Gold Finger

Active Directory ACL Analyzer

User's Guide

Gold Finger

Active Directory ACL Analyzer

Contents

Active Directory ACL 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 many security permissions in the ACL of every Active Directory object, granted to various users and groups, most of which may have been provisioned over years. In addition, SACLs of Active Directory objects govern what is audited in Active Directory.

To maintain security, provision access, perform cleanups, and fulfill GRC driven audit needs, organizations need to be able to analyze and lockdown Active Directory ACLs and SACLs.

The *Active Directory ACL Analyzer* lets organizational IT personnel easily view, analyze and audit the ACL and SACL of any Active Directory object in full detail. It can –

- ✓ Deliver a complete, sortable view of any Active Directory object's ACL and SACL
- ✓ Clearly identify exactly which users and groups have what permissions in the ACL
- ✓ Export the ACL and SACL of any Active Directory object, at the touch of a button

It thus enables organizations to easily perform Active Directory ACL and SACL audits which are needed to assess and lockdown access, perform cleanups 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.

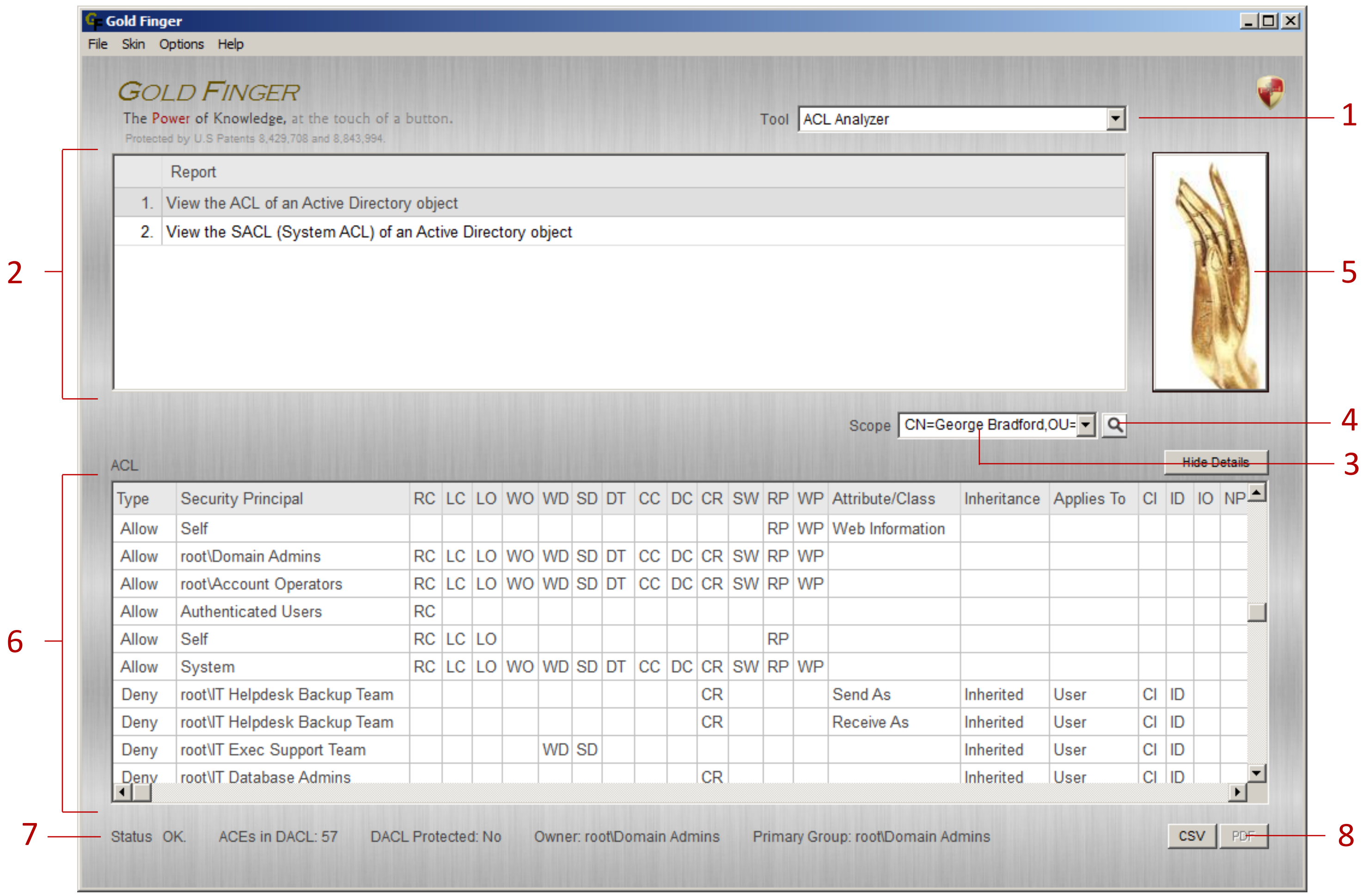
2. Getting Started

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'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. Viewing Active Directory ACLs

Gold Finger can accurately, automatically and instantly retrieve and display the complete access control list (ACL) of any Active Directory object in any Active Directory partition.

To view the ACL of a specific Active Directory object, simply –

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

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

   View the ACL of an Active Directory object

3. In the *Scope* field, enter the distinguished name (DN, e.g. *cn=users,dc=example,dc=com*) of the Active Directory object whose ACL you wish to view, analyze and/or export.

   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 ACLs

Upon completion, Gold Finger will retrieve and display a complete, fully sortable view of the ACL of the specified Active Directory object in the *ACL* pane.

By default Gold Finger will display a verbatim view of the specified Active Directory object's ACL.

To obtain a fully sortable detailed view of the object's ACL, click the ***View Details*** button. When you do, so Gold Finger will generate and display a fully sortable view of the ACL, splitting the permissions and inheritance fields into individually sortable columns, delivering full fidelity.

To analyze the displayed ACL in detailed view, you can –

1. Sort the ACL by any field by double-clicking the header of that field, located in the first row.
2. When you do so, the entire ACL will be sorted by that field. Successively double-clicking the header will reverse the sort order allowing you sort it by ascending or descending order.
3. To sort the ACL by a specific permission, such as Extended Rights, simply sort the ACL by the SDDL mnemonic of that permission i.e. CR for Extended Rights. (To learn more about SDDL mnemonics, you may wish to perform a web search for "Microsoft SDDL.")
4. When you do so, Gold Finger will sort the entire ACL by the selected individual permission making it easy to analyze the specified object's ACL and all specified security permissions.

6. Exporting Results

To export the displayed Active Directory ACL, 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.

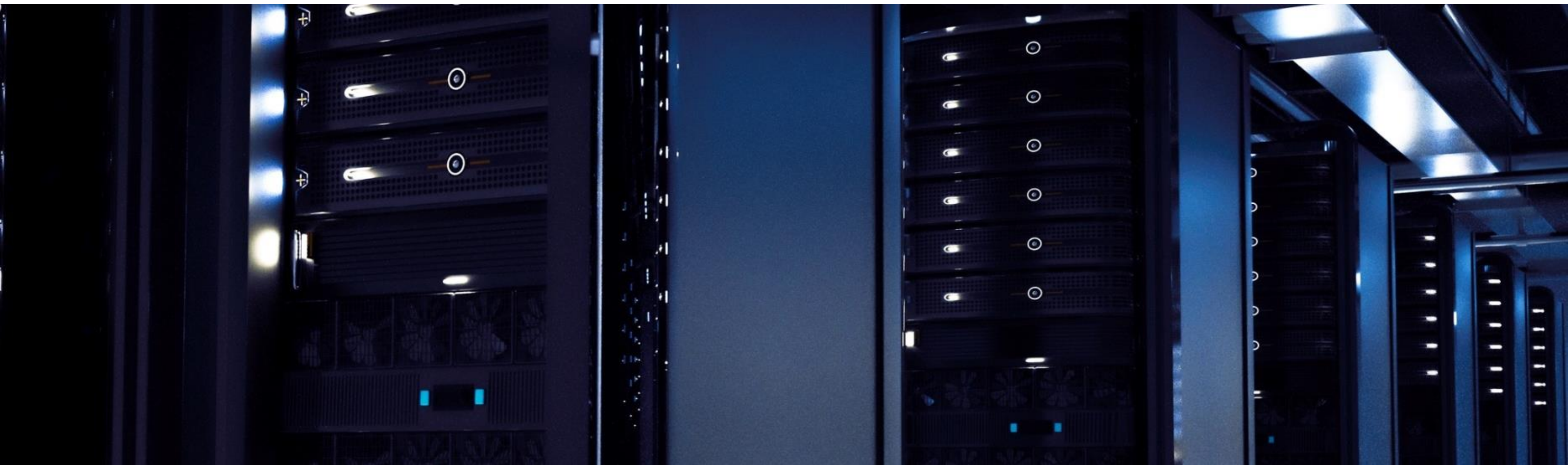
   Note: Wildcards (*) can be used in the search criteria. To search the Configuration or Schema partitions, in (1) select the forest root domain, then change the target partition option from D (domain) to C (Configuration) or S (Schema) as required.

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 ACL 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 retrieve the ACLs of Active Directory objects residing in the *System* container.

11. Viewing, Analyzing and Exporting Active Directory SACLs

Gold Finger can also accurately, automatically and instantly retrieve and display the complete SACL of any Active Directory object in any Active Directory partition. An object's SACL controls what is audited when *Directory Services* auditing is enabled on Domain Controllers.

The process for viewing, analyzing and exporting the SACL of an Active Directory object is virtually identical to the process of doing so for an Active Directory ACL. To do so –

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

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

   View the SACL of an Active Directory object

3. In the *Scope* field, enter the distinguished name (DN, e.g. *cn=users,dc=example,dc=com*) of the Active Directory object whose SACL you wish to view, analyze and/or export.

4. Click the *Gold Finger* button.

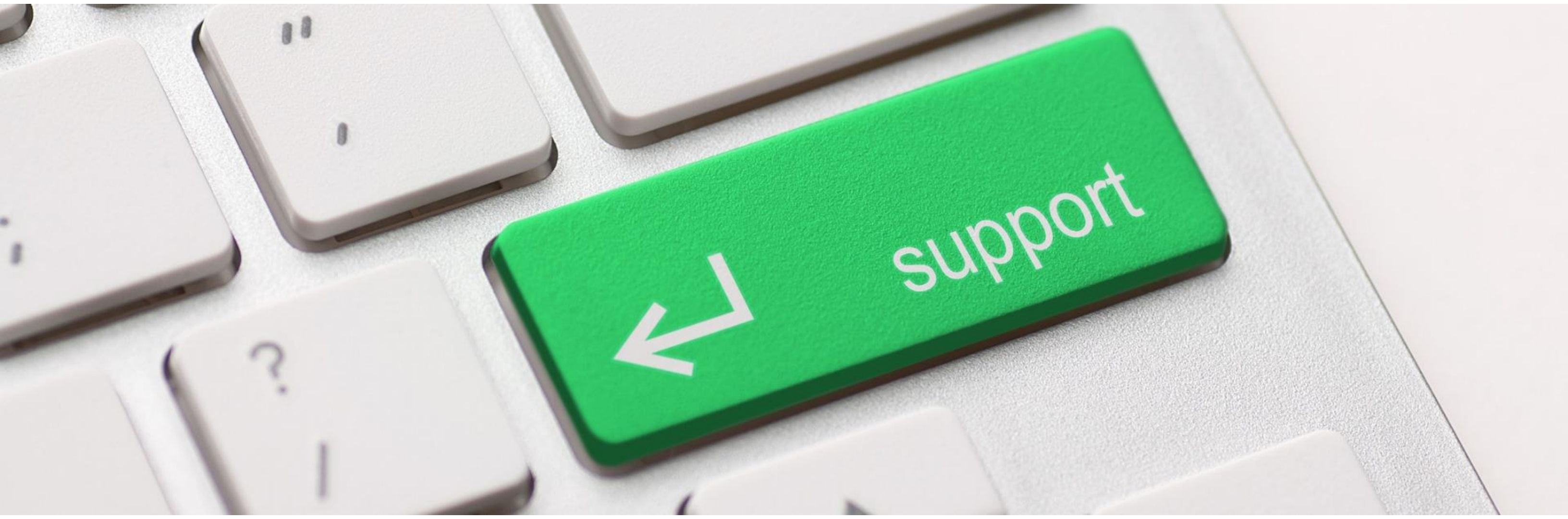
When Gold Finger displays the SACL of the specified object, one can proceed to analyze and export the SACL in the same fashion as one would utilize for analyzing and exporting ACLs.

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.