Gold Finger

Active Directory Token-size Calculator

User's Guide

Gold Finger

Active Directory Token-size Calculator

Contents

Active Directory Token-size Calculator

Introduction

In Active Directory environments where domain user or computer accounts could belong to a large number (i.e. hundreds) of Active Directory security groups, there could be situations where the number of groups to which a domain account belongs exceeds the number of security identifiers (SIDs) that can fit in a Windows access token.

In such situations, during logon, when Windows attempts to create an access token for the user, because the number of SIDs exceeds the number that fit in a Windows access token, the system is unable to successfully create an access token for the user, and as a result the user is unable to logon, resulting in an issue generally known as token-bloat.

Organizations that have or use a large number of groups can benefit from computing the Kerberos token-sizes of all accounts to identify accounts that may be at risk of token-bloat.

The accurate computation of Kerberos token-sizes is sophisticated because it requires accurately simulating the creation of a Windows access token for a domain user account, since a Windows access token is always specific to a domain, and differs in each domain.

The *Active Directory Kerberos Token-size Calculator* completely automates the accurate computation of domain specific Kerberos token-sizes for all domain user accounts. It can –

- ✓ Automatically calculate the Kerberos token-sizes of all domain user accounts
- ✓ Compute and display domain-specific token-sizes of all domain user accounts
- ✓ Identify and reveal the list of SIDs that show up in any domain account's access token

It thus enables organizations to easily identify all domain accounts that may be at a risk of token bloat, thus helping them identify all such accounts, enabling proactive mitigation.

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

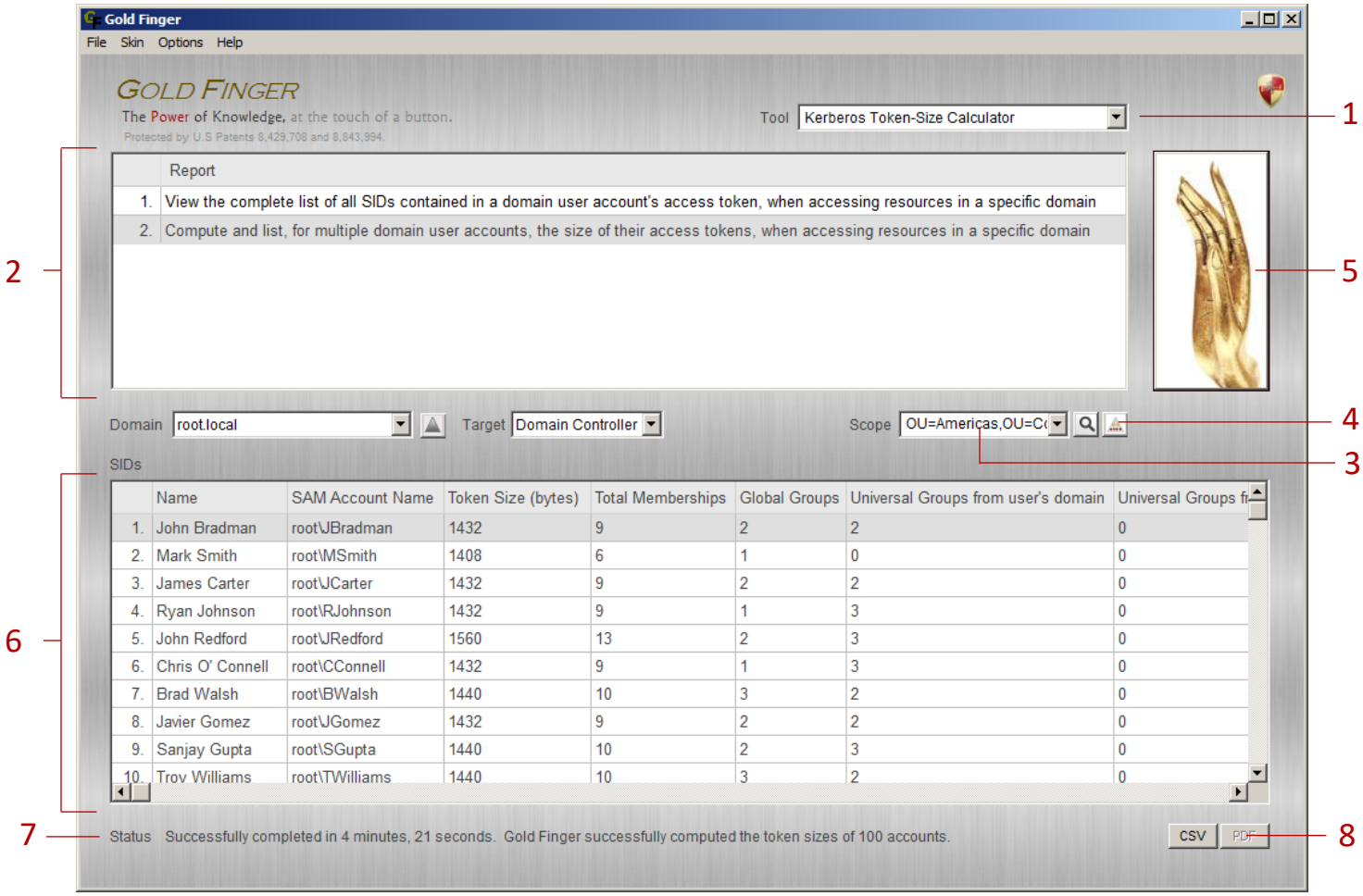
To begin, launch **Gold Finger**. To do so, click the *Start* menu, then locate the *Paramount Defenses* folder, and within it, select *Gold Finger* i.e. click on it to launch the application.

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

Active Directory Token-size Calculator

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 the List of All SIDs Contained in a Domain Account's Access Token

Gold Finger can accurately, automatically and instantly determine the list of all SIDs that show up in any Active Directory domain account's domain-specific and target-specific access token.

To view the list of all SIDs that show up in a specific Active Directory account's token, simply –

1. Use the Tool selector to select the **Active Directory Token-size Calculator** tool.

2. In the *Reports* pane, select the report – *View the complete list of all SIDs contained in a domain user account's token, when accessing resources in a specific domain.*

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 token you wish to obtain insight into.

   Note: Gold Finger includes an inbuilt *Search* utility that can 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. Select a target domain from the *Domains* dropdown, and a *Target type* (Member Server/DC).

   Note: If *Domains* dropdown is empty, click the *Enumerate Domains* button (located to the right of that dropdown) once, to have Gold Finger populate the dropdown.

5. Click the ***Gold Finger*** button. Gold Finger will automatically compute the list of all SIDs in the specified domain account's resulting access token, and display results in the *Results* pane.

5. Computing Token-Sizes of All Domain Accounts in an Active Directory Domain

Gold Finger can also accurately and automatically compute domain-specific and target-specific Kerberos token-sizes of all domain accounts in an Active Directory domain, at a button's touch.

To compute the Kerberos token-sizes of all accounts in an Active Directory domain, simply –

1. Use the Tool selector to select the **Active Directory Token-size Calculator** tool.

2. In the *Reports* pane, select the report – *Compute and list, for multiple domain user accounts, the size of their access tokens, when accessing resources in a specific domain.*

3. In the *Scope* field, enter the distinguished name (DN, e.g. *dc=example,dc=com*) of the Active Directory domain or OU that contains the accounts whose token-sizes you wish to compute.

   Note: Gold Finger includes an inbuilt *Search* utility that can 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. Select a target domain from the *Domains* dropdown, and a *Target type* (Member Server/DC).

   Note: If *Domains* dropdown is empty, click the *Enumerate Domains* button (located to the right of that dropdown) once, to have Gold Finger populate the dropdown.

5. Click the ***Gold Finger*** button. Gold Finger will automatically compute the Kerberos token-sizes of all domain user accounts in the specified scope, and display results in the *Results* pane.

6. Exporting Results and Generating PDF Reports

To export the results of a specific report, after its results have been displayed in the *Results* pane, 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.

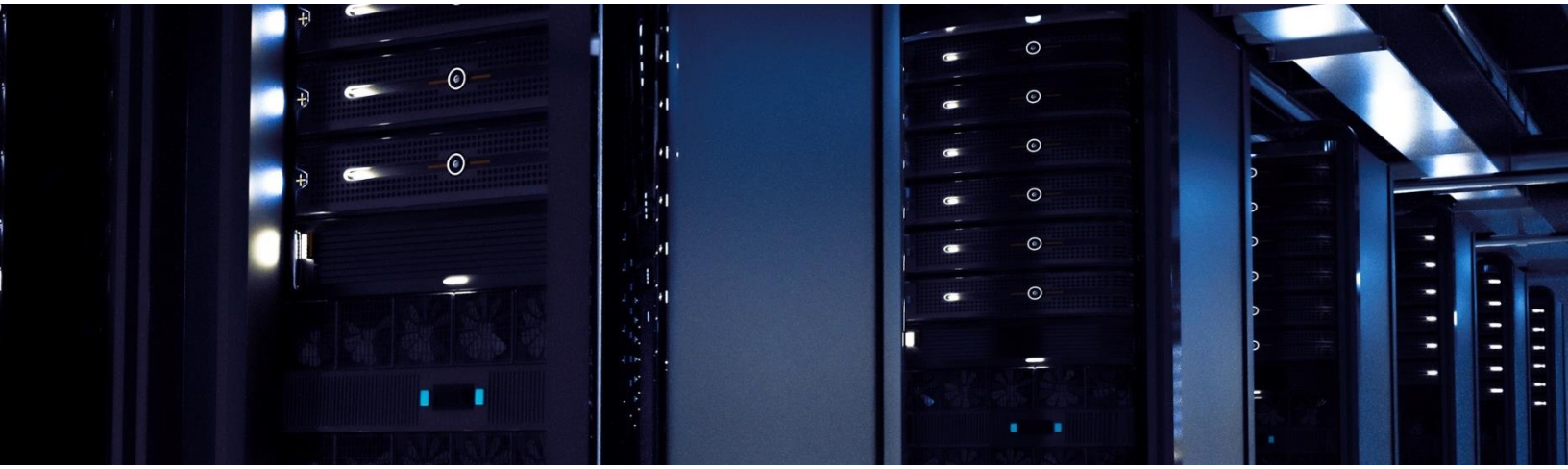
To use the inbuilt search utility to locate Active Directory objects, simply –

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 Token-size Calculator* 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 determine the list of SIDs contained in the access token of, and compute the token-sizes of, any Active Directory accounts 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.

11. Understanding Domain Specific and Target-type Specific Access Tokens

When computing Kerberos token-sizes, it is important to know that a Windows access token is always domain and target-type specific, and thus even for the same domain account, it could and will likely differ in each domain.

Specifically, in a multi-domain Active Directory environment, the Windows access token that is generated for a specific domain user account in one domain will almost always differ from the access token generated for the same domain user account in another domain, because the user's domain-local and built-in group memberships will likely be different in these domains.

Further, even in the same domain, depending on whether a domain user account's Windows access token is generated when accessing resources on a domain-joined machine (generically referred to as a *Member Server* in Gold Finger) or a domain-controller, the list of well-known security principals that are added to the user's resulting access token will also be different.

Thus, when computing Kerberos token-sizes, it is important to know and understand that in Windows, access tokens are always domain and target-type specific, and thus that even for the same domain user account, they could and almost always do differ in different domains.

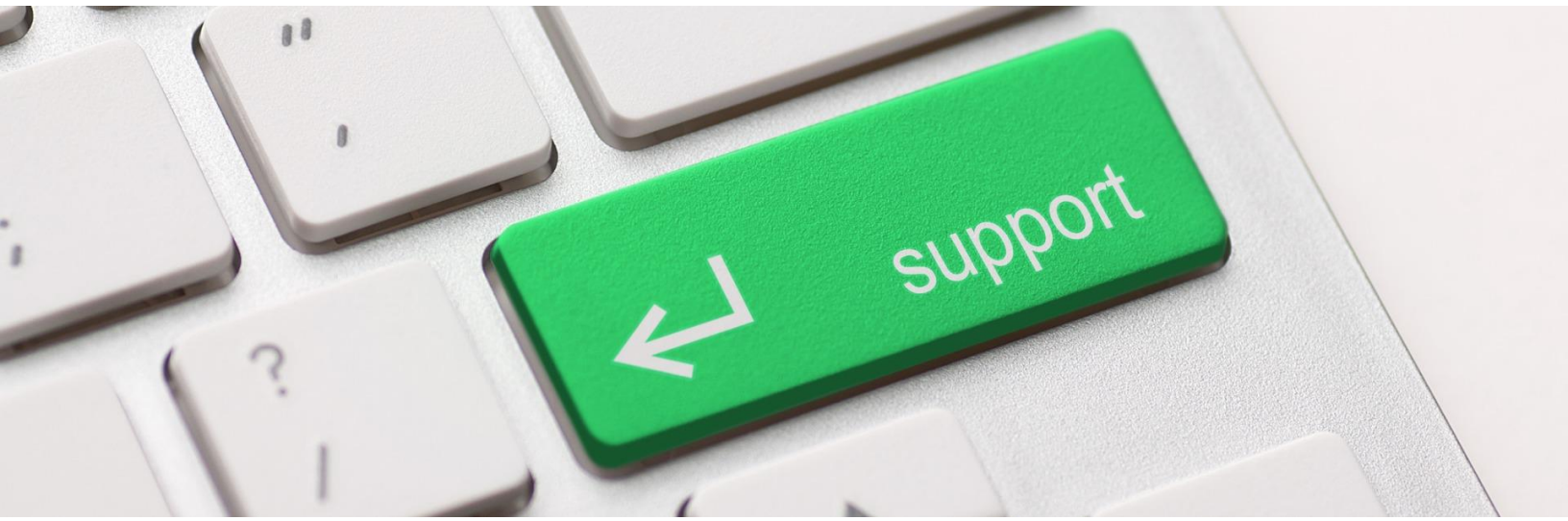
This technicality must be taken into consideration when computing Kerberos token-sizes, and most custom/third-party PowerShell scripts and other solutions do not take this into account.

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