Gold Finger

Active Directory Security Auditor

User's Guide

Gold Finger

Active Directory Security Auditor

Contents

Active Directory Security 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.

Since the entirety of an organization's identities (user accounts) are stored in Active Directory, Active Directory is the focal point of numerous basic security audits that involve assessing and maintaining the state of all the domain user accounts that represent these identities.

In addition, because Active Directory also stores all domain computer accounts, security groups, published printers, and various other objects such as service connection points, organizations periodically need to perform Active Directory inventories and clean-ups.

Thus, to ensure the basic security of all organizational identities (domain user accounts), maintain a secure and healthy Active Directory and fulfill various GRC driven audit needs, organizations need to be able to perform basic Active Directory security and inventory audits.

The *Active Directory Security Auditor* fully enables organizations to easily, efficiently and cost-effectively perform basic Active Directory security and inventory audits. It can –

- ✓ Automatically inventory all Active Directory content.
- ✓ Generate numerous basic, customizable Audit Directory security audit reports that cover various essential reporting aspects of domain user account management, such as true last logon reports as well as various domain user account state and status reports.

It thus enables organizations to easily perform basic yet essential Active Directory security and inventory audits needed to maintain security and fulfill audit and compliance needs.

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.

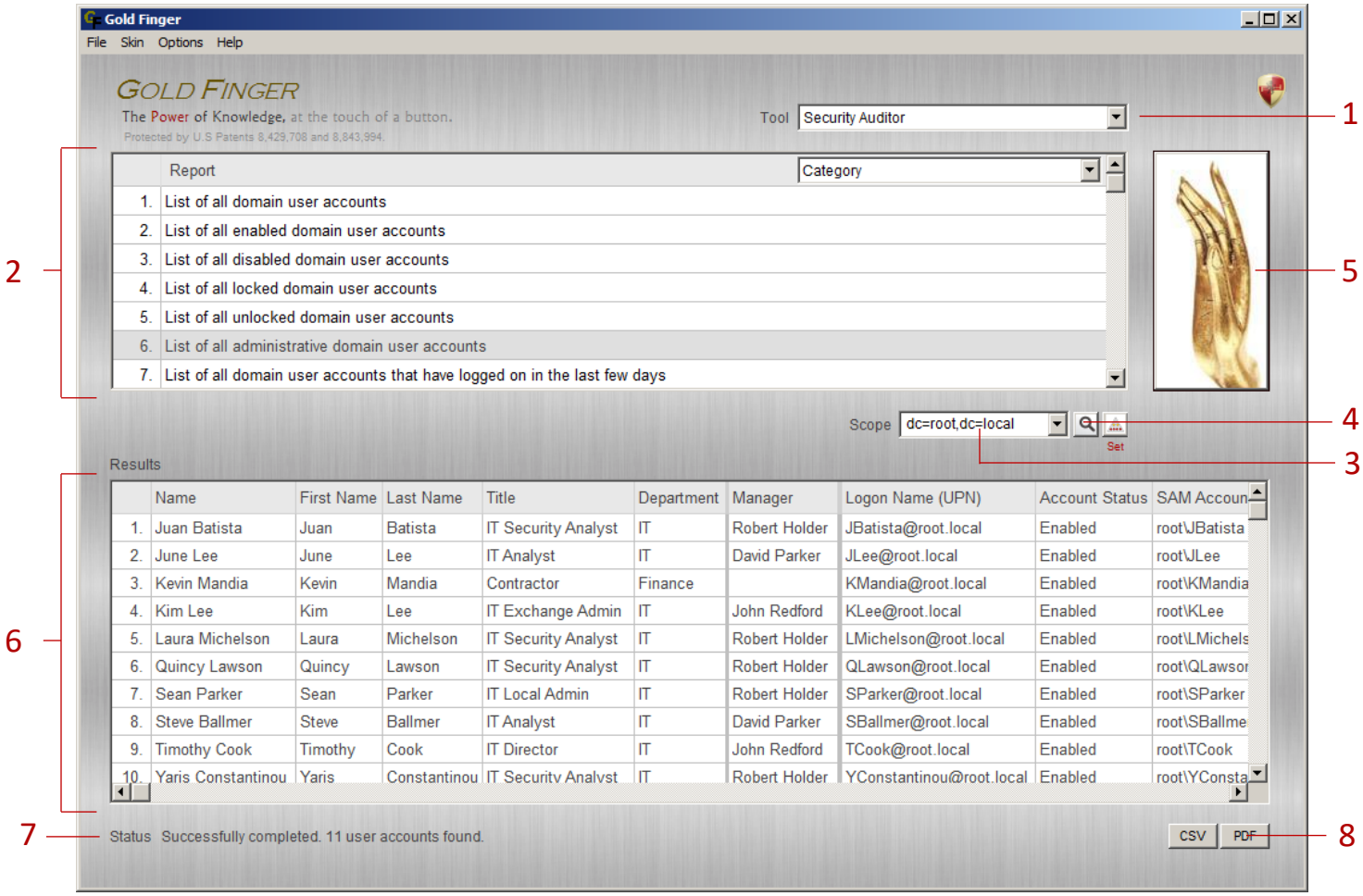
2. Getting Started

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. Generating an Active Directory Inventory / Security Audit Report

Gold Finger can accurately, automatically and instantly generate over 100 fully customizable Active Directory inventory / security audit reports at the touch of a button.

To generate an Active Directory inventory / security audit report, simply –

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

2. In the *Reports* pane, locate and select the inventory/audit report you wish to generate.

   Note: Based on the report, a *Number of Days* drop-down may appear for use.

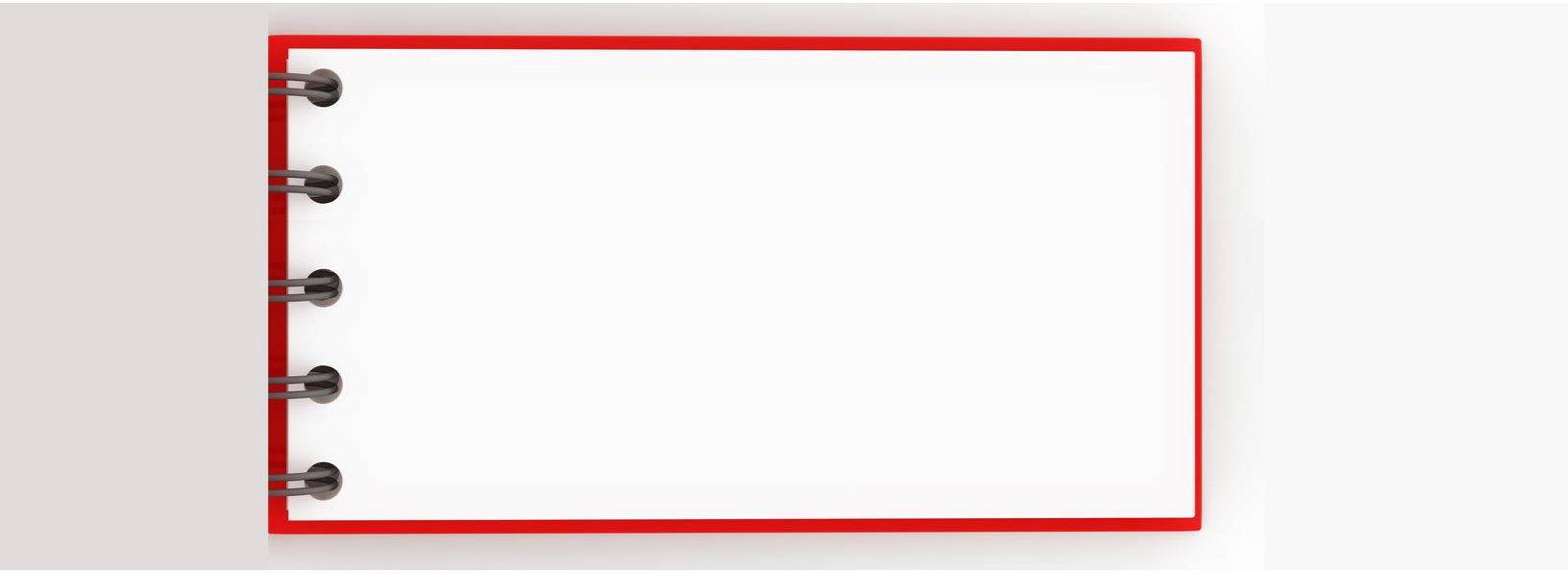
3. In the *Scope* field, enter the distinguished name (DN, e.g. *dc=example,dc=com*) of the Active Directory domain/organizational unit (OU) that you wish to inventory/audit.

   Note: Gold Finger includes an inbuilt *Search* utility to help easily 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. Gold Finger will instantly and automatically generate the requested audit report, and upon completion, display the results in the *Results* pane.

5. Generating Customizable Professional-Grade PDF Reports

Gold Finger can automatically generate fully-customizable professional-grade PDF reports that are well suited for furnishing evidence to fulfill various regulatory compliance and audit needs.



To generate a PDF report, simply click the ***PDF*** button after Gold Finger has displayed the results.

You can customize numerous elements of the PDF report, including its title, sub-title, description, footer, orientation, organizational logo, page numbers, password, and the fields to be included.

To customize PDF reports, use *PDF Report Options* via *Options* menu in the application menu-bar.

To customize the logo, which is automatically displayed on the top right-hand corner of the first page of the PDF report, simply rename your existing logo image (TIFF, BMP, PNG, JPG) to *logo*, ensure that it is less than 175 x 175 pixels, drop it in the *logo* sub-directory of the Gold Finger installation directory, and in the *PDF Report Options* dialog, check the *Display Logo* check-box.

The quickest way to access the Gold Finger installation directory is to press Alt-**I** in Gold Finger.

To generate a simple *Summary* report, one that only includes a simple listing of the generated results, simply uncheck the *Include Result Details in Reports* option in the *PDF Report options*.

6. Exporting Results

To export the results of a generated report, 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.

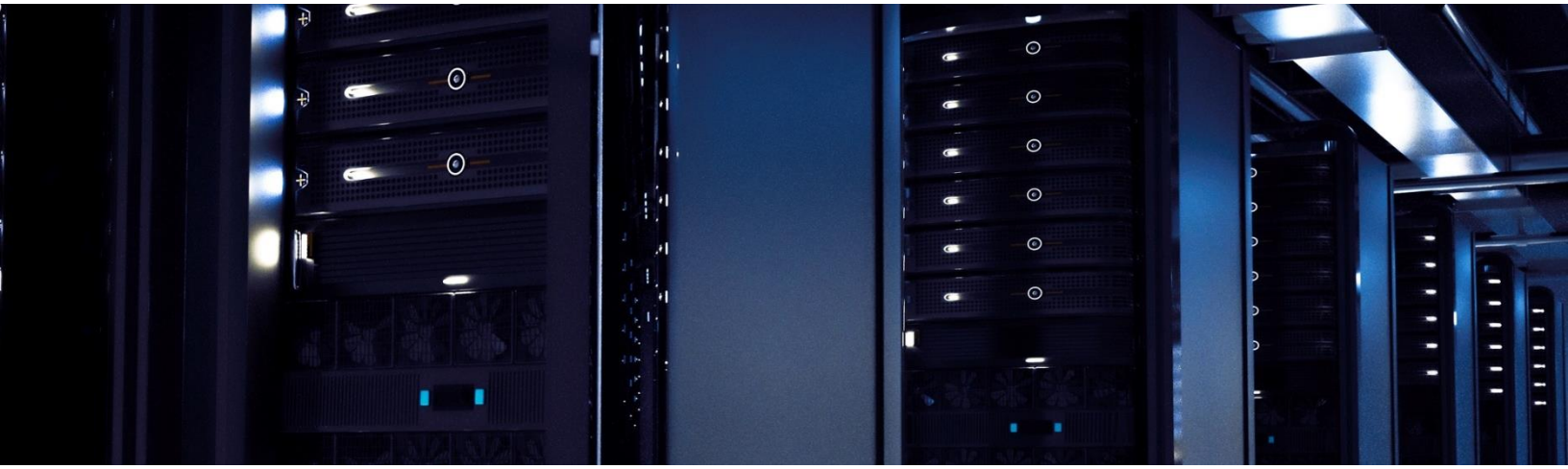
To use the inbuilt search utility to locate Active Directory objects, simply –

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 Security 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. **Use Last-Logon-Timestamp attribute in lieu of Last-Logon** – If this preference option is selected, in lieu of generating True Last-Logon reports which involve retrieving the value of the *Last-Logon* (non-replicated) attribute from all domain controllers (DCs) in a domain, Gold Finger will only retrieve the *Last-Logon Timestamp* (*replicated*) attribute from a single DC. The retrieval of the *Last-Logon Timestamp* attribute from a single DC results in a substantially faster report generation time, although results may not always be accurate. This option is a good choice when the *Number of Days* value is large enough (e.g. *30 days*) that reliance on the *Last-Logon Timestamp* attribute would be adequately sufficient.

3. **Display time values in absolute format (yyyy-mm-dd hh:mm)** – If this preference option is selected, time values are displayed in absolute format (2024-09-01 09:00 hrs), which has the benefit of enabling results to be alphabetically sorted by any time field.

10. Using Custom LDAP Filters

Gold Finger lets you customize any report 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 partial LDAP filter in the LDAP filter box. For example, to have Gold Finger search for and retrieve all domain user accounts whose title matches **C*O**, you will only need to enter ***(title=C*O)*** in the LDAP filter box. You do not need to enter the complete LDAP filter, which in this example would be *(&(objectCategory=person)(objectClass=user)(title=C*O))*.

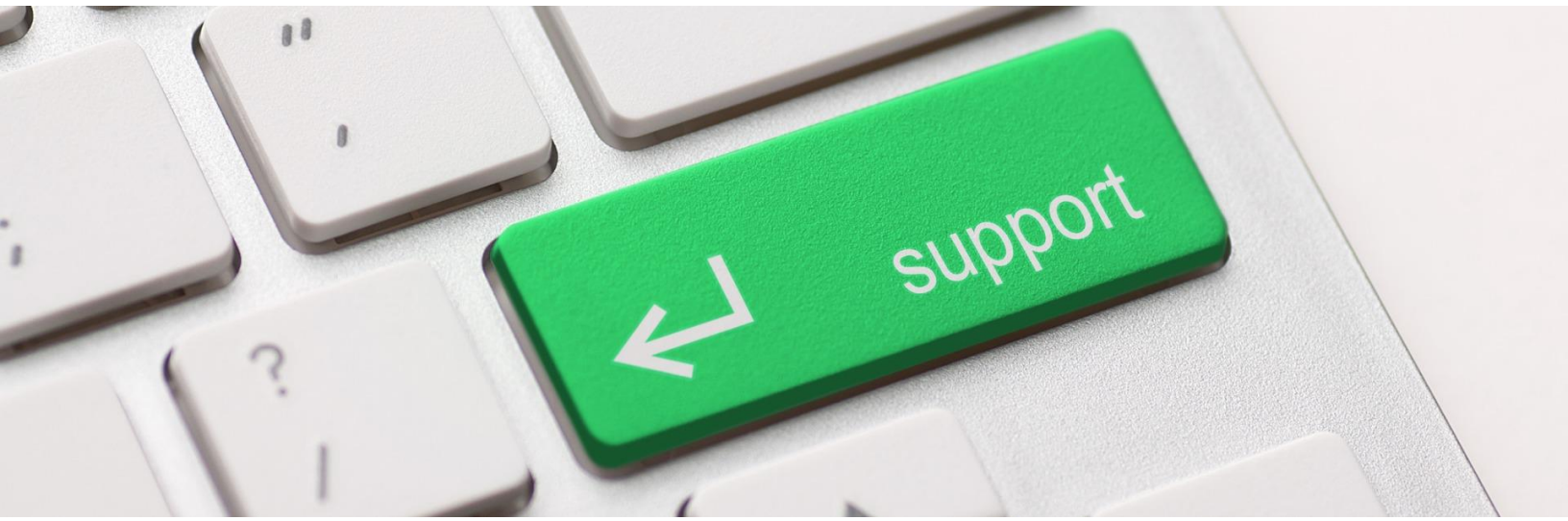
In essence, based on the category of the report being generated (e.g. user account mgmt., group mgmt. etc.,) Gold Finger automatically prepends the required *object** component(s), letting you focus on and specify just the part that you wish to customize. Should you wish to apply a complete LDAP filter, you can do so with Report 101, *List of all Active Directory objects*.

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