

# *Gold Finger*

*Active Directory ACL Exporter*



## User's Guide



# Gold Finger

## Active Directory ACL Exporter

### Contents

Introduction .....	1
1. Installation .....	2
2. Getting Started .....	2
3. Becoming Familiar with Gold Finger's User-Interface .....	3
4. Exporting Active Directory ACLs .....	4
5. Exporting Active Directory SACLs .....	5
6. Customizing Scope with LDAP Filters .....	6
7. Using Inbuilt Search .....	6
8. Using Basic Options .....	7
9. Using Advanced Options .....	7
10. Using Special Export Options .....	8
11. Obtaining Technical Support .....	9

# Active Directory ACL Exporter



## 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 access in Active Directory. In addition, there also exist thousands of audit settings in SACLs that govern exactly 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 Exporter* lets organizational IT personnel easily export, analyze and audit ACLs and SACLs of all Active Directory objects domain-wide in full detail. It can –

- ✓ Deliver a complete, sortable view of all Active Directory ACLs and SACLs domain-wide
- ✓ Clearly identify exactly which users and groups have what permissions domain-wide
- ✓ Export the ACLs and SACLs of all Active Directory objects, 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.





# Active Directory ACL Exporter



## 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.

A close-up photograph of the word 'START' painted in white, bold, capital letters on a dark asphalt surface. A yellow rectangular marker is visible above and below the word.

## 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.

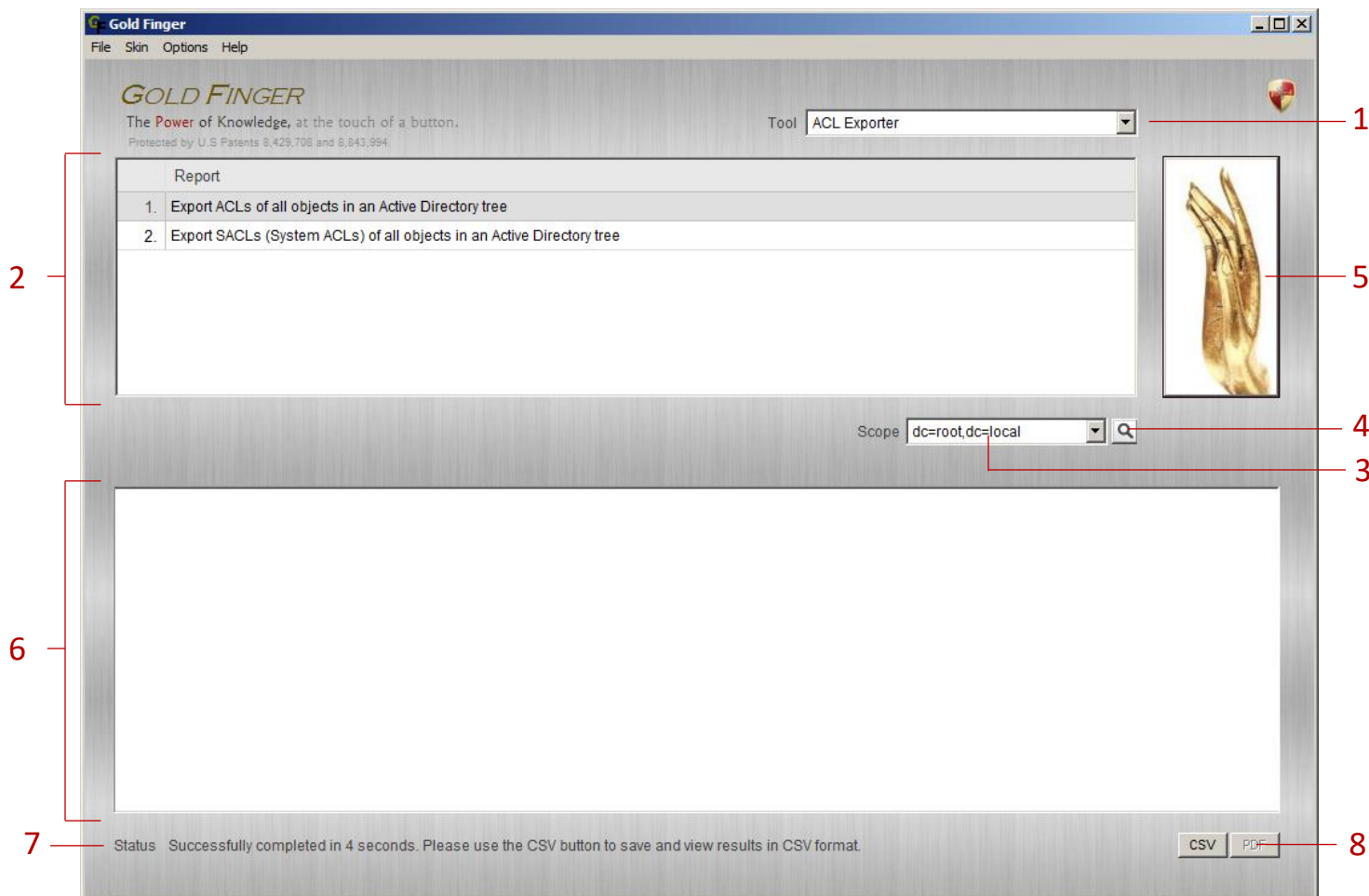
Gold Finger should be up and running in a few moments.

# Active Directory ACL Exporter



## 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. Exporting Active Directory ACLs

Gold Finger can accurately, automatically and instantly export the access control lists (ACLs) of all Active Directory objects in any Active Directory tree (partition, domain, OU or container).



To export the ACLs of all Active Directory objects in an Active Directory tree –

1. Use the Tool selector to select the **Active Directory ACL Exporter** tool.
2. In the *Reports* pane, select the report –  
*Export ACLs of all objects in an Active Directory tree*
3. In the *Scope* field, enter the distinguished name (DN, e.g. *ou=corp,dc=example,dc=com*) of the root object of the Active Directory tree you wish to export the ACLs of.

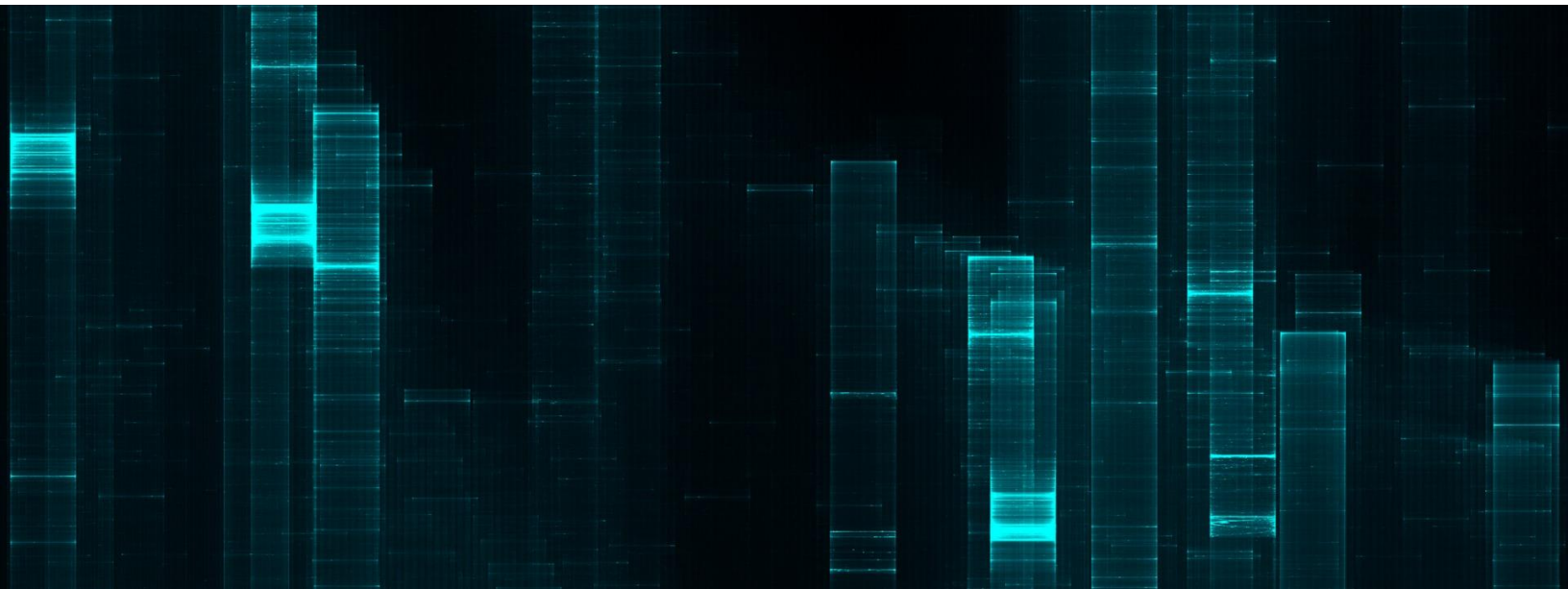
Note: Gold Finger includes an inbuilt *Search* utility that is intended and designed to help you easily and quickly search for and locate Active Directory objects based on various criteria, and have their DNs be automatically determined and inserted into the *Scope* field.

4. Click the **Gold Finger** button, and wait for Gold Finger to complete retrieving the ACLs.
5. Then, after the status bar indicates success, click the **CSV button** to complete the ACL export.



## 4. Exporting Active Directory SACLs

Gold Finger can also accurately, automatically and instantly export the SACLs of all Active Directory objects in any Active Directory tree (partition, domain, OU or container).



To export the SACLs of all Active Directory objects in an Active Directory tree –

1. Use the Tool selector to select the **Active Directory ACL Exporter** tool.
2. In the *Reports* pane, select the report –  
*Export SACLs (System ACLs) of all objects in an Active Directory tree*
3. In the *Scope* field, enter the distinguished name (DN, e.g. *ou=corp,dc=example,dc=com*) of the root object of the Active Directory tree you wish to export the SACLs of.

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, and wait for Gold Finger to complete retrieving the SACLs.
5. After the status bar indicates success, click the **CSV button** to complete the SACL export.





## 6. Customizing Scope with LDAP Filters

You can customize the scope of the ACLs/SACLs being exported by specifying an LDAP filter. To do so, click the *LDAP filter* button, which is located to the immediate right of the *Search* button.

## 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.

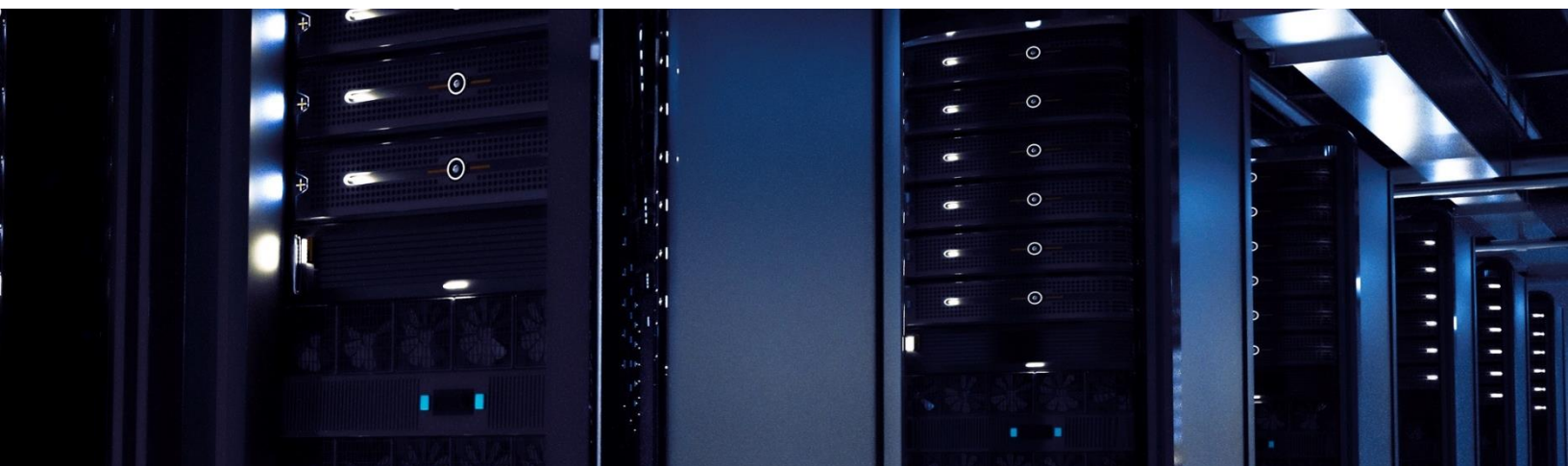
3. The search utility will then display all the Active Directory objects that meet the specified search criteria. To select a specific object, simply select it by clicking on it, then click OK.
4. Gold Finger will automatically return to its main window and the *Scope* field will now be populated with 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 Exporter* 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 ACLs of all Active Directory objects residing in the *System* container.

## 11. Using Special Export Options

Gold Finger offer three special export options that can additionally be used to export the ACLs of all objects whose ACLs are marked *Protected*, owned by a specific User or Group, or that have a specific *Primary Group* specified.

Specifically, Gold Finger offers the following three additional options -

1. Export ACLs of all objects whose ACL is marked *Protected*
2. Export ACLs of all objects owned by a specific user or group
3. Export ACLs of all objects with a specific Primary Group

To use these special options, prior to generating an ACL/SACL export report, simply select the appropriate option using the *Options* dropdown, located immediately below the *Reports* pane.

When utilizing options that require specifying a security principal, a “*Specify Security Principal*” button is displayed to the immediate right of the *Options* dropdown. Clicking this button opens the *Search* dialog, which can be used to search, locate and specify the desired security principal.

# Active Directory ACL Analyzer

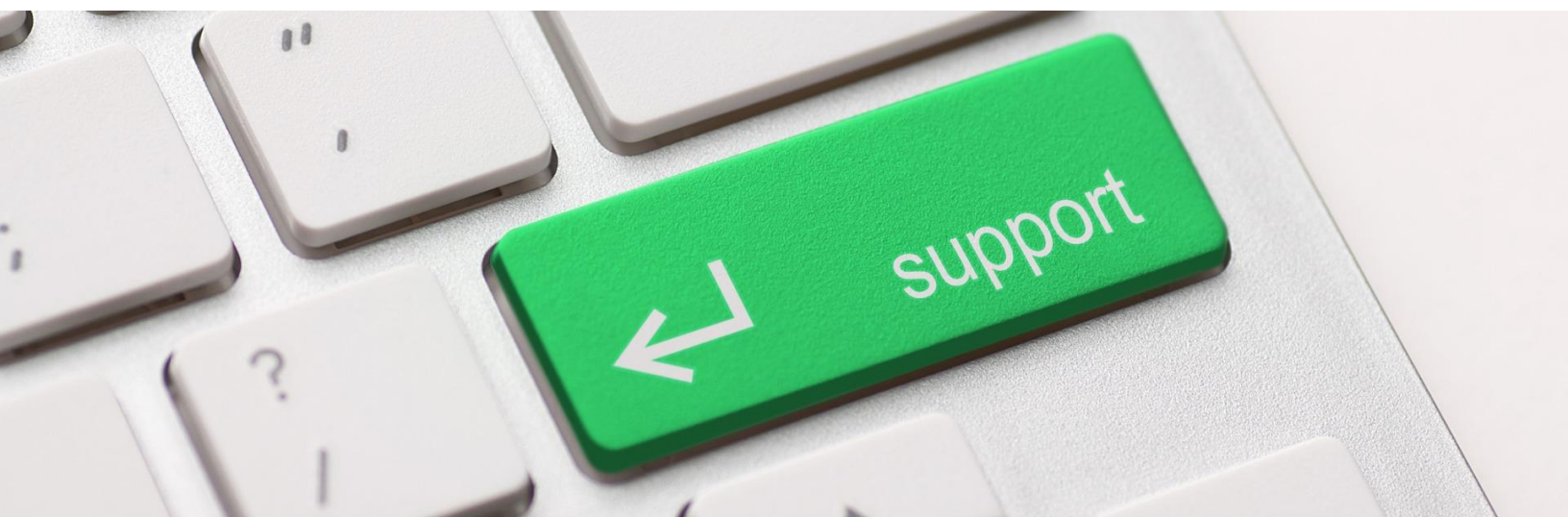


## 10. Obtaining Technical Support

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](http://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.

