



## About this guide

The *Find Sessions User's Guide* provides information for using the Find Sessions functionality that's included as part of Audit Analyzer. You can use Find Sessions to replay captured user sessions and perform other session review tasks.

### Documentation conventions

The following conventions are used in Centrify documentation:

- Fixed-width font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *italicized*, this font indicates variables. Square brackets ( [ ] ) indicate optional command-line arguments.
- **Bold** text is used to emphasize commands or key command results; buttons or user interface text; and new terms.
- *Italics* are used for book titles and to emphasize specific words or terms. In fixed-width font, italics indicate variable values.
- Standalone software packages include version and architecture information in the file name. Full file names are not documented in this guide. For complete file names for the software packages you want to install, see the distribution media.
- For simplicity, UNIX is used to refer to all supported versions of the UNIX and Linux operating systems. Some parameters can also be used on Mac OS X computers.

### Finding more information about Centrify products

Centrify provides extensive documentation targeted for specific audiences, functional roles, or topics of interest. If you want to learn more about Centrify and Centrify products and features, start by visiting the [Centrify website](#). From the Centrify website, you can download data sheets and evaluation software,



view video demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.

For access to documentation for all Centrify products and services, visit the [Centrify documentation portal](https://docs.centrify.com) at [docs.centrify.com](https://docs.centrify.com). From the Centrify documentation portal, you can always view or download the most up-to-date version of this guide and all other product documentation.

For details about supported platforms, please consult the release notes.

For the most up to date list of known issues, please login to the Customer Support Portal at <http://www.centrify.com/support> and refer to Knowledge Base articles for any known issues with the release.

## Product names

Over the years we've made some changes to some of our product offerings and features and some of these previous product names still exist in some areas. Our current product offerings include the following services:

Current Overall Product Name	Current Services Available
Centrify Zero Trust Privilege Services	Privileged Access Service
	Gateway Session Audit and Monitoring
	Authentication Service
	Privilege Elevation Service
	Audit and Monitoring Service
	Privilege Threat Analytics Service

Whether you're a long-time or new customer, here are some quick summaries of which features belong to which current product offerings:

Previous Product Offering	Previous Product Offering	Description	Current Product Offering
	Centrify Privileged Service (CPS)		Privileged Access Service
DirectControl (DC)			Authentication Service



Previous Product Offering	Previous Product Offering	Description	Current Product Offering
DirectAuthorize (DZ or DZwin)			Privilege Elevation Service
DirectAudit (DA)			Audit and Monitoring Service
	Infrastructure Services		Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service, and Privilege Threat Analytics Service
DirectManage (DM)	Management Services	Consoles that are used by all 3 services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service	
DirectSecure (DS)	Isolation and Encryption Service		Still supported but no longer being developed or updated
	User Analytics Service		Privilege Threat Analytics Service

Depending on when you purchased a Centrify product offering, you may have purchased one of the following product bundles:

Previous Product Bundle	Previous Product Bundle	Current Product Bundle	Services Included	Description
		Centrify Zero Trust Privilege Services Core Edition		Privileged Access Service and Gateway Session Audit and Monitoring
Centrify Server Suite Standard Edition	Centrify Infrastructure Services Standard Edition	Centrify Zero Trust Privilege Services Standard Edition		Privileged Access Service, Authentication Service, and Privilege Elevation Service



Previous Product Bundle	Previous Product Bundle	Current Product Bundle	Services Included	Description
Centrify Server Suite Enterprise Edition	Centrify Infrastructure Services Enterprise Edition	Centrify Zero Trust Privilege Services Enterprise Edition	Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service (includes Gateway Session Audit and Monitoring)	
Centrify Server Suite Platinum Edition				Discontinued bundle that included DirectControl, DirectAuthorize, DirectManage, DirectAudit, and DirectSecure

## Contacting Centrify

You can contact Centrify by visiting our website, [www.centrify.com](http://www.centrify.com). On the website, you can find information about Centrify office locations worldwide, email and phone numbers for contacting Centrify sales, and links for following Centrify on social media. If you have questions or comments, we look forward to hearing from you.

## Getting additional support

If you have a Centrify account, click Support on the Centrify website to log on and access the [Centrify Technical Support Portal](#). From the support portal, you can search knowledge base articles, open and view support cases, download software, and access other resources.

To connect with other Centrify users, ask questions, or share information, visit the [Centrify Community](#) website to check in on customer forums, read the latest blog posts, view how-to videos, or exchange ideas with members of the community.



# Centrify Zero Trust Privilege Services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service

*Find Sessions User's Guide*

August 2019 (release 19.6)

Centrify Corporation



## Legal Notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrifly Corporation provides this document and the software described in this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrifly Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrifly Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrifly Corporation may make improvements in or changes to the software described in this document at any time.

© **2004-2019 Centrifly Corporation. All rights reserved.** Portions of Centrifly software are derived from third party or open source software. Copyright and legal notices for these sources are listed separately in the Acknowledgements.txt file included with the software.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrifly, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrifly for Mobile, Centrifly for SaaS, DirectManage, Centrifly Express, DirectManage Express, Centrifly Suite, Centrifly User Suite, Centrifly Identity Service, Centrifly Privilege Service and Centrifly Server Suite are registered trademarks of Centrifly Corporation in the United States and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Centrifly software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,442,962 and 9,378,391.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.



# Contents

About this guide .....	1
<b>Using Find Sessions .....</b>	<b>8</b>
Starting Find Sessions .....	8
Specifying the sessions to find .....	8
Finding sessions from a command line .....	11
Finding sessions using AQL syntax .....	13
Using a web browser to access sessions .....	14
Exporting sessions and session data .....	16
Deleting sessions .....	21
Find Sessions return codes .....	23
Suppressing warning messages .....	24



# Using Find Sessions

Find Sessions is a separate executable file, installed in the same directory as Audit Analyzer, that you can use to find and open audited sessions. The program provides a graphical user interface and a command line interface for specifying the search criteria. You can use either interface to find sessions of interest. From the Find Sessions graphical user interface, you can also replay, update the review status, view the desktops used for any sessions found, display the list of indexed commands or events, and copy the session URI.

## Starting Find Sessions

You can start Find Sessions from the Windows command line, using a web browser, or by selecting the View DirectAudit Sessions menu option in other applications, such as Access Manager and Active Directory Users and Computers.

For example, in Access Manager or Active Directory Users and Computers, you can select a computer or user, right-click, then select View DirectAudit Sessions to open Find Sessions. To start Find Sessions from the Windows command line, you can navigate to the Audit Analyzer installation directory and run the following command in a command prompt window:

```
findsessions /ia
```

## Specifying the sessions to find

After you start Find Sessions by selecting View DirectAudit Sessions, from the Windows command line, or in a web browser, the program displays a graphical user interface for selecting search criteria. You can use the Common or Advanced search criteria to find sessions of interest. The Find Sessions



dialog box then displays the results that match the criteria you specify. You can then replay, update the review status, display the list of indexed commands or events, copy session URI, or view the desktops used in any of the sessions returned.

In most cases, you can find the sessions you are interested in through some combination of user name, computer name, and session time displayed on the Common tab. If you right-click to View DirectAudit Sessions from a specific computer or user, that computer or user is automatically defined as the search criteria. If you want to specify additional criteria, such as review status or auditor name, you can click the Advanced tab.

## To specify criteria by which to find sessions:

1. Start Find Sessions.
2. Select the desired installation from the Installation list.
3. On the Common tab, enter the basic search criteria as applicable for the sessions you want to find:
  - User: Type all or part of the user name to find sessions for a particular user account.
  - Machine: Type all or part of the computer name to find sessions run on a particular computer.
  - Session start time: Select this option to find sessions based on when the session started. If you select this option, you can refine the search to include sessions started or not started in a specific number of days, hours, or minutes, or to include sessions started or not started today, yesterday, this week, last week, this month, last month, this year, or last year.
4. Click **Find Now** to find the sessions that match the criteria you specified.
5. Click **Clear All** to start a new query.

## Specifying advanced criteria

In some cases, you might want to specify additional criteria for a search or to search exclusively on an attribute not found on the Common tab. For example, you might want to find only those sessions that have yet to be



reviewed or all of the sessions where a specific command or application was used. To add criteria or perform these types of specialized searches, you can click the **Advanced** tab.

## To specify advanced criteria for finding sessions:

1. Start Find Sessions.
2. Select the desired installation from the Installation list.
3. Click the **Advanced** tab.
4. Click **Add** to add a new criterion.
5. Select an appropriate attribute from the Attribute list based on the sessions you want to find.

For example, you can search for sessions based on the period of time in which they were active or based on a specific state. You can also search for sessions based on the activity that took place during the session. For example, you can find sessions where specific UNIX commands or Windows applications were used.

6. Select the appropriate criteria for the attribute you selected, then click **OK**.

The specific selections you can make depend on the attribute selected. For example, if the attribute is Review Status, you can choose Equals and the review state you want to find. If you select the attribute Comment, you can specify Contains any of and type the string that you want to find any part of.

When searching for user names or computers on the Advanced tab, use the Starts with option. If you use the default to match exactly, you must include the fully qualified domain name of the user or computer.

7. Click **Add** to add another criterion until you have defined all of the attributes for which you want to find sessions.
8. Click **Find Now** to find the sessions that match the criteria you specified.
9. Click **Clear All** to start a new query.



## Adding advanced criteria

If you have more than one advanced criteria, different criteria attributes, such as `session Time` and `State`, are separated by an implicit AND operation. Only sessions that match both criteria are returned. If you have repeated criteria attributes, for example, `time is not in past 10 days`; `time is in last month`, the attributes are separated by an implicit OR operation. Sessions that match either criteria are returned.

## Editing and removing advanced criteria

You can edit and remove any of the advanced criteria you specify. For example, if you are not finding the appropriate sessions, you might need to change or remove the criteria you have defined.

### To edit or remove criteria:

1. Start Find Sessions.
2. Select the desired installation from the Installation list.
3. Click the **Advanced** tab.
4. Select the criterion in the list of Define Criteria.
5. Click **Edit** to modify the definition or **Remove** to remove the criterion.

## Finding sessions from a command line

You can run Find Sessions as a command line utility on computers where Audit Analyzer is installed. The command line interface can be useful, for example, if you may want to find, export, or delete sessions as part of a script.

You can view usage information for the command line interface using the `/help` option.

### To use the command line interface for Find Sessions:



1. Open a Command window and navigate to the Audit Analyzer directory.

```
cd "C:\Program Files\Centrify\Audit\AuditAnalyzer"
```

2. Run the `findsessions` command with the `/help` option to view usage information.

```
findsessions /help
```

3. Specify search criteria for finding sessions using the following format:

```
findsessions /i="InstallationName" /u="username"  
/m="computerName" /t="yyyy-MM-dd HH:mm:ss"
```

The installation name is required. You must also specify at least one of the other criteria (user name, computer name, or time). You can also combine the search criteria to refine your search.

For user name and computer name, you can specify a portion of a name to find all sessions matching that name portion. For time, if you specify a date without a time, the assumed time is 12 midnight. For example, if you do the following search and you have sessions on computers named "KH-Win7" and "KH-W8," the results include sessions for both computers.

```
FindSessions /i="DefaultInstallation" /m="KH-W"
```

The following example finds sessions for "Admin" and "Administrator" users:

```
FindSessions /i="DefaultInstallation" /u="Admin"
```

The following example finds sessions that were running at a specific time regardless of what time the sessions started or ended:

```
FindSessions /i="DefaultInstallation" /t="2015-01-21  
5:25:00"
```

You can also find sessions for multiple users or computers by separating the user names or computer names using a semi-colon (;). For example, to search for audited sessions for the users `maya` and `fred`, you can specify both users in the command line like this:

```
FindSessions /i="DefaultInstallation" /u="maya;fred"
```

For more complex queries, you can also use AQL syntax on the command line. For details, see [Finding sessions using AQL syntax](#).



## Finding sessions using AQL syntax

If you are an experienced programmer and want to write complex queries, you can use AQL statements on the command line.

### To use AQL to find sessions at the command line:

1. Open a Command window and navigate to the Audit Analyzer directory.

```
cd "C:\Program Files\Centrify\Audit\AuditAnalyzer"
```

2. Run the `findsessions` command with the following syntax:

```
FindSessions /i="InstallationName" /aql="AQL query text"
```

For example, the following is a simple query that searches for sessions that were running in the current week:

```
findsessions -i="MyInstallation" /aql="1 time is in this week"
```

To find a specific session using the session identifier, you might write a query similar to the following:

```
FindSessions /i="MyInstallation" /a="1 sessionid = \"a4006f20-6465-4db1-a2e7-a4e1f646c835\""
```

To find a specific session using the user display name, you might write a query similar to the following:

```
findsessions /i="installationname" /a="1 displayname=\"maya\""
```

## Simplifying AQL queries

Writing valid AQL queries for the command line can be challenging. The basic format for AQL statements in Backus-Naur notation consists of the following parts:

```
<aql> ::= <version> {<quick_terms>} | {<type> | <groupby> | <filter>}
```



To simplify the process of generating the AQL queries you want to use on the command line, you can use Audit Analyzer to create a new private query and use the user interface to specify the query criteria. After you have created the query, you can right-click the query node, and click **Export Query Definition** to save the query definition as a file. You can then extract the AQL statement from the query definition. You can then delete the private query node from Audit Analyzer if it is not needed.

For example, run the command with the definition from the private query:

```
findsessions -i="MyInstallation" /aql="1 type= shellui,  
wingui; time is in this week; review = Reviewed"
```

## Using a web browser to access sessions

On computers that have Audit Analyzer installed, you can also find and play back sessions from a web browser. Because the `cda://` protocol is automatically registered on the computer with Audit Analyzer, you can use a web browser to open Find Sessions or to replay a specific session. For example, you can embed a `cda://` link in a web page to automatically generate a list of sessions, or you might want to embed a link to a session or set of sessions in a web-based report or event notification.

### Opening Find Sessions from a web browser

You must be able to specify a query using AQL syntax to open Find Sessions from a web browser. If you want to start playing back a session from a web browser, you must know the session identifier. You can extract the session identifier from the session URI.

### To start Find Sessions from a web browser:

1. Open a web browser.
2. Type the installation name and a search string using AQL syntax in the address bar of the web browser.



For example, if you want to search an installation named `MyInstallation5` for sessions that involved the `Administrator` user, you would type the following in the address bar:

```
cda://MyInstallation5/?search=\"1  
user=\"Administrator*\"\\
```

3. Click **Allow** to open the Find Sessions with the Advanced tab displayed and “`user=Administrator*`” listed for the Define Criteria.
4. Click **Find Now** to find sessions matching the criteria you specified.

## Playing back a session from a web browser

If you want to start playing back a session from a web browser, you must know the session identifier. You can extract the session identifier from the session URI.

### To get the session identifier:

1. In the session player, select `File > Copy Session URI`.
2. Open a text editor and paste the session URI into the file.
3. Delete the portion of the URI that identifies the player and installation, so that only the object GUID remains.

For example, if the URI looks like this:

```
rep://myInstallation/b62bc280-678c-439a-aec3-  
09a9b7ee4395
```

Remove the part of the URI so that you only have the session identifier:

```
b62bc280-678c-439a-aec3-09a9b7ee4395
```

### To play back a specific session from a web browser:

1. Open a web browser.
2. Type the installation name and session ID in the address bar of the web browser:

```
cda://<installationName>/<session_id>
```

For example:



```
cda://myInstallation/b62bc280-678c-439a-aec3-09a9b7ee4395
```

The session player opens and plays the specified session.

## Exporting sessions and session data

In addition to specifying the criteria for finding sessions of interest, you can use Find Session to selectively export session data to a file. You can export the following information:

- A list of sessions matching the criteria you specify.
- An indexed list of events associated with the Windows sessions that match the criteria you specify.
- An indexed list of commands associated with the UNIX sessions that match the criteria you specify.
- The UNIX input associated with the UNIX sessions that match the criteria you specify.
- The UNIX input and output associated with the UNIX sessions that match the criteria you specify.

You specify the export operation, type of data to export, file format, and file location using the following command line options:

```
/export=[SessionList|WashEvents|UnixCommand|UnixInput|UnixInputOutput]
/format=[html|htm|csv|pdf|xml]
/path=<folder_path>
```

You can use these options in combination with other criteria, such as `/user` or `/machine`, to export information for a specific user, computer, or time. You can specify the `/format` option used for exporting the sessions of interest. If you don't specify the `/format` option, sessions matching the criteria you specify are exported as comma-separated values (`.csv`) in a text file. If you are exporting Windows events, UNIX commands, UNIX input, or UNIX input and output, each session is exported as a separate file in the format you specify.

If you are exporting UNIX commands, UNIX input, or UNIX input and output, you can also use the command line options `/role` and `/ticket` to export sessions based on specific role or trouble-ticket information. Before you can use these options, however, you must configure the information required. For



example, if you want to find all of the UNIX commands executed by a user running the `db_backup` role, you must first define and assign the `db_backup` role using Access Manager.

## Exporting a session list

To export a list of sessions from the command line, use the following syntax:

```
FindSessions /i="InstallationName" /export="SessionList"  
/format="format" /path="folder"
```

For example, to export the session list for all users in HTML format and save the output in the `C:\Temp\Exported Sessions` folder, you would type a command like this:

```
FindSessions /i="MyInstallation" /export="SessionList"  
/format="html" /path="C:\Temp\Exported Sessions"
```

The command generates the list of sessions in the format specified. In this case, the command would generate an HTML file named `sessionList` in the `C:\Temp\Exported Sessions` folder with the following information for each session exported:

- User name, display name, account used, computer name, and audit store for the session.
- Start time, end time, and current state of the session.
- Client name associated with the session.
- Review status, user who last modified the review status, the time the status was last modified, and the comment added when the session was last modified.
- Size of the session in KB.
- Session URI that can be used to replay the session.

## Exporting Windows events

To export an indexed event list for Window sessions from the command line, use the following syntax:

.....

```
FindSessions /i="InstallationName" /export="WashEvents"  
/path="folder"
```

For example, to export the indexed event list for the sessions associated with a specific user and save the output in the `C:\Temp\Session Events` folder, you would type a command like this:

```
FindSessions /i="MyInstallation" /user="chris.howard"  
/export="WashEvents" /path="C:\Temp\Session Events"
```

The command generates the list of events as comma-separated values in a text file. For example:

```
"Time", "Application", "Title", "Type", "Desktop", "Audited", "Role", "Ticket"  
  
"1/29/2015 1:53:14 PM", "Windows Explorer", "Start",  
"Application Activate", "Default", "Y", "<None>", "<None>"  
"1/29/2015 1:53:56 PM", "DirectAuthorize System Tray",  
"Options", "Application Activate", "Default",  
"Y", "<None>", "<None>"  
...  
"1/29/2015 3:00:51 PM", "Windows Explorer", "Start",  
"Window Activate", "LocalSQLAdmin", "Y", "<None>", "<None>"  
"1/29/2015 3:01:16 PM", "Microsoft SQL Server Management  
Studio Express", "Microsoft SQL Server Management Studio  
Express", "Application Activate", "LocalSQLAdmin",  
"Y", "<None>", "<None>"  
.
```

## Exporting UNIX command lists

To export an indexed command list for UNIX sessions from the command line, use the following syntax:

```
FindSessions /i="InstallationName" /export="UnixCommand"  
/path="folder"
```

For example, to export the indexed command for the sessions associated with a specific computer and save the output in the `C:\Temp\UNIX` folder, you would type a command like this:

```
FindSessions /i="MyInstallation" /machine="rhes-63"  
/export="UnixCommand" /path="C:\Temp\UNIX"
```



The command generates the list of commands as comma-separated values in a text file. For example:

```
"Time", "Command", "Role", "Ticket"  
"10/9/2014 3:12:14 PM", "/bin/bash ", "<None>", "<None>"  
"10/9/2014 3:12:19 PM", "adflush", "<None>", "<None>"  
"10/9/2014 3:12:23 PM", "su -", "<None>", "<None>"  
"10/9/2014 3:12:27 PM", "Password: ", "<None>", "<None>"  
"10/9/2014 3:12:30 PM", "adflush", "<None>", "<None>"  
"10/9/2014 4:26:14 PM", "exit", "<None>", "<None>"
```

### Searching for sessions by role or trouble-ticket information

When you use the `/export=UnixCommand` option, you can also use the command line options `/role` and `/ticket` to export sessions based on specific role or trouble-ticket information.

Use `/role` to specify search criteria based on one or more privilege elevation service roles. You can specify multiple roles separated by semicolons (;). For example, add `/role="db_backup/zonename;mail_admin/zonename"` to the command line to search for UNIX sessions that were run using the `db_backup` or `mail_admin` role.

**Tip** When you search for sessions by role name, be sure to include the zone name. Otherwise, `FindSessions` doesn't return the sessions and instead displays the message, "No session is selected to be exported".

```
FindSessions /i="MyInstallation" /export="UnixCommand"  
/role="db_backup/zonename;mail_admin/zonename"  
/path="C:\Temp\UNIX"
```

You can use the `/ticket` option to specify search criteria based on the trouble-ticket information if you have configured in the `dzcheck` script to collect this information. You can specify multiple tickets separated by semicolons (;). For example, add `/ticket="ticket 1;ticket 2"` to the command line to search for sessions `ticket1` or `ticket2` were specified.

You cannot use wildcards to search for role names or ticket information. If you specify both the `/role` and `/ticket` options, `FindSessions` returns the sessions that match both the specified roles and the specified trouble-ticket information. For information about configuring the `dzcheck` script and how to capture trouble-ticket information, see the *Administrator's Guide for Linux and UNIX*.

.....

## Exporting UNIX input

To export UNIX input from the command line, use the following syntax:

```
FindSessions /i="InstallationName" /export="UnixInput"  
/path="folder"
```

For example, to export the UNIX input for a specific user and save the output in the `C:\Temp\Input` folder, you would type a command like this:

```
FindSessions /i="MyInstallation" /user="tai-ul"  
/export="UnixInput" /path="C:\Temp\Input"
```

The command exports UNIX input to a text file. For example:

```
"UnixInputData", "Role", "Ticket"  
"[1/20/2015 4:13:38 PM] K:  
PS1=NetShell:<CR>", "<None>", "<None>"  
"[1/20/2015 4:13:38 PM] K: stty kill ^u erase  
^h<CR>", "<None>", "<None>"  
"[1/20/2015 4:13:38 PM] K: TERM=dumb<CR>", "<None>", "<None>"  
"[1/20/2015 4:13:38 PM] K: set  
TERM=dumb<CR>", "<None>", "<None>"  
"[1/20/2015 4:13:40 PM] K: cat  
/etc/passwd<CR>", "<None>", "<None>"  
"[1/20/2015 4:13:40 PM] K: echo $?<CR>", "<None>", "<None>"  
"[1/20/2015 4:13:40 PM] K: cat  
/etc/group<CR>", "<None>", "<None>"  
"[1/20/2015 4:13:40 PM] K: echo $?<CR>", "<None>", "<None>"
```

When you use the `/export=UnixInput` option, you can also use the command line options `/role` and `/ticket` to export sessions based on specific role or trouble-ticket information. For details about using these options, see [Using Find Sessions](#).

## Exporting UNIX input and output

To export UNIX input and output from the command line, use the following syntax:

```
FindSessions /i="InstallationName"  
/export="UnixInputOutput" /path="folder"
```

.....

For example, to export UNIX input and output for a specific computer and save the output in the C:\Temp\output folder, you would type a command like this:

```
FindSessions /i="MyInstallation" /m="firefly-sf"  
/export="UnixInputOutput" /path="C:\Temp\Output"
```

The command exports UNIX input and output to a text file. For example:

```
"UnixInputOutputData", "Role", "Ticket"  
"[1/21/2015 10:53:20 AM] 0: /bin/bash ", "<None>", "<None>"  
"[1/21/2015 10:53:23 AM] 1: [maya@firefly-sf Desktop]$  
pwd", "<None>", "<None>"  
"[1/21/2015 10:53:23 AM] K: pwd<CR>", "<None>", "<None>"  
"[1/21/2015 10:53:23 AM] 2:  
/home/maya/Desktop", "<None>", "<None>"  
"[1/21/2015 10:53:34 AM] 3: [maya@firefly-sf Desktop]$ cd  
/tmp", "<None>", "<None>"  
"[1/21/2015 10:53:34 AM] K: cd /tmp<CR>", "<None>", "<None>"  
"[1/21/2015 10:53:54 AM] K: ls -al  
in*<CR>", "<None>", "<None>"  
"[1/21/2015 10:53:54 AM] 4: [maya@firefly-sf tmp]$ ls -al  
in*", "<None>", "<None>"  
"[1/21/2015 10:53:54 AM] 5: -r-xr-xr--. 1 root root 313027  
Dec 16 05:51 install.sh", "<None>", "<None>"  
"[1/21/2015 10:54:04 AM] K: su -<CR>", "<None>", "<None>"  
"[1/21/2015 10:54:04 AM] 6: [maya@firefly-sf tmp]$ su -  
", "<None>", "<None>"  
"[1/21/2015 10:54:10 AM] 7: Password: ", "<None>", "<None>"  
"[1/21/2015 10:54:10 AM] K: xxxxxxxx<CR>", "<None>", "<None>"
```

When you use the /export=UnixInputOutput option, you can also use the command line options /role and /ticket to export sessions based on specific role or trouble-ticket information. For details about using these options, see [Using Find Sessions](#).

## Deleting sessions

You can also use Find Sessions to delete sessions matching the criteria you specify from the command line. You can use the /delete option in combination with other criteria, such as /user or /machine, to delete information for a specific user, computer, or time. However, if you specify the

.....

/delete on the command line, all of the sessions returned by the query are deleted.

To delete sessions from the command line, use the following syntax:

```
FindSessions /i="InstallationName" /delete
```

For example, to delete the sessions for a specific user on a specific computer, you would type a command like this:

```
FindSessions /i="MyInstallation" /user="tai-u1"  
/machine="rhel63" /delete
```

Note that you cannot use the /delete option in combination with the /export option. If you want to export session information before deleting, you must do so in two separate operations.

## Sample script for deleting multiple sessions

You can use Find Sessions to delete multiple sessions manually from the command line or using Windows Task Scheduler to automate the task. However, if you are deleting multiple sessions at once, you might want to execute the command from a batch file to ensure that Find Sessions will wait for the operation to complete and return the result of the operation.

The following is a sample script to delete sessions from TestInstallation recorded in the current month.

```
-----Start of FindSessions_Delete.bat-----  
@ECHO OFF  
cd "C:\Program Files\Centrify\Audit\AuditAnalyzer"  
Start /WAIT FindSessions.exe /i="TestInstallation" /a="1  
time is in this month" /delete  
if ERRORLEVEL 1 (goto FindSessionError)  
goto Succeeded  
:FindSessionError  
echo  
#####  
#####  
echo ## FindSession execution failed. ErrorLevel:  
%ERRORLEVEL% ##  
echo  
#####  
#####  
goto exit
```

.....

```
:Succeeded
echo FindSession execution succeeded.
:exit
-----End of FindSessions_Delete.bat-----
```

You can use a similar batch file if you want to export multiple sessions at the same time. To write a script for exporting information, you would specify the type of information to export and the path for saving the exported output. For example, if you want to export UNIX commands for MyInstallation to the c:\UNIX folder, the script could include a command like this:

```
Start /WAIT FindSessions.exe /i="MyInstallation"
/export="UnixCommand" /path="C:\UNIX"
```

## Find Sessions return codes

For your reference, Find Sessions supports the following return codes to report the status of an operation performed:

This code	Indicates this result
0	The operation was successful.
1	The operation failed because Find Sessions could not parse the Session URI.
2	The operation failed because Find Sessions could not parse the user input.
3	The operation failed because Quick queries are not supported.
4	The operation failed because there were errors in the AQL format.
5	The operation failed because of an incompatible version of AQL was detected.
6	The operation failed because no installation was selected.
7	The operation failed because the installation specified was not found.
8	The operation failed because the AQL string contains the <group by> keyword.
9	The operation failed because no sessions were selected.
10	The operation failed because Find Sessions could not export the list of events.
11	The operation failed because Find Sessions could not export the session list.
12	The operation failed because Find Sessions could not export UNIX input or output.
13	Not all selected sessions were deleted.
14	An unknown error occurred.



## Suppressing warning messages

By default, Find Sessions will generate warning messages if you attempt to export sessions without expected activity. For example, if you run a command to export UNIX input and output using `/export="UnixInputOutput"` and there is no user input activity, you might see warning messages similar to the following:

```
Finished exporting the sessions successfully.  
Warning, URI:rep://BLD08/f435d61c-f191-4344-8adf-  
9d1432cb35ea,  
Message: There is no user inputs captured in this session.
```

You can safely suppress these warning messages using the `/suppresswarning` or `/sw` command line option. For example, you might run a command similar to this:

```
C:\AuditAnalyzer> findsessions /i="BLD08" /role="verify"  
/format=csv /path="C:\Temp" /export="UnixInputOutput"  
/a="1 time is in today" /suppresswarning
```

This command would export the UNIX output without displaying warning messages about there being no user input.