



Gold Finger

Active Directory Membership Auditor

User's Guide



Gold Finger

Active Directory Membership Auditor

Contents

Introduction	1
1. Installation	2
2. Getting Started	2
3. Becoming Familiar with Gold Finger's User-Interface	3
4. Auditing/Enumerating an Active Directory Group's Membership	4
5. Analyzing Active Directory Group Membership Audit Results	5
6. Auditing/Enumerating an Active Directory Account's Group Memberships	6
7. Exporting Results and Generating PDF Reports	7
8. Using Inbuilt Search	7
9. Using Basic Options	8
10. Using Advanced Options	8
11. Using Retrieval Options	9
12. Obtaining Technical Support	10

Active Directory Membership Auditor



Introduction

Security is fundamentally about access control, and in Windows Server based networks access to almost all IT resources is controlled using Active Directory security groups.

Membership in an Active Directory security group can grant an individual instant access to all IT organizational resources access to which is being controlled using that security group.

Further, a substantial amount of unrestricted and delegated privileged access is also made possible by Active Directory security groups, necessitating control and periodic reviews.

Consequently, to ensure the security of all organizational IT resources, it is important to periodically audit, review and verify the membership of Active Directory security groups.

Active Directory security group memberships can be complicated to easily and accurately audit because security groups can be and often are nested within security groups, and in some cases security groups can also be circularly nested.

The *Active Directory Membership Auditor* lets organizational IT personnel easily audit, review and verify the complete membership of any Active Directory security group. It can –

- ✓ Deliver a complete view of any Active Directory security group's membership
- ✓ Clearly identify all group members, as well as the nested groups they belong to
- ✓ Export the complete flattened membership of any Active Directory security group

It thus enables organizations to easily perform Active Directory group membership audits which are needed to maintain cyber security, lockdown access and fulfill audit needs.



Active Directory Membership Auditor



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.



START

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 Membership Auditor



3. Becoming Familiar with Gold Finger's User-Interface

Gold Finger's sheer simplicity is reflected in its minimalist user-interface.

The screenshot shows the Gold Finger Membership Auditor application window. The interface is minimalist and includes the following elements:

- 1. Tool Selector:** A dropdown menu currently set to "Membership Auditor".
- 2. Reports pane:** A list of three report options:
 1. View the direct membership of an Active Directory security group
 2. View the complete nested group membership of an Active Directory security group
 3. View the complete list of all Active Directory security groups to which a user belongs
- 3. Scope field:** A dropdown menu set to "CN=IT Team,OU=IT Admin".
- 4. Search utility:** A search box with a magnifying glass icon.
- 5. Gold Finger (Run) button:** A button with an image of a hand holding a gold ring.
- 6. Results pane(s):** A table displaying the results of a report. The table has columns: Name, SAM Account Name, Title, Department, Account Status, Nesting, and DN. The data is as follows:

	Name	SAM Account Name	Title	Department	Account Status	Nesting	DN
1.	IT Staff	root\IT Staff					CN=IT Staff,OU=IT
2.	IT Managers	root\IT Managers					CN=IT Managers,C
3.	John Bradman	root\JBradman	IT Auditor	IT	Enabled	{ root\IT Staff }	CN=John Bradman
4.	James Carter	root\JCarter	IT Auditor	IT	Enabled	{ root\IT Staff }	CN=James Carter,
5.	Ryan Johnson	root\RJJohnson	IT Account Manager	IT	Enabled	{ root\IT Staff }	CN=Ryan Johnson
6.	John Redford	root\JRedford	IT Manager	IT	Enabled	{ root\IT Staff } { root\IT Managers }	CN=John Redford,(
7.	Chris O' Connell	root\CCConnell	IT Application Developer	IT	Enabled	{ root\IT Staff }	CN=Chris O' Conn
8.	Brad Walsh	root\BWalsh	IT Web Administrator	IT	Enabled	{ root\IT Staff }	CN=Brad Walsh,O
9.	Javier Gomez	root\JGomez	IT Exchange Admin	IT	Enabled	{ root\IT Staff }	CN=Javier Gomez,
10.	Saniav Guota	root\SGuota	IT Exchange Admin	IT	Enabled	{ root\IT Staff }	CN=Saniav Guota
- 7. Status indicator:** A "Status" label at the bottom left.
- 8. CSV and PDF buttons:** Two buttons for exporting the report results.

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

Active Directory Membership Auditor



4. Auditing/Enumerating an Active Directory Group's Membership

Gold Finger can accurately, automatically and instantly audit/enumerate both the direct and nested (complete flattened) group membership of any Active Directory security group.



To audit/enumerate the membership of a specific Active Directory security group, simply –

1. Use the Tool selector to select the **Active Directory Membership Auditor** tool.
2. In the *Reports* pane, select either of the following reports, as appropriate –
View the direct membership of an Active Directory security group
View the complete nested group membership of an Active Directory security group
3. In the *Scope* field, enter the distinguished name (DN, e.g. *cn=domain admins,cn=users,dc=example,dc=com*) of the domain security group whose membership you wish to audit.

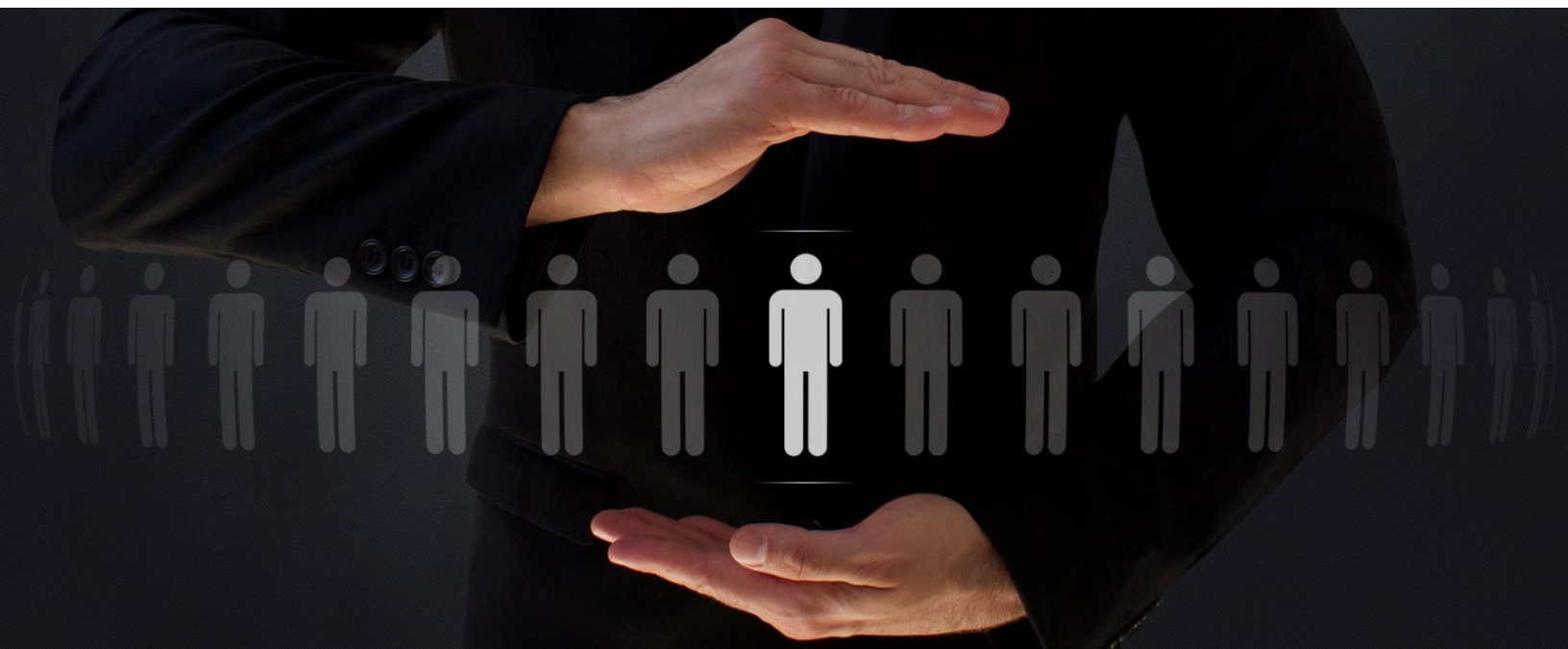
Note: Gold Finger includes an inbuilt *Search* utility that is intended and designed to help you easily and quickly search for and locate Active Directory objects based on various criteria, and have their DNs be automatically determined and inserted into the *Scope* field.

4. Click the **Gold Finger** button.



5. Analyzing Active Directory Group Membership Audit Results

Upon completion, depending on the report selected, Gold Finger will accordingly display the direct or fully flattened membership of the specified security group in the *Membership* pane.



If the *View the direct membership of an Active Directory security group* report was selected, Gold Finger will retrieve and display the membership of the specified Active Directory security group verbatim i.e. the membership will be identical to that displayed by Microsoft's tooling.

If the *View the complete nested group membership of an Active Directory security group* report was selected, Gold Finger will automatically and recursively expand all nested security groups, including any circularly nested groups, and completely flatten the membership of the specified security group to determine and display the group's actual complete flattened membership.

Gold Finger will also provide complete insight into how a specific security principal is a member of the specified security group i.e. exactly which nested group(s) that security principal belongs to, as a result of which he/she is currently a member of the specific security group.

Gold Finger can thus be used to enumerate/audit both the direct as well as the complete flattened membership of any Active Directory security group, at the touch of a button.



4. Auditing/Enumerating an Active Directory Account's Group Memberships

Gold Finger can also accurately, automatically and instantly audit/enumerate the list of all* Active Directory groups to which an Active Directory domain user/computer account belongs.



To audit/enumerate the list of all groups to which an Active Directory account belongs, simply –

1. Use the Tool selector to select the **Active Directory Membership Auditor** tool.
2. In the *Reports* pane, select the report –

View the complete list of all Active Directory security groups to which a user belongs

3. In the *Scope* field, enter the distinguished name (DN, e.g. *cn=administrator,cn=users,dc=example,dc=com*) of the domain account whose memberships you wish to audit.

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. Upon completion, Gold Finger will display the list of all* security groups to which the specified domain account belongs, in the *Membership* pane.

* Built-in security groups, being domain-specific, may not be included.



6. Exporting Results and Generating PDF Reports

To export the group membership of a specific domain security group, after its membership is displayed, simply click the **CSV** button, specify a location for the output CSV file and click OK. To generate a (customizable via *PDF Options*) PDF report, click the **PDF** button, 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.

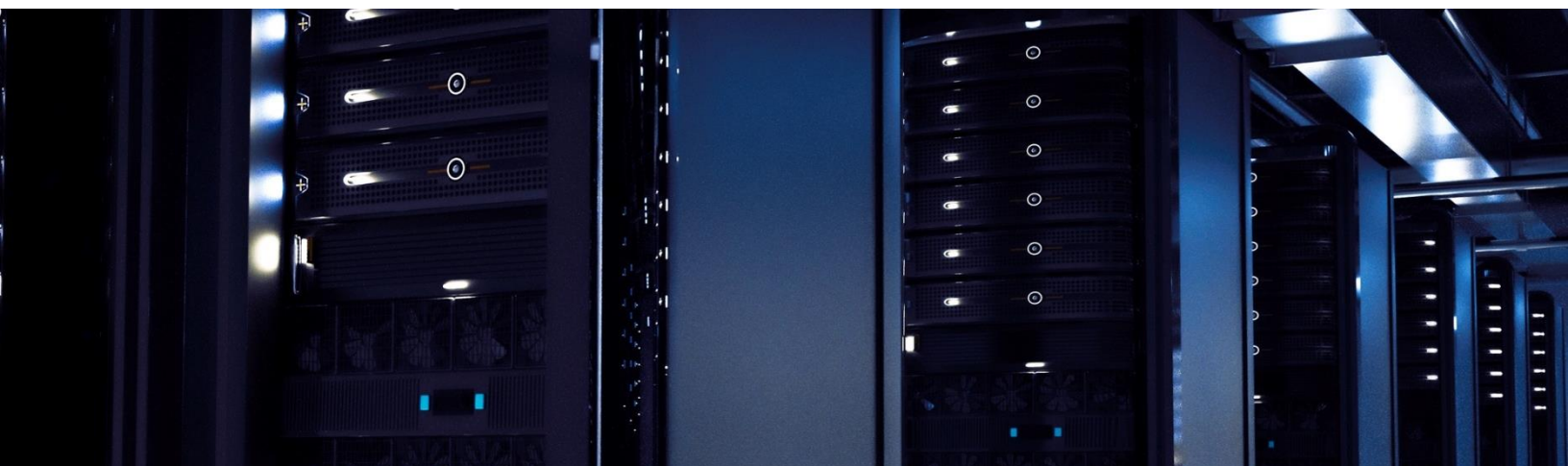
Note: Wildcards (*) can be used in the search criteria. To search the Configuration or Schema partitions, in (1) select the forest root domain, then change the target partition option from D (domain) to C (Configuration) or S (Schema) as required.

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 Membership 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 audit/enumerate the membership of any Active Directory security groups residing in the *System* container.
3. **Display member group nesting in lieu of description** – If this preference option is selected, in lieu of the description column, Gold Finger will display a *Nesting* column, in which it will display the appropriate group nesting details for all security principals that are members of the specified security group by virtue of being a member of a(ny) nested security group(s).

11. Using Retrieval Options

Gold Finger offer six retrieval options that can be used to filter the type of members that are retrieved and displayed by Gold Finger when enumerating group memberships. These options can be specified using the *Retrieval* drop-down located below the *Reports* pane, and are -

1. **All Members (Default)** – Retrieve and display all members of the security group
2. **User Accounts Only** – Retrieve and display domain user account members only
3. **Computer Accounts Only** – Retrieve and display domain computer account members only
4. **Well-Knowns/FSPs Only** – Retrieve and display well-known/FSP members only
5. **Security Groups Only** – Retrieve and display security group members only
6. **User and Computer Accounts Only** – Retrieve and display domain user and computer account members only

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



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.

