Gold Finger

Active Directory Effective Access Auditor

User's Guide

Copyright 2006 – 2024 Paramount Defenses Inc. All rights reserved. Paramount Defenses and Gold Finger are trademarks or registered trademarks of Paramount Defenses Inc. Microsoft, Windows, Windows Server, Entra and Active Directory are the trademarks of Microsoft Corporation.

Gold Finger

Active Directory Effective Access Auditor

Contents

Active Directory Effective Access Auditor

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 many security permissions in the ACL of every Active Directory object, granted to various users and groups, and it is the net resulting cumulative i.e. effective permissions that actually govern exactly who has what effective access on each object, and thus govern who can enact what privileged/administrative tasks on Active Directory objects.

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 audit effective access on Active Directory objects.

The *Active Directory Effective Access Auditor* is unique in its ability to be able to accurately and automatically audit effective access in terms of administrative tasks in Active Directory. It can –

- ✓ Accurately audit effective access on any object in an Active Directory domain
- ✓ Audit effective access in terms of administrative tasks entitled on Active Directory objects
- ✓ Identify the underlying permissions that entitle a user to a specific administrative task

It thus uniquely enables and empowers organizations to easily perform critical audits that are required to accurately assess and lockdown privileged access and to maintain 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.

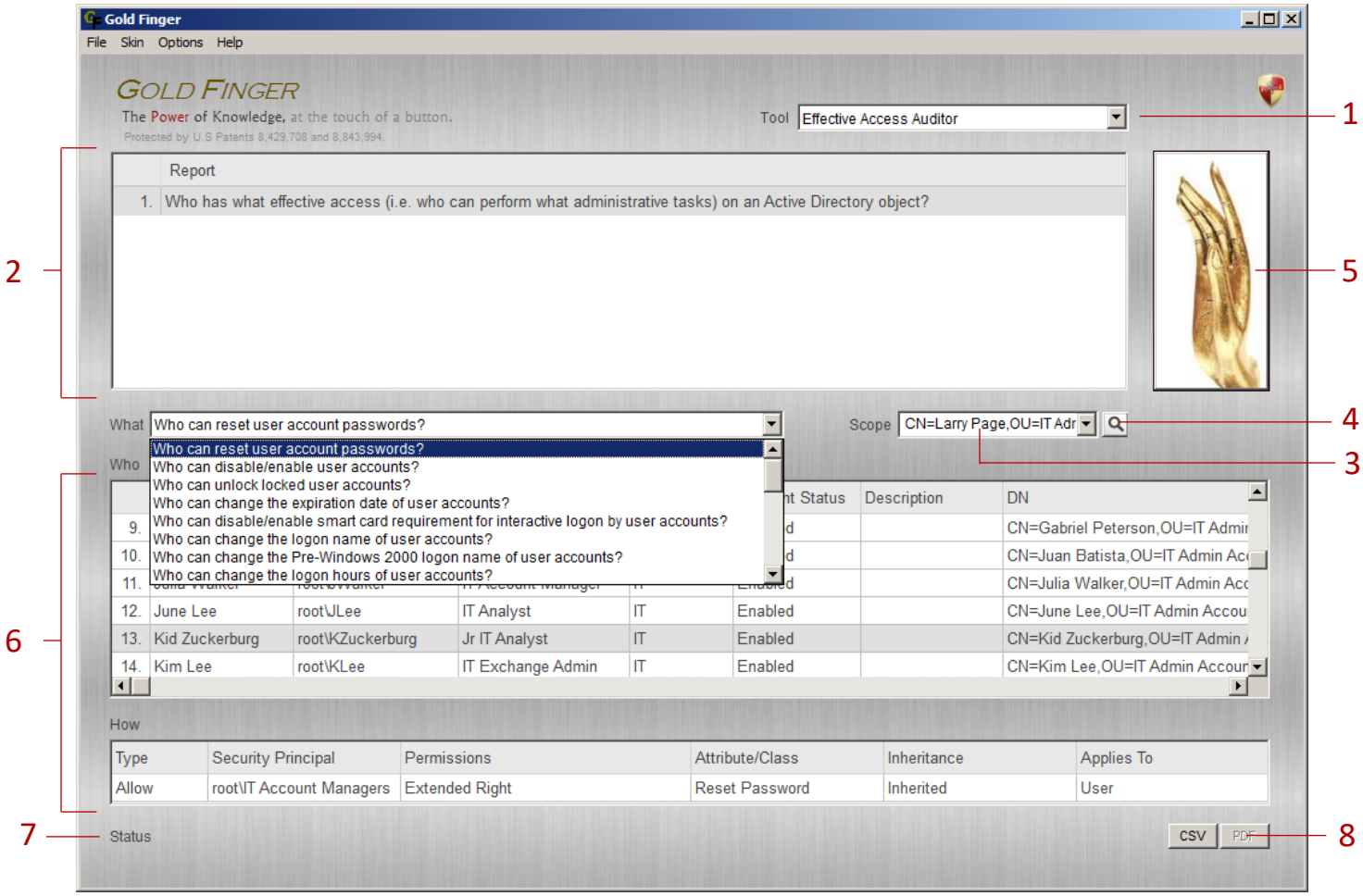
2. Getting Started

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. Auditing Active Directory Effective Access

Gold Finger can accurately, automatically and instantly audit effective access provisioned on any Active Directory object, in terms of administrative tasks, in any Active Directory domain.

To audit effective access on a specific Active Directory object, simply –

1. Use the Tool selector to select the **Active Directory Effective Access Auditor** tool.

2. In the *Reports* pane, select the report –

   Who has what effective access (i.e. who can perform what administrative tasks) on an Active Directory object?

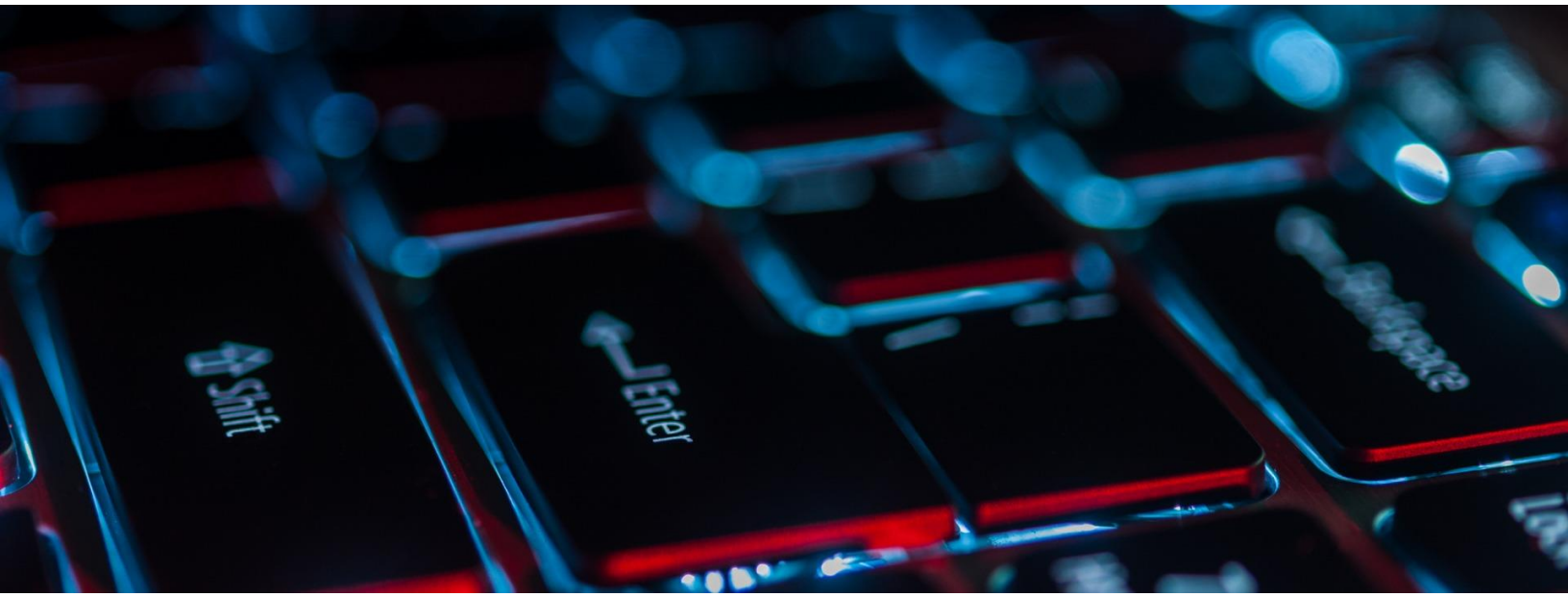
3. In the *Scope* field, enter the distinguished name (DN, e.g. *cn=domain admins,cn=users, dc=example,dc=com*) of the Active Directory object you wish to audit effective access on.

   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 Effective Access Audit Results

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



The list of all administrative tasks that are effectively entitled on the specified object are listed in the *What* drop-down, which is located immediately below the *Reports* pane.

To analyze effective access audit 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 on the target object will be displayed in the *Who* pane.
3. To find out how a specific user is entitled to performing the selected administrative task on the target object i.e. which security permission in the specified object's ACL is entitling a specific user to the selected task, locate and click on the user's name in the *Who* pane.
4. When you do so, Gold Finger will display the entitling security permission in the *How* pane.

> Note: Knowing exactly which security permission in the object's ACL is responsible for entitling a specific user to perform a specific administrative task is extremely valuable because it lets you lock down all identified excessive/unauthorized access.

6. Exporting Results

To export the results of Gold Finger's effective access audit, simply click the ***CSV*** button, specify a location for the output CSV 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.

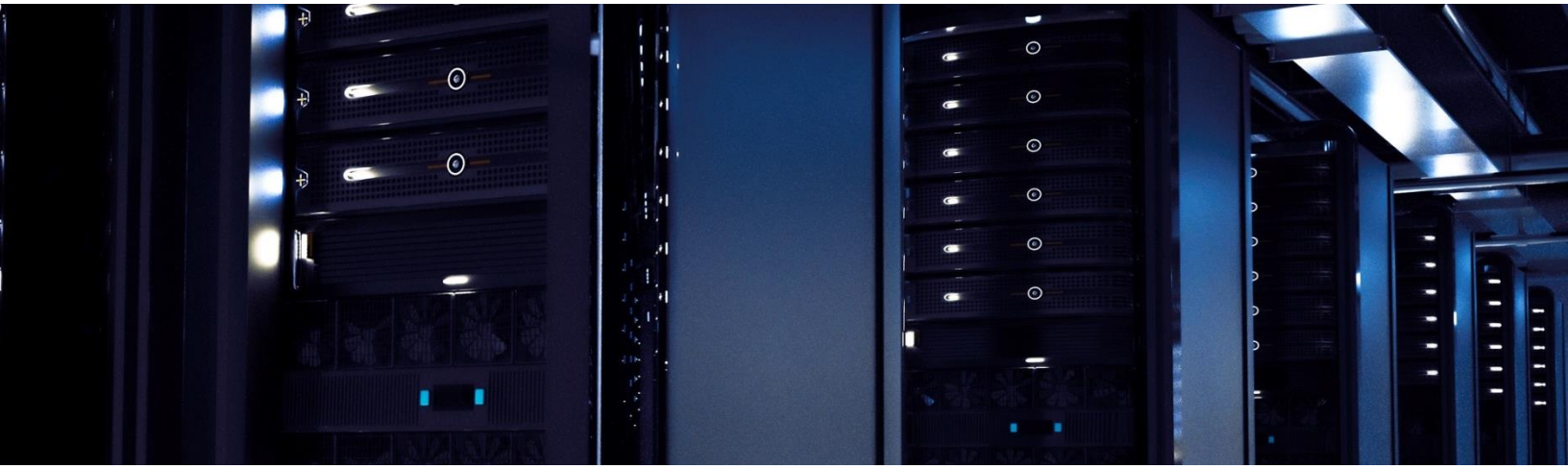
To use the inbuilt search utility to locate Active Directory objects, simply –

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 Effective Access Auditor* 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 effective 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 auditing effective access, Gold Finger will include the impact of "Delete Tree" permissions on the target object and on all 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.

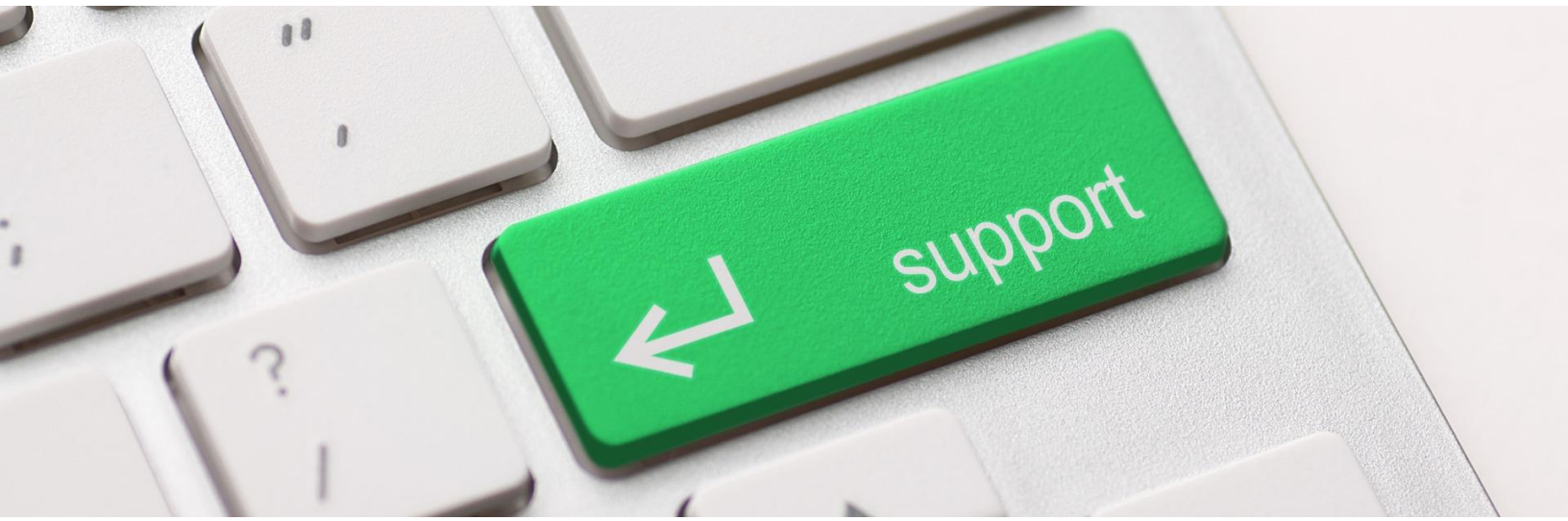
7. **Exclude assessment of deletion tasks** - If this optimization option is selected, Gold Finger will skip evaluating who can delete the specified target object, considerably reducing assessment time. If you are not primarily interested in determining who can delete the specified target object, unchecking this option will considerably reduce assessment time.

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

This document contains proprietary information protected by copyright. The software referred to in this document is furnished to you under a software license, and it may only be used in accordance with the terms of use specified in its End-user License Agreement (EULA.)

No part of this document may be reproduced or transmitted in any form or by any means, for any other purpose other than for your organizational use in accordance with the software's EULA, without the express written permission of Paramount Defenses Inc.

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