Gold Finger

Active Directory Permissions Analyzer

User's Guide

Gold Finger

Active Directory Permissions Analyzer

Contents

Active Directory Permissions Analyzer

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 thousands of security permissions in Active Directory, which may have been provisioned over years, and granted to various users and groups, and they effectively govern exactly who has what privileged access in Active Directory.

To maintain security and fulfill GRC driven audit needs, at a minimum, organizations need to be able to easily and reliably audit who has what permissions in their Active Directory.

The *Active Directory Permissions Analyzer* can instantly, precisely and automatically analyze thousands of permissions specified inside Active Directory to help organizations accurately, efficiently and easily audit permissions domain-wide in Active Directory. It can –

- ✓ Uncover who has what permissions where in Active Directory
- ✓ Identify what permissions a specific user or group has in Active Directory
- ✓ Determine which users or groups have a specific permission in Active Directory

It thus enables organizations to easily perform these important permissions audits which are required to assess and lockdown access and 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.

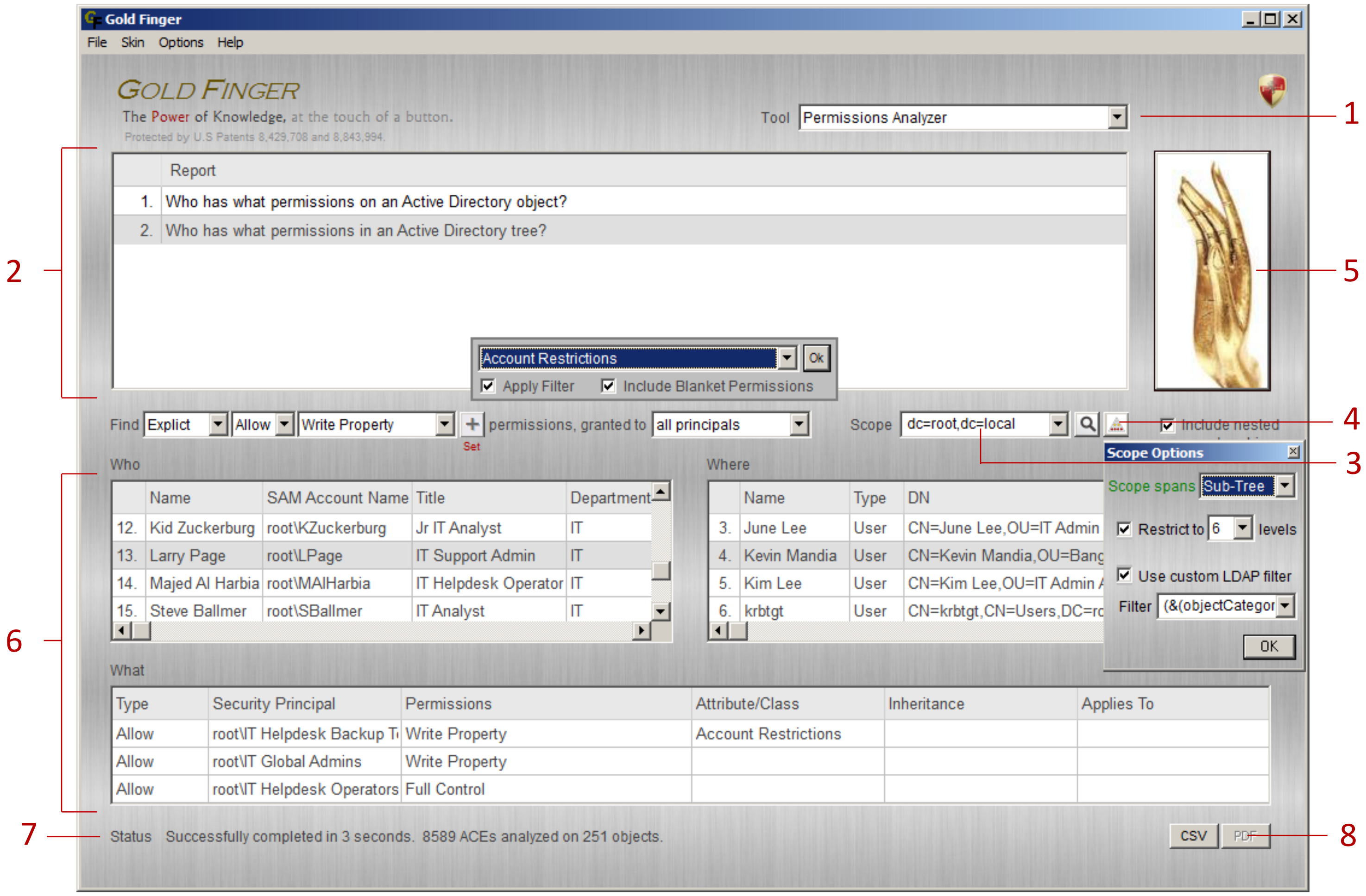
2. Getting Started

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
File Skin Options Help
GOLD FINGER
The Power of Knowledge, at the touch of a button.
Protected by U.S Patents 8,429,708 and 8,843,994.
1
2
3
4
5
6
7
8
Set
CSV
PDF
OK
Ok

Tool: Permissions Analyzer

	Report
1.	Who has what permissions on an Active Directory object?
2.	Who has what permissions in an Active Directory tree?

Account Restrictions
☑ Apply Filter ☑ Include Blanket Permissions

Find Explict Allow Write Property permissions, granted to all principals

Scope dc=root,dc=local ☑ Include nested

Scope Options
Scope spans Sub-Tree
☑ Restrict to 6 levels
☑ Use custom LDAP filter
Filter (&(objectCategor

Who

	Name	SAM Account Name	Title	Department
12.	Kid Zuckerburg	root\KZuckerburg	Jr IT Analyst	IT
13.	Larry Page	root\LPage	IT Support Admin	IT
14.	Majed Al Harbia	root\MAlHarbia	IT Helpdesk Operator	IT
15.	Steve Ballmer	root\SBallmer	IT Analyst	IT

Where

	Name	Type	DN
3.	June Lee	User	CN=June Lee,OU=IT Admin
4.	Kevin Mandia	User	CN=Kevin Mandia,OU=Bang
5.	Kim Lee	User	CN=Kim Lee,OU=IT Admin /
6.	krbtgt	User	CN=krbtgt,CN=Users,DC=ro

What

Type	Security Principal	Permissions	Attribute/Class	Inheritance	Applies To
Allow	root\IT Helpdesk Backup Te	Write Property	Account Restrictions		
Allow	root\IT Global Admins	Write Property			
Allow	root\IT Helpdesk Operators	Full Control			

Status Successfully completed in 3 seconds. 8589 ACEs analyzed on 251 objects.

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. Analyzing Security Permissions in an Active Directory Domain

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

To audit security permissions in a specific Active Directory domain or organizational unit (OU) –

1. Use the Tool selector to select the **Active Directory Permissions Analyzer** tool*.*

2. In the *Reports* pane, select the report *Who has what permissions in an Active Directory tree?*

3. In the *Scope* field, enter the distinguished name (DN, e.g. *dc=example,dc=com*) of the Active Directory domain or Organizational Unit (OU) you wish to analyze security permissions in.

   Note: Gold Finger includes an inbuilt *Search* utility to help 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. Specify your permissions analysis criteria by using options available below the *Reports* pane – Find *Explicit/Inherited*, *Allow/Deny*, *any*/a specific permission*, granted to *all principals/a specific principal* (specifiable by clicking *Principal* button), then click the ***Gold Finger*** button.

   * To specify a particular Schema element, such as a specific Schema class, attribute or extended right, click the **+** button. Before clicking on it the first time, please press Alt-**R** to have Gold Finger retrieve and load the Active Directory Schema.

5. Reviewing Active Directory Permissions Analysis Results

Upon completion, the results of Gold Finger's security permissions analysis are displayed using three user-interface elements: the *Who, Where* and *What* panes.

The list of all security principals who have the specified permissions in the specified domain/OU are listed in the *Who* pane.

To analyze permissions analysis results –

1. Begin by reviewing the list of individuals in the *Who* pane. To find out where (i.e. on which Active Directory objects) a specific user has the specified permissions, click on their name.
2. When you do so, the list of all Active Directory objects in whose access control list (ACL) that user has the specified permissions will be displayed in the *Where* pane.
3. Next, to view the exact security permissions that exist in the ACL of a specific object listed in the *Where* pane, simply click on that object.
4. When you do so, Gold Finger will display all security permissions that exist in that specific object's ACL that meet the specified permissions analysis criteria, in the *What* pane.

> Note: You can pivot the entire results by *Who*, *Where* or *What* by exporting the results to a CSV file, and opening the CSV file in any spreadsheet application.

6. Exporting Results

To export the results of Gold Finger's security permissions analysis, after the results have been displayed, 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 –

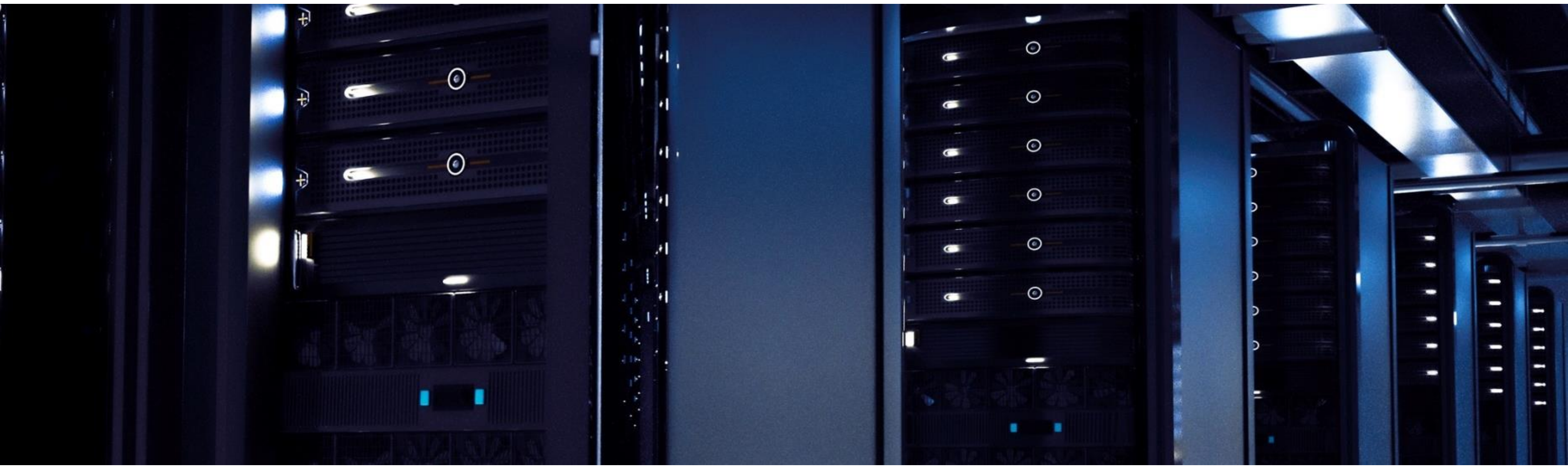
1. Launch search by clicking the ***Search*** button, which is located to the right of the *Scope* field.
2. Select (1) the domain you wish to search for, (2) the object type you wish to search for, (3) the search criteria you wish to use, and (4) the criteria value, then click the *Search* button.

   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 Permissions Analyzer* 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 analyze security permissions 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. **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.

10. Using Custom LDAP Filters

Gold Finger lets you customize the scope of permissions analysis using a custom LDAP filter.

To apply a custom LDAP filter, use the *Scope Options* dialog which can be accessed by clicking the *Scope Options* button, which is located to the immediate right of the *Search* button.

To apply a custom LDAP filter, simply check the *Use Custom LDAP Filter* check-box and enter a custom LDAP filter in the LDAP filter box. For example, to have Gold Finger only analyze ACLs of domain user accounts, enter the LDAP filter *(&(objectCategory=person)(objectClass=user))*.

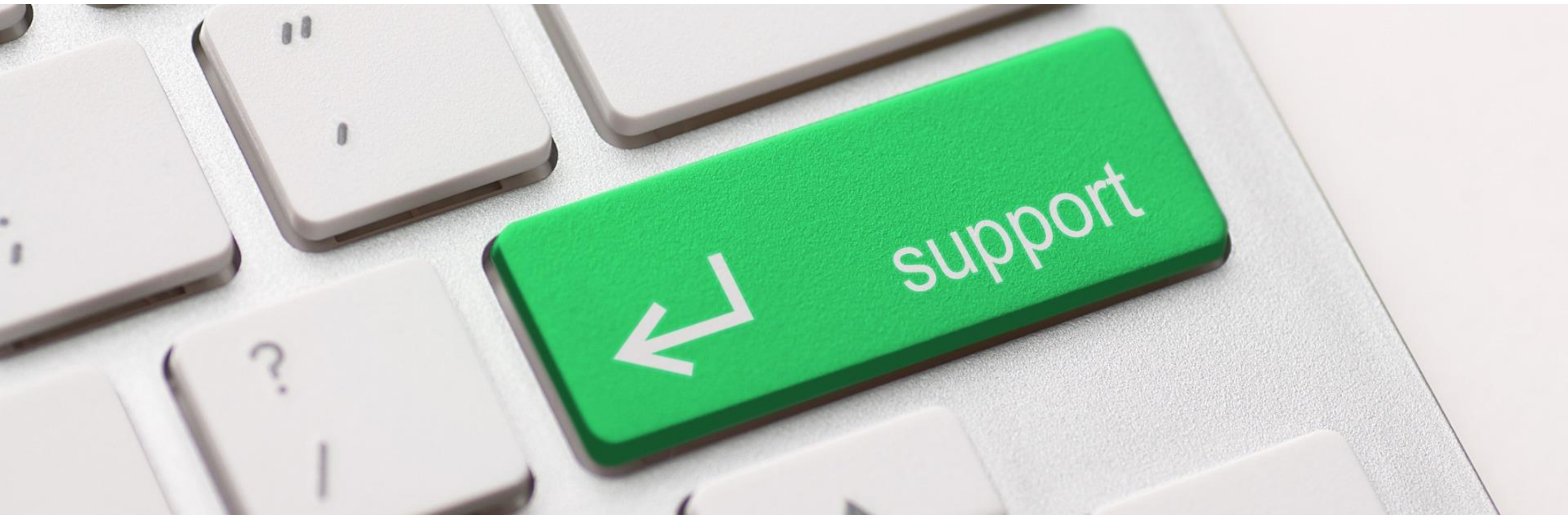
You can specify any LDAP filter of your choice to have the permissions analysis be restricted to only those Active Directory objects that meet the criteria specified by your custom LDAP filter.

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.

www.paramountdefenses.com