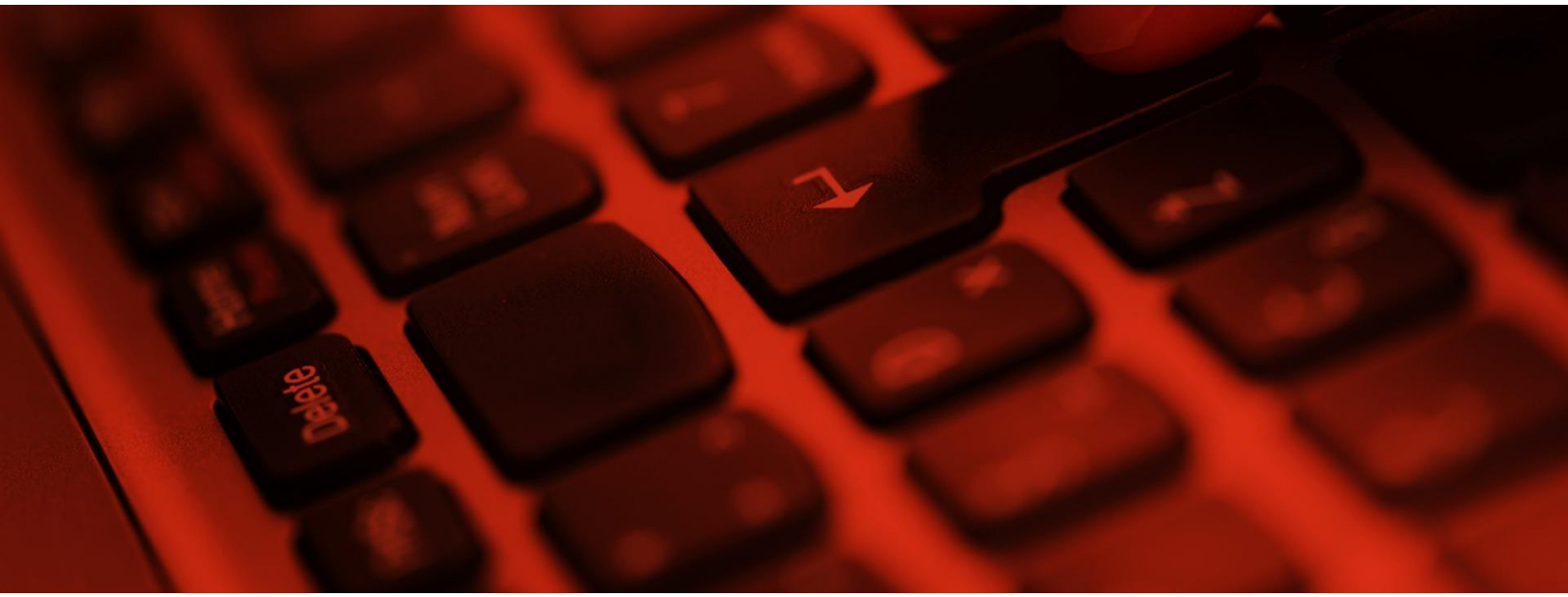
3. In the *Scope* field, enter the distinguished name (DN, e.g. *dc=example,dc=com*) of the Active Directory domain or OU you wish to assess privileged access in.

   Note: Gold Finger includes an inbuilt *Search* utility that is intended and designed to help you easily and quickly search for and locate Active Directory objects based on various criteria, and have their DNs be automatically determined and inserted into the Scope field.

4. Click the ***Gold Finger*** button.

5. Analyzing Active Directory Privileged Access Audit Results

Upon completion, the results of Gold Finger's privileged access assessment are displayed using four user-interface elements: the *What* drop-down, and the *Where*, *Who* and *How* panes.



The list of all administrative tasks that were selected for the domain/OU-wide privileged access assessment are listed in the *What* drop-down, located immediately below the *Reports* pane.

To analyze privileged access assessment results –

1. Select the administrative task you are interested in by locating it in the *What* drop-down.
2. When you do so, the list of all domain (user/computer) accounts that are entitled to i.e. who can perform that administrative task in the specified scope will be displayed in the *Who* pane.
3. To find out where a specific user can perform the selected administrative task, i.e. on which objects a user can perform the selected task, click on the user's name in the *Who* pane.
4. When you do so, Gold Finger will display the list of all objects in the specified scope on which the selected user can perform the selected administrative task in the *Where* pane.
5. To find out how a specific user is entitled to performing the selected administrative task on a specific object i.e. which security permission in that specific object's ACL is entitling a specific user to the selected task, click on the target object's name in the *Where* pane.
6. When you do so, Gold Finger will display the entitling security permission in the *How* pane.

6. Exporting Results and Generating PDF Reports

To export the results of Gold Finger's privileged access assessment, click the ***CSV*** button, specify a location for the output CSV file and click OK. To generate a (customizable via *PDF Options*) PDF report, simply click the ***PDF*** button, specify a location for the output PDF file and click OK.

7. Using Inbuilt Search

Gold Finger features an inbuilt search utility to help easily locate Active Directory objects, and have their distinguished names be automatically determined and inserted into the *Scope* field.

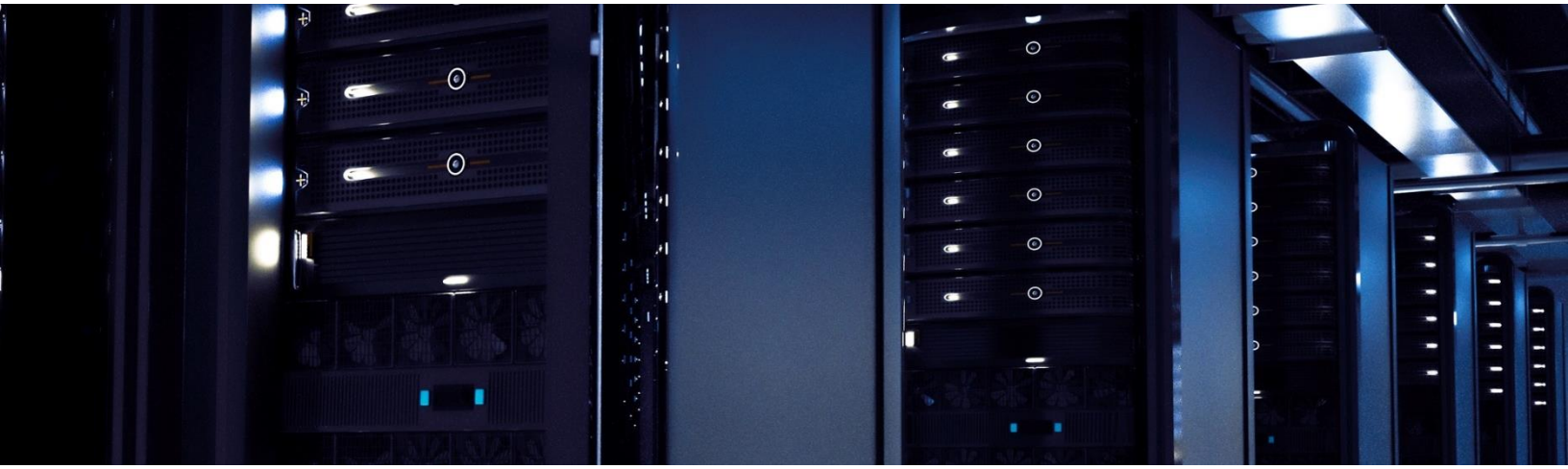
To use the inbuilt search utility to locate Active Directory objects, simply –

1. Launch search by clicking the ***Search*** button, which is located to the right of the *Scope* field.
2. Select (1) the domain you wish to search for, (2) the object type you wish to search for, (3) the search criteria you wish to use, and (4) the criteria value, then click the *Search* button.

   Note: Wildcards (*) can be used in the search criteria. To search the Configuration or Schema partitions, in (1) select the forest root domain, then change the target partition option from D (domain) to C (Configuration) or S (Schema) as required.
3. The search utility will then display all the Active Directory objects that meet the specified search criteria. To select a specific object, simply select it by clicking on it, then click OK.
4. Gold Finger will automatically return to its main window and the *Scope* field will now be populated with the distinguished name (DN) of the selected Active Directory object.

8. Using Basic Options

Gold Finger offers options to target specific domain controllers and use alternate credentials. To configure *Basic Options*, use the *Options* menu accessible via the application menu-bar.



The basic options available for all tools in Gold Finger include –

1. **Use Specified Domain Controller (DC)** – This option lets you target a specific DC. To use this option, you only need to enter the target DC's NetBIOS name (e.g. Corp-DC-1)

2. **Use Specified Alternate Credentials** – This option lets you specify alternate credentials. To use this option, the username entered must be in the form of a User Principal Name (UPN.)

Note: To use these options, you must also check the corresponding check-boxes.

9. Using Advanced Options

Gold Finger also offers advanced options to enhance performance and reduce assessment time. To configure *Advanced Options*, use the *Options* menu accessible via the application menu-bar.

The advanced options available for the *Active Directory Privileged Access Assessor* are –

1. **Use "Display Name" for user accounts** – If this preference option is selected, Gold Finger will display the *Display Name* of domain user accounts in the *Name* field.

Using Advanced Options (continued)

2. **Include "System Container" contents** – If this optimization option is selected, Gold Finger will be able to calculate privileged access on objects residing in the *System* container.

3. **Include "Anonymous" in "Everyone"** – If this preference option is selected, Gold Finger will include the *Anonymous* well-known security principal when dynamically evaluating the membership of the *Everyone* well-known security principal.

4. **Include impact of object ownership** – If this preference option is selected, Gold Finger will include the impact of an object's owner having implicit *Modify permissions* on the object.

5. **Include impact of "Delete-Tree" permissions on deletion tasks** – If this optimization option is selected, when assessing privileged access, Gold Finger will include the impact of "Delete Tree" permissions on all target objects and all their ancestor objects up to the domain root.

6. **Exclude data processing for CSV output** – If this optimization option is selected, Gold Finger will skip processing data for CSV exports, thereby reducing the assessment time.

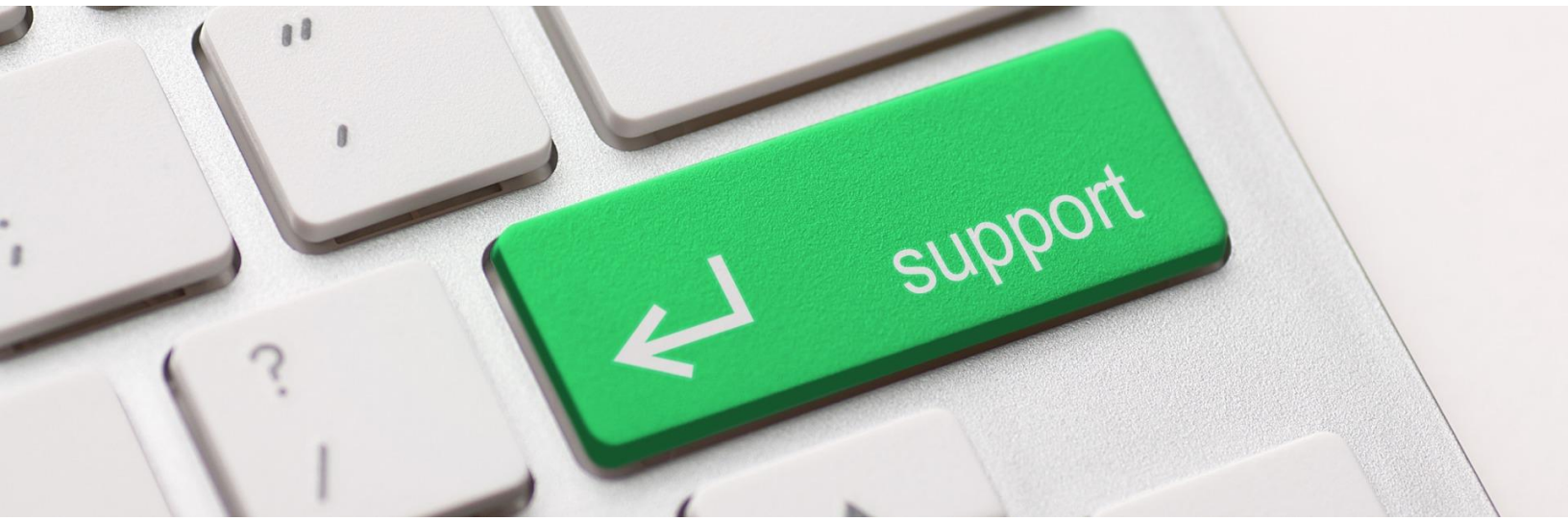
7. **Generate a separate CSV file for each report** - If this preference option is selected, when operating in the "Multiple Reports" mode, when the CSV button is clicked, the resulting CSV file will only contain privileged access results for the administrative task that is currently selected in the *What* drop-down. This enables the creation of a separate CSV file for each selected administrative task, thus distributing privileged access assessment results across multiple reasonably sized CSV files, with a separate file for each administrative task.

10. Obtaining Technical Support

Should you require technical support or assistance, please begin by visiting our website.

Solutions to commonly encountered issues and an FAQ are also available on our website.

To request support, please visit www.paramountdefenses.com/resources/support



Copyright Notice

Should you have any questions about the use of this guide, please contact us at –

Paramount Defenses, 620 Newport Center Dr., Suite 1100, Newport Beach, CA 92660. USA.


PD