Centrify Infrastructure Services

Evaluation Guide for Windows

November 2018 (release 18.11)

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, Centrify 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 Centrify 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 Centrify 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. Centrify Corporation may make improvements in or changes to the software described in this document at any time.

Portions of Centrify 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.

Centrify, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrify for Mobile, Centrify for SaaS, DirectManage, Centrify Express, DirectManage Express, Centrify Suite, Centrify User Suite, Centrify Identity Service, Centrify Privilege Service and Centrify Server Suite are registered trademarks of Centrify 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.

Centrify 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

The *Evaluation Guide for Windows* describes how to install and configure an environment suitable for evaluating Centrify access and auditing features in a Windows-only environment.

Intended audience

This guide is intended for administrators who are evaluating whether Centrify is an appropriate solution for access control, privilege management, and auditing of user activity on Windows computers. The guide assumes you have a working knowledge of Windows and that you are familiar with how to perform common administrative tasks.

Using this guide

This guide gives you a hands-on experience working with Centrify software on Windows computers. It includes instructions for installing and configuring the software in a standalone environment and step-by-step exercises that lead your through key tasks and their results.

The chapters are organized as follows:

- How Centrify works for Windows introduces the key features you will be evaluating.
- Setting up the evaluation environment describes how to prepare an evaluation environment to for access control, privilege management, and auditing on a Windows client computer.

- Creating and using Centrify roles and desktops provides exercises that show you how to define and validate access control and privilege management using rights and roles.
- Auditing sessions illustrates how you can audit user activity by capturing and reviewing user sessions.

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 at 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 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.

Contacting Centrify

You can contact Centrify by visiting our website, 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.

Setting up the evaluation environment

This chapter describes how to prepare for an evaluation of Centrify Infrastructure Services on a Windows computer. It includes instructions for installing infrastructure services components and the Centrify agent for Windows to enable a full evaluation of access control, privilege management, and auditing on Windows computers.

Installing and configuring infrastructure services requires about a half hour. If you need to install Microsoft SQL Server Express with Advanced Features, which is also included in the package, add another 10 to 15 minutes to the setup.

Preview of the tasks you will perform

You will perform the following tasks to set up the evaluation environment. You should perform the tasks in the order shown to prepare your environment for a meaningful evaluation that demonstrates the key features of the Centrify solution for Windows computers.

1. Ensure you have at least one Active Directory *domain controller* and one Windows *domain computer*—also referred to as the Windows *client computer*.

   See Basic requirements for the evaluation for details about the system requirements for these computers.

2. Acquire Centrify software for the Windows client computer.

   See Request or download Centrify software for details about acquiring Centrify software.

3. On the Active Directory domain controller, create an Active Directory user and group to be used in the evaluation.

   See Create an Active Directory user and group for details about this procedure.

4. Install Access Manager and administrative tools on the Windows client computer.

   See Prepare to evaluate access management for details about installing these features.

5. Use Access Manager to configure Active Directory on the domain controller.

   See Configure Active Directory using Access Manager for details about configuring Active Directory from Access Manager.

6. Use Access Manager to create a Centrify zone.

   See Create the first zone for details about creating a zone.

7. Use Access Manager to assign the Windows Login role to your Active Directory account.

   See Assign yourself the default Windows Login role for details about this procedure.

8. If you are evaluating Centrify auditing features, you need access to an instance of Microsoft SQL Server and an audit installation, which consists of several auditing-specific components.

   See Identify a Microsoft SQL Server instance for details about installing a SQL Server Express instance for demonstration purposes. See Prepare to evaluate auditing for details about installing audit components.

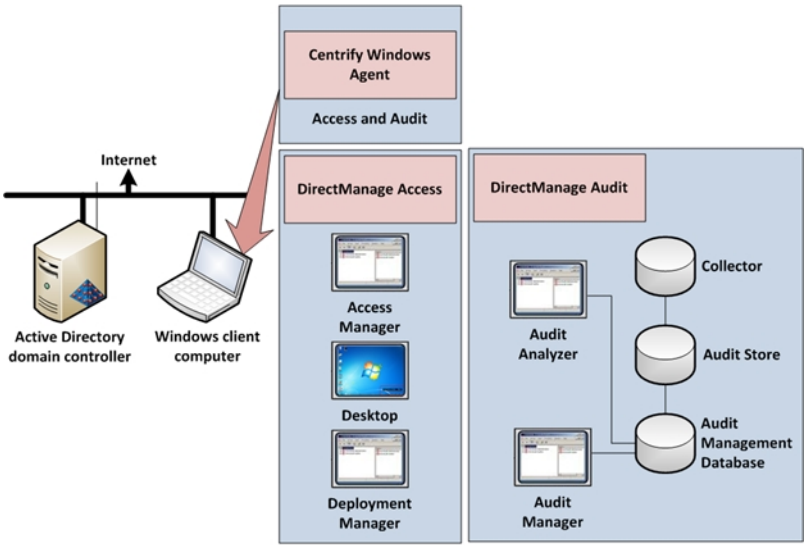
9. Install the Centrify agent for Windows on the Windows client computer.

   See Install the Centrify agent for Windows for details about this procedure.

Basic requirements for the evaluation

The installation procedures described in this guide are based upon a minimal configuration with one Windows Centrify-managed computer (the *Windows*

Active Directory domain controller, as illustrated in the following figure.



You can add more Windows computers to the configuration to expand the scenario or to make the evaluation more consistent with a production deployment.

Prepare an Active Directory domain controller

You must have an Active Directory domain controller to use in this evaluation. You should also have a properly configured Domain Name Service that enables the computers used in the evaluation to communicate. The following table lists the basic Windows Server operating system requirements for the domain controller.

For this	You need this
Active Directory domain controller	▪ Windows Server 2008 R2, ▪ Windows Server 2012, ▪ Windows Server 2012 R2, or ▪ Windows Server 2016

Note In the configuration illustrated, no software is installed on the domain controller. However, you can install all of the software on the domain controller if you choose.

Select a Windows domain computer

The Windows client computer that you use for the evaluation should have a supported Windows operating system and minimum system requirements.

For this	You need this
Windows operating system	Windows 7 or later If you want to use a server platform, you can install components on Windows Server 2008 R2 or Windows Server 2012 R2.
.NET Framework	.NET Framework 4.6.2 or later If .NET is not installed, the Centrify setup program will install it for you.
CPU speed	Minimum 2 GHZ
RAM	4 GB
Disk space	20 GB free space

Desktop rights can be used on Windows servers and workstations that have a traditional Windows desktop. If the computer you are using is running Windows Server 2012 or 2012 R2, Windows does not provide access to applications natively when you switch from the default desktop to a privileged desktop due to changes to the underlying interfaces and supported features within the operating system. To enable access to applications on computers running these versions of Windows, the Centrify agent for Windows provides a custom start menu. The Centrify start menu allows you to open and run applications as you would on Windows 7 or Windows Server 2008 R2. The Centrify start menu is installed on the left side of the taskbar and displays the Centrify logo. This start menu is only available if you are using a role with Centrify desktop rights and cannot be modified.

Centrify also recommends that you install the Microsoft Windows Server Administration Tools Pack on the computer on where you install Access Manager. The Administration Tools Pack includes the Active Directory Users and Computers utility—`dsa.msc`—used in many of the exercises.

If you are using the recommended configuration with a separate Windows client computer that is not the domain controller, be sure that the Windows client computer is joined to the Active Directory domain.

Request or download Centrify software

You can request an evaluation package of Centrify Infrastructure Services to be delivered on a CD or in a compressed file format from the Centrify website. Alternatively, you can download a free trial.

To download Centrify Infrastructure Services trial software:

1. Navigate to https://www.centrify.com/free-trial/.
2. Choose **infrastructure services**, enter company information, click the checkbox for "I am not a robot" and click **Start Trial**.

Note You will receive an email with the next steps in downloading your free trial.

Create an Active Directory user and group

Evaluation scenarios covered in this guide require an Active Directory user with normal user privileges to demonstrate different features. For example, you will create access rights that grant elevated privileges to a role and assign this user to the role to use those rights.

To prepare for the evaluation scenarios:

1. On the Active Directory domain controller, open Active Directory Users and Computers.

   For example, create the user `amy.adams` to represent a domain user with a valid logon account.

2. Select **Action > New > User** and follow the prompts to create a new Active Directory user.
3. Select **Action > New > Group** and follow the prompts to create a new Active Directory group.

   For example, create the group `Eval Group` to represent a typical Active Directory security group to which you would assign a role.

4. Right-click the user name and select **Add to a group** to add the new user

to the new group.

You might also want to add your own Windows account to the new group. Adding your own account to the Evaluation group makes it easier to demonstrate some features, such as assigning roles to group members.

Prepare to evaluate access management

If you are evaluating access control and privilege management features, you must install the administrative tools on the Windows client computer to prepare for the evaluation. Later, you will also install the Centrify agent for Windows on the Windows client computer as described in Install the Centrify agent for Windows.

To install Access Manager from the installer:

1. Log on to the Windows client computer using a Windows account that has Active Directory administrator privileges on the domain controller.
2. From the Centrify CD or directory that has Centrify software, open **autorun**.
3. On the Getting Started page, click **Identity & Privilege** to start the setup program for Centrify Identity & Privilege.
4. Follow the prompts displayed and select Centrify Administration as the components to install.

   For a Windows-only evaluation, none of the Centrify Utilities components are applicable.
5. Accept the defaults for the remaining selections, then click **Finish** to close the setup program.

Configure Active Directory using Access Manager

The setup program adds shortcuts for selected components to your desktop to give you immediate access to the consoles you will use. Before you can use Access Manager to create zones, define access rights and roles, and assign roles to users and groups, however, you use it to run a Setup Wizard that prepares the Active Directory forest with parent containers for licenses and zones.

To use the Setup Wizard to configure Active Directory:

1. From the desktop, open Access Manager.
2. Select **Use currently connected user credentials** to use your current log on account, then click **Next**.
3. Select **Generate Centrify recommended deployment structure** and **Generate default deployment structure**, then click **Next**.
4. Click Browse to select the container you would like to use for the deployment structure.

   You can select any domain in the forest, including the forest root domain.
5. Select a location for installing license keys in Active Directory, then click **Next**.

   The Setup Wizard displays information about the Read permissions that must be granted on the container. Click **Yes** to continue.
6. Type, copy and paste, or import the license key you received, click **Add**, then click **Next**.
7. Click **Next** to use the default container for Centrify zones.
8. Click **Next** to skip the following options:
   - Grant computer accounts permission to update their own account information.
   - Register the administrative notification handler.
   - Activation of Centrify profile property pages.
9. Review the summary, click **Next**, then click **Finish**.

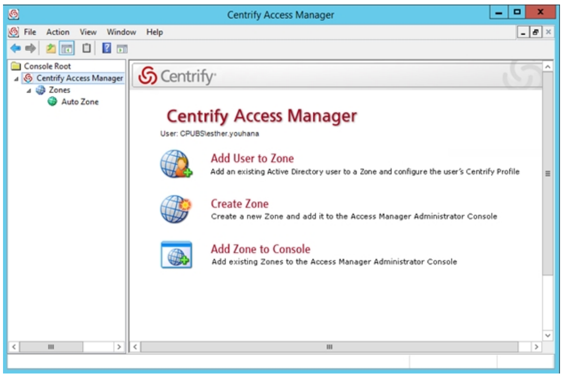
The wizard opens the Access Manager console. For reference, the user account under which you are logged in displays in the main panel just below **Access Manager**.

Create the first zone

In this section, you create a zone for the Windows client computer. After you create the zone, you can start creating access rights, defining roles, and assigning roles to Active Directory users and groups.

To create a new zone:

1. In Access Manager, click **Create Zone**.



Centrify Access Manager

User: CPUBS\esther.youhana

Add User to Zone

Add an existing Active Directory user to a Zone and configure the user's Centrify Profile

Create Zone

Create a new Zone and add it to the Access Manager Administrator Console

Add Zone to Console

Add existing Zones to the Access Manager Administrator Console

2. Type a name and description for the zone, for example `Headquarters`, then click **Next** to accept the defaults for the other fields.
3. Click **Finish**.

You now have one parent zone in Access Manager. Expand **Access Manager > Zones** to view your new zone in the console.

Assign yourself the default Windows Login role

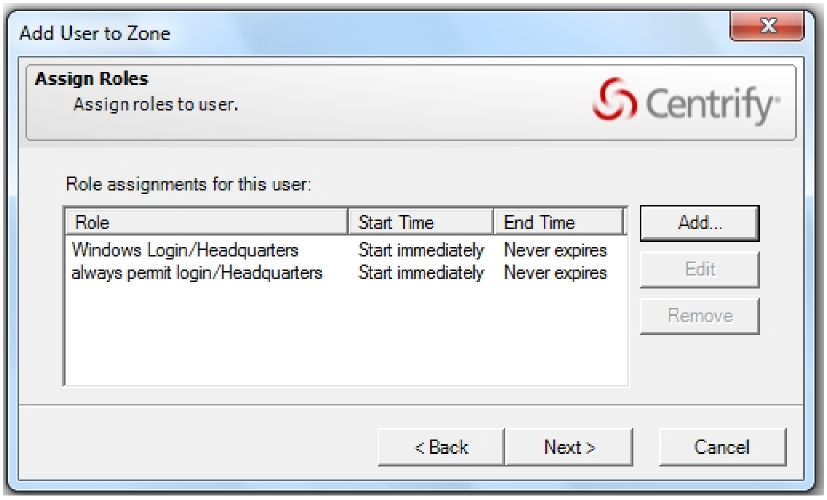
After you install the Centrify agent for Windows, you must be assigned to a role that allows you to log on. To finish the preparation of the evaluation environment for access control and privilege management, you are going to assign a role with the log in privilege to your Active Directory account. The Windows Login role is a predefined role that grants permission to log on locally and connect remotely for Centrify-managed Windows computers.

To assign the Windows Login role to your account:

1. In Access Manager, expand Zones and select the zone you created in Create the first zone.
2. Right-click the zone, and select **Add User**.
3. Select **Active Directory user** and click **Next**.
4. Type the path to your account or click **Browse** to search for and select your Active Directory user account, then click **Next**.

   For example, click Browse and type all or part of the name, then click **Find Now**. You can then select your account name in the list of results and click **OK**.
5. Deselect **Define user UNIX profile** and make sure **Assign roles** is selected, then click **Next**.
6. Click **Add**, select the predefined **Windows Login** role, and click **OK**.
7. Check the role assignment start and end times for your account are set to Start immediately and Never expire, then click **OK**.
8. Repeat Step 6 and Step 7 to add the **Rescue - always permit login** role.

   Your Add User to Zone window should show the following roles:



Add User to Zone

Assign Roles

Assign roles to user.

Role assignments for this user:

Role	Start Time	End Time
Windows Login/Headquarters	Start immediately	Never expires
always permit login/Headquarters	Start immediately	Never expires

9. Click **Next**, then click **Finish**.

If you are evaluating auditing features, go on to Prepare to evaluate auditing. If you are only evaluating access-related features, skip to Install the Centrify agent for Windows.

Prepare to evaluate auditing

If you are evaluating access and auditing features or only auditing, there are several components that make up the auditing infrastructure. For evaluation, you can install all of the components on the same computer.

Identify a Microsoft SQL Server instance

If you are evaluating both access and auditing features or only auditing, you must have at least one Microsoft SQL Server instance for storing audit-related information.

For evaluation purposes, you can use an existing Microsoft SQL Server database instance to which you have administrative access or automatically install and configure an instance of Microsoft SQL Server Express with Advanced features directly from the Centrify Audit Configuration Wizard.

You should only use Microsoft SQL Server Express for evaluation and testing. You should not use Microsoft SQL Server Express for a production environment.

Install auditing components

In this section, you run the Centrify setup program to install the auditing and monitoring components, including the Audit Manager and Audit Analyzer consoles, on the Windows client computer.

To install the Centrify Auditing and Monitoring Service from the installer:

1. Log on to the Windows client computer using a domain account with administrative privileges, such as `DEMO\administrator`. Do not log on as a local user.
2. From the Centrify CD or directory that has Centrify software, open **autorun**.

3. On the Getting Started page, click **Audit & Monitor** to start the setup program for the auditing and monitoring serice.
4. Follow the prompts displayed and select all of the Centrify Administration and Centrify Services components to install, then click **Next**.
5. Accept the defaults for the remaining selections and confirm that the **Launch Configuration Wizard** option is selected, then click **Finish** to close the setup program.

   Note If the **Launch Configuration Wizard** option is not selectable, a possible cause is that you are logged on to the Windows client computer as a local user (for example, local administrator) rather than as a user with domain administrative privileges. In this scenario, select **Start > Switch user** and log on as a Windows domain user with administrative privileges (for example, `DEMO\administrator`). Then launch Audit Manager from the desktop icon, and select **Action > New Installation** to start the audit configuration wizard.
6. In the Welcome page for the audit configuration wizard, click **Next**.
7. Select **Create a new installation** and type a name for your installation, then click **Next** to capture audit trail events without recording video of an audited user’s desktop activity.

   Audit trail events provide a summary of user activity, for example, when users log on and off, open and close applications, and use role assignments with elevated rights. If you want to be able to review what was displayed on the screen during an audited user’s session, you can select **Enable video capture auditing of user activity**. This option increases the database storage required for auditing.
8. Select **Install a new SQL Server Express instance on this computer** and specify the instance name, then click **Next**.
9. Verify the default path to the Microsoft SQL Server Express setup program, the disk space requirements, and the location for the files, then click **Next**.

   Note If an incompatible instance of SQL Server Express is already installed, the wizard displays an error message instructing you to uninstall that instance. Use the Windows control panel to

Note uninstall the incompatible instance of SQL Server Express, and then try the SQL Server Express installation from the wizard again.

10. Review the summary, then click **Finish**.

The audit configuration wizard automatically configures the audit store scope, audit store database, and a collector on the local computer. After the auditing infrastructure is in place, you can install the Centrify Agent for Windows and join the computer to the zone you created.

Install the Centrify agent for Windows

You are now ready to install the Centrify Agent for Windows client computer to begin the evaluation. In a production environment, you would install the agent on all of the Windows computers in the domain that you want to manage or audit.

Note The following instructions assume you are still logged in with your administrator account. Be sure that this account has at least the `Windows Login` and `Rescue - always permit login` roles assigned as described in Assign yourself the default Windows Login role to ensure you can log on after the agent is installed. If the account you are using to install the agent does not have the Windows Login role assigned, the agent configuration wizard will allow you to assign the Windows Login role to the domain administrators (Domain Admins) group when you join a zone.

1. If the Getting Started window is not open on your screen, open your Centrify folder and launch **autorun**.
2. Click **Agent**.
3. Follow the prompts displayed to accept the license agreement and install both Access and Audit features.
4. Review the page whose title begins "Ready to install Centrify Agent for Windows", then click **Install**.
5. Click **Finish** to proceed to the agent configuration.
6. Select the installation you created in Prepare to evaluate auditing as the **Installation name**. then click **Next**.

7. Select the zone you created in Create the first zone.
8. Click **Finish**.

You must restart the computer after you configure the Centrify Privilege Elevation Service. When prompted, click **Yes** to restart the computer immediately.

After you restart the computer, log on with your administrator account. Left-click on the Centrify icon on your taskbar to confirm that you are viewing your default desktop. In the next chapter, you will see how to configure access rights and roles and how to select from roles you are assigned.

How Centrify works for Windows

This chapter introduces core concepts and features that you should be familiar with before starting an evaluation of Centrify software for managing Windows computers.

This chapter includes the following topics:

- Providing access control and accountability
- Organizing computers and access rights
- Restricting access to administrative privileges
- Auditing user activity on a managed computer

Providing access control and accountability

In many organizations, most computer users are given very restricted access privileges to minimize the exposure of sensitive services and data to possible compromise. However, there are often a few applications, procedures, or services that require enhanced privileges and to which these users need access. For example, a user might occasionally have to install software or run a restricted internal application. For this purpose, these organizations often provide these users with login information for accounts with enhanced privileges. Unfortunately, this policy substantially undermines security, because there’s no way to tell—even on an audited system—who actually logged on to these accounts, and once logged on, a malicious user is not restricted to the procedures for which he was given the login information in the first place.

Centrify solves this problem by enabling you to assign roles that give a user access to only those services or applications and restricted access privileges only when the user needs them.

For Windows computers, Centrify provides three main services: access control, privilege management, and auditing. These services can be used together or independently.

To provide access control, privilege management, and auditing for Windows computers, Centrify relies on the following:

- **Centrify Authentication Service** and **Centrify Privilege Elevation Service** features enable you to define access control privileges, create roles composed of a set of privileges, and assign users or groups to those roles. You can also use Centrify zone technology to limit the scope of a role to limited sets of computers. You can, also, configure roles with start and expiration dates or to be active on specific days of the week and hours of the day.
- **Centrify Auditing and Monitoring Service** enables you to collect and store an audit trail of user activity and provides a console for searching and replaying captured sessions.
- **Centrify agent for Windows** enables you to deploy access and auditing features on the Windows computers you want to manage.

You can use Centrify Privilege Elevation Service without auditing if you aren't interested in collecting and storing information about session activities. You can also deploy infrastructure services without access and privilege management features if you are only interested in auditing activity on Windows computers. However, the real value of Centrify software for Windows computers comes from using the services together as an integrated solution for managing elevated privileges and ensuring regulatory compliance across all platforms in your organization. That way you can restrict access to only those instances when elevated permissions are absolutely necessary, and audit only user activity that merits auditing.

Organizing computers and access rights

This guide is intended to help you evaluate how you can use Centrify software to manage access and administrative privileges for Windows computers and applications. However, Centrify also enables you to include UNIX, Linux, and

Mac OS X computers in Active Directory, providing you with a single repository for all managed computers, users, privileges, and roles. Centrify enables this cross-platform integration through the use of **Centrify zones**.

A Centrify zone is a logical object that you create using Access Manager. You use the zone to organize computers, rights, and roles into groups. In each group, you can define different access rights, different role availability rules, and different role assignments. You can create the zones in a hierarchy of parent and child zones, so that rights and roles can inherited or zone-specific.

As part of the evaluation, you will create a Centrify zone for the Windows computers, define access rights that are specifically for Windows computers, create roles that include those access rights, and assign roles to users and groups.

Restricting access to administrative privileges

By defining roles with specific access permissions, you can use Access Manager to specify the conditions under which users can perform privileged operations. A user logs on to the Windows computer with his or her normal, restricted login, and then selects the role they need to perform a privileged operation only when that access is needed. You can restrict a role or desktop to certain times or days of the week, and you can set a beginning and expiration date for the access. You can set any role or desktop to require auditing, so that the user cannot use the role or desktop unless it is being audited.

Access Manager provides three kinds of Windows access rights. For Windows computers, these specialized access rights are:

- **Desktop** access rights enable you to create additional working environments and run any application in that desktop as a member of Active Directory or built-in group.
- **Application** access rights enable you to run a specific local application as another user or as a member of an Active Directory or built-in group. This access right is similar to the standard **Run as** menu option, except that someone assigned a role with this right doesn't need to know the privileged user's password to use it.
- **Network** access rights enable you to connect to a remote computer as another user or as a member of an Active Directory or built-in group to

perform operations, such as start and stop services, that require administrative privileges on the remote computer.

You configure these access rights using the Access Manager console. The rights are enforced through a Centrify agent for Windows installed on each computer you want to manage.

Auditing user activity on a managed computer

When you install the Centrify agent for Windows on a computer, you have the option to enable access management, auditing, or both. If you enable auditing features, the agent can capture detailed information about user activity and all of the events that occurred in each user session on the managed computer. The user activity captured includes an audit trail of the actions a user has taken and a video record of everything displayed on the screen. For users who have privileged access to computers and applications, the auditing and monitoring service helps ensure accountability and improve regulatory compliance. By recording user sessions, you can see exactly who had access to which computers and what they did, including any changes they made to key files or configurations.

The auditing and monitoring service collects user activity as it occurs. The recorded activity is transferred to a Microsoft SQL Server database so that it is available for querying and playback. You can search the stored user sessions to look for policy violations, user errors, or malicious activity.

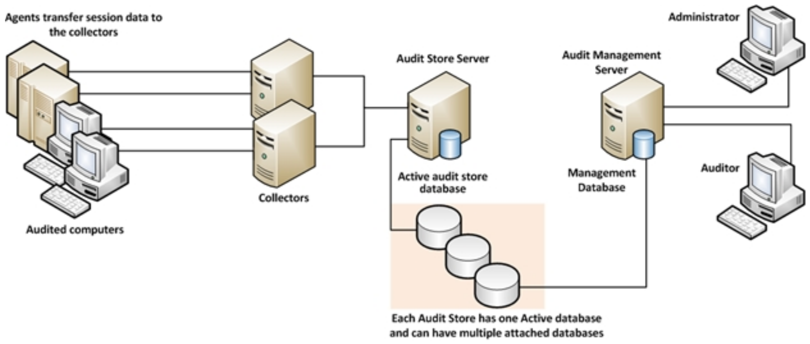
To ensure scalability and enterprise readiness, the auditing infrastructure consists of multiple components called a **auditing and monitoring service installation**:

- **Audited computers** are the computers on which you want to monitor activity. To be audited, the computer must have the Centrify agent for Windows installed with auditing enabled and be joined to an Active Directory domain.
- One or more **collectors** receive the captured activity from the agents on audited computers and forward it to an audit store database.
- An **audit store** defines a scope, such as an Active Directory site or a subnet, and one or more databases that store captured activity and audit trail records from the collectors and store it for querying.

- A **management database** keeps track of all the agents, collectors, and audit stores that make up a single DirectAudit installation.
- **Consoles** enable administrators to configure and manage all of the audit-related components and auditors to query and review user sessions.

When you enable auditing on a computer with the Centrify agent for Windows, the agent captures user activity on that computer and forwards it to a collector computer. If no collectors are available, the agent caches the session data locally and transfers it to a collector later. The collector sends the data to an audit store database. When administrators or auditors want to review the captured data, they use the Audit Analyzer to search for and play back the session. The Audit Analyzer connects to the management database which retrieves the data from the appropriate audit store. The administrator can control the audit data available to any specific user or group through auditor roles that limit audit access rights and privileges.

The following figure illustrates the basic architecture and workflow in a small scale installation.


Agents transfer session data to the collectors
Audited computers
Collectors
Audit Store Server
Active audit store database
Each Audit Store has one Active database and can have multiple attached databases
Audit Management Server
Management Database
Administrator
Auditor

Creating and using Centrify roles and desktops

At the end of the last chapter, you restarted the Windows client computer and logged in with your administrator account.

This chapter describes how to define access rights and create roles that grant elevated privileges, assign roles to users and groups, and view details about the rights and roles available. This chapter also shows you how to select and switch between roles for running local applications and connecting to network computers.

The following topics are covered:

- Verify your account is assigned basic login rights
- Assign the Windows Login role to a group
- Add predefined rights to a zone
- Create an application right
- Create a desktop right
- Create a network right
- Review rights and roles in the Authorization Center

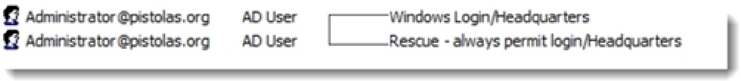
Verify your account is assigned basic login rights

At this point, you should be logged on to the Windows client computer with an administrator account that has been assigned the “Windows Login” and “Rescue - always permit login role” predefined roles as described in Assign yourself the default Windows Login role. Because the client computer has Access Manager and the Centrify agent for Windows installed, you can verify that your account has been assigned these predefined roles using Access Manager or the Authorization Center.

To use Access Manager to verify your assigned roles:

1. Expand Zones and the zone you created in Create the first zone.
2. Expand Authorization and select Role Assignments.

   In the right pane, you should see your role assignments displayed similar to this:



```
Administrator@pistolas.org   AD User   Windows Login/Headquarters
Administrator@pistolas.org   AD User   Rescue - always permit login/Headquarters
```

In this example, the Windows Login and Rescue roles are assigned to the Administrator account in the zone named Headquarters

Assign the Windows Login role to a group

After a computer joins a Centrify zone, users must be granted access to that computer by being assigned a role with the right to log on. So far, only the Administrator account has that privilege. This exercise illustrates how you can give that privilege to other users through their Active Directory group membership.

In most cases, you can assign the Windows Login role to all local Windows users, all Active Directory users, or both, if you want to automatically allow new users to log on locally or remotely. However, the Window Login role does not override any native Windows security policies. For example, if the Local Security Policy on the domain controller does not allow Domain Users to log on locally, assigning the Windows Login role to the Domain Users security group will not allow members of that group to log on locally.

If the Windows client computer you are using for the evaluation does not allow users to log on locally or does not accept remote desktop connections, you might have to make `Eval Group` a member of a specific Windows security group, such as Server Operators or Remote Desktop Users, to complete further exercises.

. . . . . .

To assign the Windows Login role to an Active Directory group:

1. On the Window client computer, open Access Manager.
2. Expand the zone, then expand Authorization.
3. Right-click **Role Assignments** and select **Assign Role**.
4. Select **Windows Login** from the list of role definitions, then click **OK** to display Assign Role.

   By default the role is set to start immediately and never expire.
5. Select **Accounts below** to assign the role to the group you created in Create an Active Directory user and group.

   For purposes outside of this exercise, you could assign the role to more users by selecting **All accounts** and then specifying **All Active Directory** accounts, **All local Windows accounts**, **All local UNIX accounts**, or any combination of these three selections.
6. Click **Add AD Account** to display Add User Role Assignment.
7. Change the **Find** filter from **User** to **Group**.
8. Type all or part of the group name, click **Find Now**, then select the group in the results and click **OK**.

   For example, type `Eval` to search for `Eval Group` and select that group in the results.
9. Click **OK** to complete the assignment and close the Assign Role window.

   Now all members of `Eval Group` can log on to this computer.

To verify the role assignment, you can log off as the administrator and log in as the user you created in Create an Active Directory user and group, for example, `amy.adams`. When you log on using the new account, the default desktop has no administrative privileges. For example, the new user cannot stop or start services on the local computers because the account do not have the administrative privileges required to do so. The next exercise shows you how to give a user elevated privileges when she is running a specific application.

Add predefined rights to a zone

There are many predefined rights available that grant access to specific Windows applications. For example, there is a predefined Performance Monitor right that allows you to run Performance Monitor on a computer without being a local administrator or knowing an administrative password.

You can add any or all of these predefined rights to any zone so they are available to include in role definitions. Alternatively, you can add predefined rights to individual role definitions without adding them to zones. In either case, you create grant predefined rights in the context of a role definition.

To add predefined rights to a zone and the Windows Login role:

1. On the Windows client computer, open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone (for example, Headquarters) where you want to add predefined rights.
3. Expand **Authorization > Role Definitions**.
4. Select the Windows Login role definition, right-click, then select **Add Right**.
5. Select **Any Windows Rights** from the Type list to filter the list of rights displayed.
6. Select the Headquarters zone from the list of zones, and then click **Create Predefined Rights**.

   The list of predefined rights that you can add to the Headquarters zone and to the Windows Login role is displayed. In the next steps, you will select which rights to add to the Headquarters zone. From the rights that you add to the Headquarters zone, you will select which, if any, to also add to the Windows Login role.
7. From the list of predefined rights, select the rights that you want to add to the Headquarters zone and to the Windows Login role, and then click **OK**.

   By default, all of the predefined rights that you select will be added to the Headquarters zone and to the Windows Login role. In the next step, you will deselect rights so that they are added only to the zone and not to the role.

8. Deselect predefined rights that you do not want to add to the Windows Login role.

   Rights that you deselect are added only to the Headquarters zone. Rights that you leave selected are added to both the Headquarters zone and the Windows Login role.

9. Click **OK** to add the predefined rights to the zone, role, or both according to your selections in Step 8.

   If you deselected all available predefined rights, the **OK** button is not available to click. In this scenario, click **Cancel** to add the rights to the zone without adding them to the role definition.

   After you perform this step, the predefined rights that you deselected are not added to the Windows Login role, but are added to the Headquarters zone so that they can be added later to roles in the zone as needed.

You can click **Refresh** in Access Manager to see the predefined rights listed as Windows application rights.

Create an application right

An application right lets you run a specific application as a different user. An administrator assigns an application right rather than a desktop right when the user needs only occasional administrative responsibilities for a specific application and needs only temporary or infrequent use of the elevated privileges. (Desktop rights provide administrative access to more than a single application at a time. See Create a desktop right for details about desktop rights.)

If you have completed the exercises in the previous sections, you are ready to create your first application right. If you have not completed all of the exercises to this point, you might not be able to perform all of the following exercises successfully.

In the following exercises, you will:

- Verify the Active Directory domain user `amy.adams` does not have permission to use the Windows Control Panel to change security settings.
- Configure a new application right that gives administrative privileges for the Control Panel application.
- Define a new role that uses the application right.
- Assign the role definition that includes the Control Panel application right to the Active Directory domain user `amy.adams`.
- Verify that the role assignment grants the user `amy.adams` the right to change a setting in Control Panel.

To verify the user does not have administrative privileges for the Control Panel:

1. On the Windows client computer, log on as the `amy.adams` domain user account.
2. Use Windows Explorer to open the `C:\Windows\System32` folder.
3. Create a shortcut for the `control.exe` program on the desktop.
4. Use the shortcut to open the Control Panel, select System and Security, then open **Allow a program through Windows Firewall**.

   Notice that you cannot make changes to the list of Allowed programs and features. If you click Change Settings, you are prompted to enter an administrator account name and password.
5. Click **Cancel** to close **Allow programs to communicate through Windows Firewall** and close the Control Panel.
6. Log off as `amy.adams` and log on with your administrator account.

To create a new application right for the Control Panel:

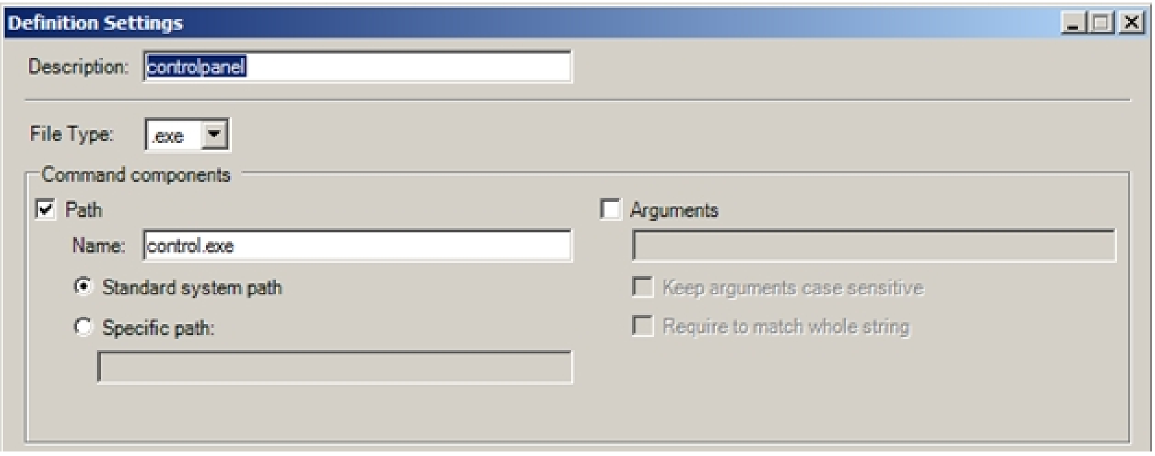
1. On the Windows client computer, open Access Manager and expand to display **Authorization > Windows Right Definitions**.
2. Select **Applications**, right-click, then select **New Windows Application**.
3. On the General tab, type `Control Panel Right` for the name of this application right and an optional description.

4. Click the Match Criteria tab, then click **Add**.

   In the Match Criteria tab, you specify one or more application executable files to be included in this application right. You can specify application executable files in many ways. The capability to specify more than one executable file in a single application right takes into account situations in which one application might reside in different locations on different computers. For details about different ways of specifying executable files, see the “Defining desktop application rights” help topic in the Access Manager online help.

   In this example, you will specify one application executable file using the application executable name and path.

5. Type a name for the criteria definition, select **Path**, then type the application executable name `control.exe` to specify the Windows Control Panel as the application to which this right grants access. For example:



Definition Settings

Description: controlpanel

File Type: .exe

Command components

☑ Path

Name: control.exe

● Standard system path

○ Specific path:

□ Arguments

□ Keep arguments case sensitive

□ Require to match whole string

6. Click **OK** to use the default standard system path for the application without specifying any other criteria.

7. Click the **Run As** tab, select **Self with added group privileges**, then click **Add Built-in Groups** to select the administrative group to use.

   For the evaluation, you should use a built-in group to avoid adding test users and groups to your Active Directory environment. Alternatively, you could specify an existing user account, create a new user account for this right, or select **Self with added group privileges**, then click **Add AD Groups** to search for and select a previously-defined Active Directory group with administrative privileges.

8. Select the **Administrators** group, then click **OK**.

9. Select **Re-authenticate current user** to require users to authenticate their identity when they use a role with this right.
10. Select **Require multi-factor authentication** If you would like to enable multi-factor authentication for the right.

    Before you enable multi-factor authentication, you should be aware that multi-factor authentication for Centrify-managed Windows computers relies on the infrastructure provided byCentrify Identity Services. For more information on preparing to use multi-factor authentication, see the *Multi-factor Authentication Quick Start Guide*.
11. Click **OK** again to complete the definition of the application right.

    The new application right is now defined. Next you must create a new role definition to use the application right.
12. To update the list of application rights in Access Manager so that you can review the new application right, select **Action > Refresh**.

To define a new role with an application right for the Control Panel:

1. Select **Role Definitions**, right-click, then select **Add Role**.
2. In the General tab, type `ControlPanelAdmin` as the name of the new role.

   Do not change the default settings for the System Rights tab and the Audit tab.
3. Click **OK**.

   The new role definition is created, but the role does not have any rights yet.
4. Select the `ControlPanelAdmin` role listed under **Role Definitions**, right-click, then select **Add Right**.
5. Select **Control Panel Right** in the list of rights, then click **OK**.

   You can filter the list of rights. For example, you can filter rights by name, type, zone, or description. After you select the right and click OK, the role definition has one right. You can add other rights to it. After you have identified all of the access rights for the role definition, you can assign the role to a user or group.

To assign the role definition with the application right to a

user or group:

1. Select **Role Assignments**, right-click, then select **Assign Role**.
2. Select `ControlPanelAdmin` in the list of role definitions, then click **OK** to display **Assign Role**.
3. Click **Add AD Account** to search for and select the user `amy.adams`, then click **OK**.
4. Select **Role Assignments** to see that the user `amy.adams` is assigned the Windows Login and ControlPanelAdmin roles.
5. Open the **Privilege Elevation Service Settings** (from the Agent Configuration shortcut > Centrify Privilege Elevation Service > Settings), click the **Troubleshooting** tab, then click **Refresh** to force the agent to get the latest authorization information without waiting for the cache to expire.

To verify the user has administrative privileges for the Control Panel:

1. Log off as the administrator and log in as `amy.adams`.
2. Right-click the `control.exe` shortcut on the desktop.

   If you want to open an application from the Start menu, press the Shift key when you right-click.
3. Select **Run with Privilege**.

   Selecting **Run with Privilege** is similar to selecting standard Windows “Run as” or “Run as administrator” menu items, but does not require you to provide a password for an administrative or shared service account. Instead, you always use your own password to authenticate your identity.
4. Select `ControlPanelAdmin` in the list of the roles available, then click **OK**.
5. Type the password for the `amy.adams` login account, then click **OK**.
6. Select System and Security, then open **Allow a program through Windows Firewall**.

   Notice that you can now make changes to the list of programs allowed through the firewall.

This section showed you how to set up a role that allows privilege escalation for a single application and how the user can select that role to run the application with privileges without knowing the administrator's user name or password.

Create a desktop right

In the preceding section, you saw how to elevate privileges by creating an application right for a specific application. To grant administrative access to more than a single application at a time, you can allow users to open a desktop that has administrative privileges.

If you have completed the exercises in the previous sections, you are ready to create your first desktop right. If you have not completed all of the exercises to this point, you might not be able to perform the following exercise successfully.

In the next exercise, you will create a desktop access right, create a new role, assign the desktop right to the new role, and assign the role to `Eval Group`. At the end of this exercise, you will use the desktop right to modify a restricted folder. The steps in this exercise are similar to the steps that you performed in the preceding exercise to create an application right.

To create a role definition with a desktop access right:

1. Log on with your administrator account and open Access Manager.
2. Create the new desktop right.
    - Select **Windows Right Definitions > Desktops**, right-click, then select **New Windows Desktop**.
    - Type `DesktopRight` as the name of the new desktop right on the General tab.
    - Click the **Run As** tab, then click **Add Built-in Groups**.
    - Select the **Administrators** group, then click **OK**.
    - Select **Re-authenticate current user** to require users to authenticate their identity when they use a role with this right, then click **OK**.

- Select **Require multi-factor authentication** If you would like to enable multi-factor authentication for the right.

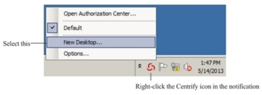
Before you enable multi-factor authentication, you should be aware that multi-factor authentication for Centrify-managed Windows computers relies on the infrastructure provided by Centrify Identity Services. For more information on preparing to use multi-factor authentication, see the *Multi-factor Authentication Quick Start Guide*.

3. Create a new role definition.
   - Select **Role Definitions**, right-click, then select **Add Role**.
   - Type `DesktopAdmin` as the name of the new role on the General tab.
   - Click **OK**.
4. Add the desktop right to the new role.
   - Select **Role Definitions**, right-click the `DesktopAdmin` role, and select **Add Right**.
   - Select `DesktopRight` and click **OK**.
5. Assign the role to a group.
   - Select **Role Assignments**, right-click, then select **Assign Role**.
   - Select `DesktopAdmin` from the list and click **OK** to display **Assign Role**.
   - Click **Add AD Account**.
   - Change the **Find** filter from User to Group.
   - Search for and select the group you created for the evaluation (for example, `Eval Group`), then click **OK**.
   - Verify that the account is included in the Accounts list in the Assign Roles dialog box, then click **OK**.
   - Open the **Privilege Elevation Service Settings** (from the Agent Configuration shortcut > Centrify Privilege Elevation Service > Settings), click the Troubleshooting tab, then click **Refresh** to get the latest authorization information.

To verify that the role with desktop rights grants elevated privileges:

1. Log off as the administrator and log on as `amy.adams`.
2. Open Windows Explorer and go to the `C:\Windows` folder.
3. Try to create a new folder in this location.

   From the default desktop for this account, the user does not have the necessary privileges to create a new folder. The only way she can create a new folder is by using administrator credentials.
4. Click the carat in the system tray notification area to display hidden icons, then click the Centrify icon to display the applet options.
5. Select **New Desktop**.

   
   Open Authorization Center...
Default
New Desktop...
Options...
Select this
1:47 PM
5/14/2013
Right-click the Centrify icon in the notification
6. Select the `DesktopAdmin` role, then click **OK**.
7. Type the password for the logon account, then click **OK**.

   Notice that your new role is displayed when you left click on the Centrify icon in your task bar.
8. Try to create a new folder in the `C:\Windows` directory.

   Now you can create a new folder because the desktop that you are using has all of the rights associated with the Administrators group.

Note On Windows 10 and Windows Server 2016 systems, task bar menus are not available in an Elevated Desktop.

In this exercise, you created a role with the right to create a desktop with administrator privileges. You found that opening a new desktop with that role allowed you to perform administrative functions using your own credentials.

Switching between active desktops

You can have multiple desktops available for you to use. For example, you might have separate desktop roles for managing Exchange and SQL Server that grant different rights. After you create a desktop for each role, you can switch between desktops by clicking the Centrify icon, then selecting the desktop you want to use. You can also set up hot keys to switch between desktops using a keystroke combination.

When you are finished working with a desktop, you can click the Centrify icon, then select **Close Desktop**.

Create a network right

In the preceding section, you saw how you can provide a user with a desktop that has elevated privileges on a local computer (the Windows client computer in this case). However, using administrative privileges on your local Windows client computer does not give you privileges on a remote computer. In this section, you create a network access right that gives a user administrator privileges on a remote computer.

To illustrate network access rights using the local Windows client computer and a remote computer, you must install the Centrify agent for Windows on the remote computer and join that remote computer to the zone you created in Create the first zone (for example, Headquarters).

You can use the domain controller or another computer as the remote computer for this exercise. Install the Centrify agent for Windows on the computer that you are using as the remote computer and join that computer to the Headquarters zone before proceeding.

If you are using only one Windows client computer for the evaluation and cannot install the agent on the domain controller or another remote computer, you should skip this exercise.

To prepare for the exercise that demonstrates this feature:

1. Install the Centrify agent for Windows on the computer that you are using as the remote computer.

   See Install the Centrify agent for Windows for more information.

2. Log on to the remote computer with your administrator account and create a folder on the C: drive named `ShareFolder`.
3. Select the folder, right-click, then select **Properties**.
4. Click the **Sharing** tab, then click **Share**.
5. Select Find people, type “back” to search for and select the built-in Backup Operators group, then click **OK**.
6. Right-click the Backup Operators group and set the Permission Level to

Read/Write, then click **Share**.

7. Click **Done**, click **Close** to exit, then log off the remote computer as the administrator.
8. Log on to the local Windows client computer as `amy.adams`.
9. Try to open `ShareFolder` on the remote computer.
10. Verify that Windows tells you that you do not have sufficient permissions, then click **Cancel**.

To create a network access right and add it to the DesktopAdmin role:

1. Log on to the local Windows client computer with your administrator account and open Access Manager.
2. Create the new network access right.
    - Select **Windows Right Definitions > Network Access**, right-click, then select **New Network Access**.
    - Type `ShareAccess` as the name of the new access right on the **General** tab.
    - Click the **Access** tab, select **Self with added group privileges**, then click **Add Built-in Groups**.
    - Select the **Backup Operators** group, then click **OK**.
    - Select **Re-authenticate current user** to require users to authenticate their identity when they use a role with this right, then click **OK**.
    - Select **Require multi-factor authentication** If you would like to enable multi-factor authentication for the right.

    Before you enable multi-factor authentication, you should be aware that multi-factor authentication for Centrify-managed Windows computers relies on the infrastructure provided by the Centrify identity platform and the cloud-based Centrify Identity Services. For more information on preparing to use multi-factor authentication, see the *Multi-factor Authentication Quick Start Guide*.
3. Add the new right to the existing `DesktopAdmin` role.

- Under **Role Definitions**, select the `DesktopAdmin` role, right-click, then select **Add Right**.
- Select the **ShareAccess** right in the list, then click **OK**.

4. Assign the role to a selected computer in the zone.

    - Expand the zone to **Computers > computer name> Role Assignments** node. If you are using a local and remote computer for this exercise, select the remote computer for making the role assignment.
    - Select **Role Assignments**, right-click, then select **Assign Role**.
    - Select `DesktopAdmin` in the list of roles, then click **OK**.

5. Assign the role to an Active Directory group.

    - Click **Add AD Account**.
    - Change the **Find** filter from User to Group to search for and select the group you created for the evaluation (for example, `Eval Group`), then click **OK**.
    - Verify that the account is included in the Accounts list in the Assign Roles dialog box, then click **OK**.
    - Open the **Privilege Elevation Service Settings** (from the Agent Configuration shortcut > Centrify Privilege Elevation Service > Settings), click the Troubleshooting tab, then click **Refresh** to get the latest authorization information.

To verify the role with network access rights grants elevated privileges:

1. Log on to the local Windows client computer as `amy.adams`.

    If you try to open `ShareFolder` in the default desktop, Windows denies access.

2. Open the Centrify applet, select **New Desktop**, and select the `DesktopAdmin` role.

    This role has the network access right that gives you remote access to the computer running as the account with Read/Write permission.

3. Open `ShareFolder` and verify that Windows gives you access.

In this exercise, you added a remote access right to a role that already had a desktop right and saw how changing desktops changes the user’s rights.

Review rights and roles in the Authorization Center

The Authorization Center is an option available from the Centrify applet menu. You can use the Authorization Center to display detailed information about your currently available rights and role assignments.

To view the Authorization Center:

1. Click the Centrify icon in the notification area.
2. Select **Open Authorization Center**.
3. Click through the tabs to view detailed information about your rights, roles, role assignments, and auditing status.

Auditing sessions

If you have completed all the steps in the preceding chapters, the auditing and monitoring service has been auditing your sessions as an administrator and the user account you created. This chapter describes how to view audited sessions, update the review status, and use queries to find the sessions in which you’re interested.

The topics are presented in the following order:

- Using Audit Analyzer to replay a session
- Marking sessions for review or action
- Using the indexed event list
- Creating custom queries
- Creating a quick query
- Auditing only specific events
- Additional auditing tools

Using Audit Analyzer to replay a session

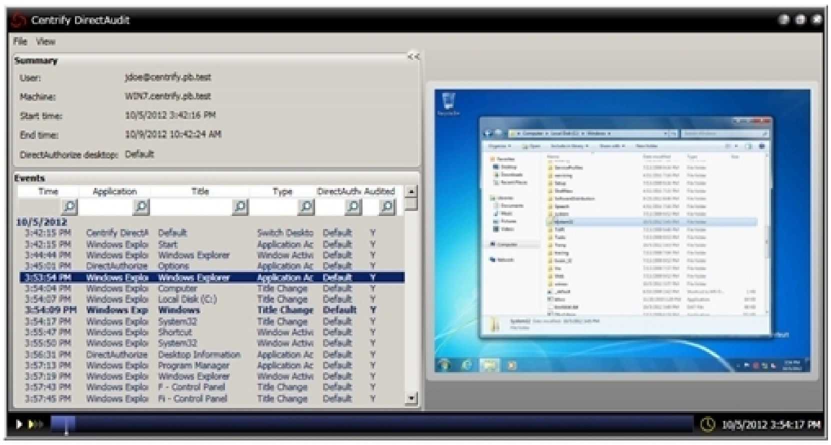
If you selected both Centrify Privilege Elevation Service and Centrify Auditing and Monitoring Service features, the Centrify agent for Windows has been capturing your activity as you logged on and off and switched between roles. You can replay those recorded sessions to see detailed information about what you did during the evaluation. Before you can replay the sessions captured, however, you use Audit Analyzer to locate the sessions you are interested in using a set of predefined queries. For example, there are predefined queries for sessions that started Today and This Month and sessions where the Windows Command Prompt or Windows MMC tools were used.

To select and replay a session:

1. Open Centrify Audit Analyzer to view captured sessions grouped by predefined queries.
2. Select a predefined query, such as **Today** or **Active Sessions**, in the left pane to display a list of sessions in the right pane.

   Note that the date queries show sessions that started during the specified time interval. If a session started three days ago and is still active, it is listed under This Week and Active Sessions, but not under Today or Yesterday.
3. Double-click a session to retrieve the session from the database and open the session replay window.

   The session replay window displays information similar to the following:



Click an Event in the list to go directly to that activity

Summary

User: jdoe@centrify.pb.test

Machine: WIN7.centrify.pb.test

Start time: 10/5/2012 3:42:16 PM

End time: 10/9/2012 10:42:24 AM

DirectAuthorize desktop: Default

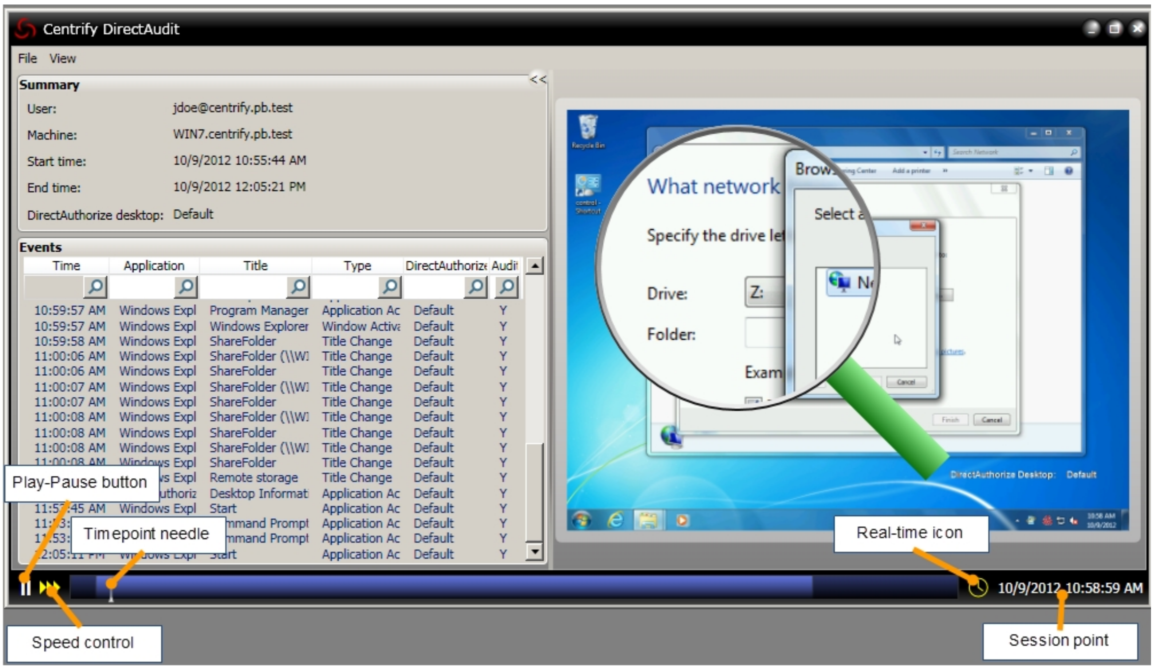
Events

Time	Application	Title	Type	DirectAuth	Audited
10/5/2012					
3:42:15 PM	Centrify DirectA	Default	Switch Deskto	Default	Y
3:42:15 PM	Windows Explo	Start	Application Ac	Default	Y
3:44:44 PM	Windows Explo	Windows Explorer	Window Activ	Default	Y
3:45:01 PM	DirectAuthorize	Options	Application Ac	Default	Y
3:53:54 PM	Windows Explo	Windows Explorer	Application Ac	Default	Y
3:54:04 PM	Windows Explo	Computer	Title Change	Default	Y
3:54:07 PM	Windows Explo	Local Disk (C:)	Title Change	Default	Y
3:54:09 PM	**Windows Exp**	**Windows**	**Title Change**	**Default**	**Y**
3:54:17 PM	Windows Explo	System32	Title Change	Default	Y
3:55:47 PM	Windows Explo	Shortcut	Window Activ	Default	Y
3:55:50 PM	Windows Explo	System32	Window Activ	Default	Y
3:56:31 PM	DirectAuthorize	Desktop Information	Application Ac	Default	Y
3:57:13 PM	Windows Explo	Program Manager	Application Ac	Default	Y
3:57:19 PM	Windows Explo	Windows Explorer	Window Activ	Default	Y
3:57:43 PM	Windows Explo	F - Control Panel	Title Change	Default	Y
3:57:45 PM	Windows Explo	Fi - Control Panel	Title Change	Default	Y

   The replay progress is shown in the play bar along the bottom of the window. If you double-click an event, you can watch the recording of just that event.

Magnifying the recorded session

You can click the magnifier in the replay window to enlarge a portion of the recorded screen. The magnifier appears as a magnifying-glass pointer in the replay pane. Click to toggle the magnifier on or off.



Centrify DirectAudit

Summary

User: jdoe@centrify.pb.test

Machine: WIN7.centrify.pb.test

Start time: 10/9/2012 10:55:44 AM

End time: 10/9/2012 12:05:21 PM

DirectAuthorize desktop: Default

Events

Time	Application	Title	Type	DirectAuthoriz	Audi
10:59:57 AM	Windows Expl	Program Manager	Application Ac	Default	Y
10:59:57 AM	Windows Expl	Windows Explorer	Window Activ	Default	Y
10:59:58 AM	Windows Expl	ShareFolder	Title Change	Default	Y
11:00:06 AM	Windows Expl	ShareFolder (\\WI	Title Change	Default	Y
11:00:06 AM	Windows Expl	ShareFolder	Title Change	Default	Y
11:00:07 AM	Windows Expl	ShareFolder (\\WI	Title Change	Default	Y
11:00:07 AM	Windows Expl	ShareFolder	Title Change	Default	Y
11:00:08 AM	Windows Expl	ShareFolder (\\WI	Title Change	Default	Y
11:00:08 AM	Windows Expl	ShareFolder	Title Change	Default	Y
11:00:08 AM	Windows Expl	ShareFolder (\\WI	Title Change	Default	Y
11:00:08 AM	Windows Expl	ShareFolder	Title Change	Default	Y
[illegible]	s Expl	Remote storage	Title Change	Default	Y
[illegible]	uthoriz	Desktop Informat	Application Ac	Default	Y
11:5 :45 AM	Windows Expl	Start	Application Ac	Default	Y
11: 3:	[illegible]	mmand Prompt	Application Ac	Default	Y
1 53:	[illegible]	mmand Prompt	Application Ac	Default	Y
2:05:11 PM	Windows Expl	Start	Application Ac	Default	Y

10/9/2012 10:58:59 AM

Controlling play back speed or session location

For normal playback operation, you can click Play or Pause to start or pause a session. You can also fast forward by clicking the Speed control. The Timepoint needle shows you the current location in the session. You can drag the needle to any point in the session. The Real-time icon to the right of the time bar indicates that the session plays in a smooth time sequence. If you want to play back the session moving swiftly from one user action to the next, click the icon to gray it out. The Session point indicates the date and time of the Timepoint needle.

Marking sessions for review or action

You can use Audit Analyzer to manage the status of sessions that are pending review or action. For example, you can update the status of individual sessions using the following states:

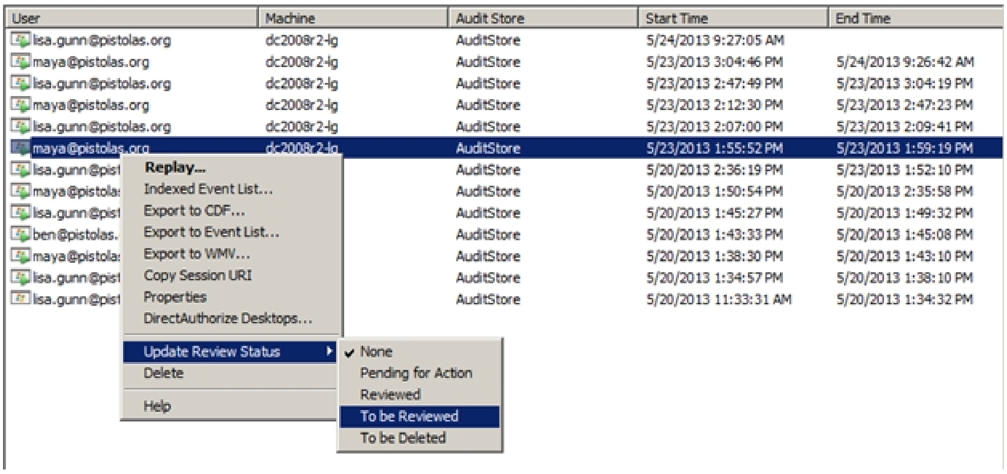
- To be Reviewed
- Reviewed
- Pending for Action
- To be Deleted

After you have marked sessions to be reviewed or pending action, you can use the predefined queries **Sessions to be Reviewed** and **Sessions Pending for Action** to see only the sessions in those states.

To update the review status for a session:

1. Select a query then select an individual session.
2. Right-click and select **Update Review Status**, then select a review state.

   For example, if the session is new and has not been reviewed, select **To be reviewed**.



User	Machine	Audit Store	Start Time	End Time
lisa.gunn@pistolas.org	dc2008r2-lg	AuditStore	5/24/2013 9:27:05 AM	
maya@pistolas.org	dc2008r2-lg	AuditStore	5/23/2013 3:04:46 PM	5/24/2013 9:26:42 AM
lisa.gunn@pistolas.org	dc2008r2-lg	AuditStore	5/23/2013 2:47:49 PM	5/23/2013 3:04:19 PM
maya@pistolas.org	dc2008r2-lg	AuditStore	5/23/2013 2:12:30 PM	5/23/2013 2:47:23 PM
lisa.gunn@pistolas.org	dc2008r2-lg	AuditStore	5/23/2013 2:07:00 PM	5/23/2013 2:09:41 PM
maya@pistolas.org	dc2008r2-lg	AuditStore	5/23/2013 1:55:52 PM	5/23/2013 1:59:19 PM
lisa.gunn@pist		AuditStore	5/20/2013 2:36:19 PM	5/23/2013 1:52:10 PM
maya@pistola:		AuditStore	5/20/2013 1:50:54 PM	5/20/2013 2:35:58 PM
lisa.gunn@pist		AuditStore	5/20/2013 1:45:27 PM	5/20/2013 1:49:32 PM
ben@pistolas.		AuditStore	5/20/2013 1:43:33 PM	5/20/2013 1:45:08 PM
maya@pistola:		AuditStore	5/20/2013 1:38:30 PM	5/20/2013 1:43:10 PM
lisa.gunn@pist		AuditStore	5/20/2013 1:34:57 PM	5/20/2013 1:38:10 PM
lisa.gunn@pist		AuditStore	5/20/2013 11:33:31 AM	5/20/2013 1:34:32 PM

3. Type a comment at the prompt, then click **OK**.
4. Click **Sessions to be Reviewed** in the left pane to see the session displayed.

   You can also view the review status and comments for a session by right-clicking a session, then select Properties.
5. Select one or more sessions and update the review status to Reviewed.

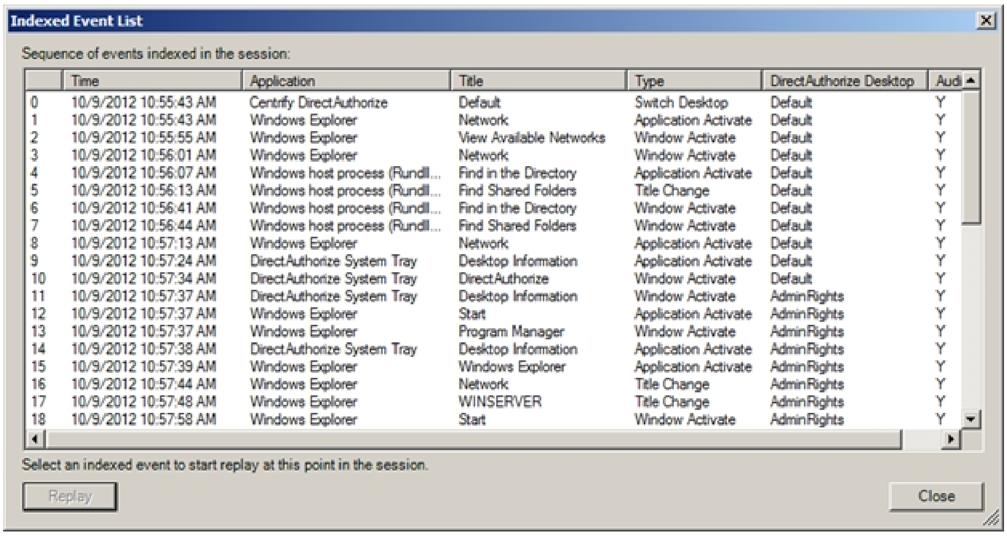
   Again, you will be prompted to provide a comment for the change in status. Type a new comment and click OK.

Using the indexed event list

If you don’t want to replay an entire session, you can use the indexed event list to view a summary of events recorded in a session, then selective start the replay at a specific event of interest.

To use the indexed event list:

1. Select a query then select an individual session.
2. Right-click and select **Indexed Event List**.



Sequence of events indexed in the session:

	Time	Application	Title	Type	DirectAuthorize Desktop	Audi
0	10/9/2012 10:55:43 AM	Centrify DirectAuthorize	Default	Switch Desktop	Default	Y
1	10/9/2012 10:55:43 AM	Windows Explorer	Network	Application Activate	Default	Y
2	10/9/2012 10:55:55 AM	Windows Explorer	View Available Networks	Window Activate	Default	Y
3	10/9/2012 10:56:01 AM	Windows Explorer	Network	Window Activate	Default	Y
4	10/9/2012 10:56:07 AM	Windows host process (Rundll...	Find in the Directory	Application Activate	Default	Y
5	10/9/2012 10:56:13 AM	Windows host process (Rundll...	Find Shared Folders	Title Change	Default	Y
6	10/9/2012 10:56:41 AM	Windows host process (Rundll...	Find in the Directory	Window Activate	Default	Y
7	10/9/2012 10:56:44 AM	Windows host process (Rundll...	Find Shared Folders	Window Activate	Default	Y
8	10/9/2012 10:57:13 AM	Windows Explorer	Network	Application Activate	Default	Y
9	10/9/2012 10:57:24 AM	DirectAuthorize System Tray	Desktop Information	Application Activate	Default	Y
10	10/9/2012 10:57:34 AM	DirectAuthorize System Tray	DirectAuthorize	Window Activate	Default	Y
11	10/9/2012 10:57:37 AM	DirectAuthorize System Tray	Desktop Information	Window Activate	AdminRights	Y
12	10/9/2012 10:57:37 AM	Windows Explorer	Start	Application Activate	AdminRights	Y
13	10/9/2012 10:57:37 AM	Windows Explorer	Program Manager	Window Activate	AdminRights	Y
14	10/9/2012 10:57:38 AM	DirectAuthorize System Tray	Desktop Information	Application Activate	AdminRights	Y
15	10/9/2012 10:57:39 AM	Windows Explorer	Windows Explorer	Application Activate	AdminRights	Y
16	10/9/2012 10:57:44 AM	Windows Explorer	Network	Title Change	AdminRights	Y
17	10/9/2012 10:57:48 AM	Windows Explorer	WINSERVER	Title Change	AdminRights	Y
18	10/9/2012 10:57:58 AM	Windows Explorer	Start	Window Activate	AdminRights	Y

Select an indexed event to start replay at this point in the session.

3. Select a session event in the lists to start the replay at that event.

Creating custom queries

Predefined queries searches the audit store database for sessions that meet the specific criteria. To see the search criteria, right-click a query, select **Properties**, then click the Definition tab.

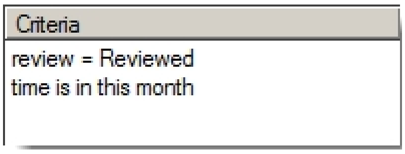
You can write your own queries to search for sessions that meet specific criteria of your choosing. The following example illustrates how to build a query that finds all of the sessions that have been reviewed.

To create a custom query for sessions that have been reviewed:

1. Open Audit Analyzer.
2. Select **Audit Sessions**, right-click, then select **New Shared Query**.
3. Type `Reviewed Sessions` for the name of the query and enter a description for the query. For example, type `Sessions that have been reviewed by department auditors`.

4. Deselect UNIX session as the type of session to include.
5. Click **Add** to add criteria.

   Notice that `review = Reviewed` appears in the Criteria field of the New Query dialog box.
6. Select **Review Status** from the Attribute list, select **Reviewed**, then click **OK**.
7. Click **Add** again.
8. Select **Session Time**, select the bottom radio button and **Is in**, then select **this month** and click **OK**.
9. Verify the Criteria displays both rules, then click **OK** to complete the query.

   review = Reviewed
   time is in this month

   After you click OK, the query is listed under **Shared Queries**.
10. Click the custom query to get the results.

Creating a quick query

You can also perform quick text string searches in Audit Analyzer.

To create a quick text string query for sessions:

1. Open Audit Analyzer.
2. Select **Audit Sessions**, right-click, then select **New Quick Query**.
3. Type a search string into the dialog box.

   As you type, the Quick Query displays a list of possible matches that start with the text you are typing. If an item in the list is what you are looking for, select it, then click **Find** to display all matching sessions in the right pane.

Auditing only specific events

The integration of access management and auditing makes it possible for you to audit only when a user switches to a specific desktop or role. Although you can use database queries in Audit Analyzer to find recorded events of a particular type, you can save space in your database by recording only those events in which you’re most interested.

Specify which roles or desktops to audit

To limit auditing to specific roles or desktops, you turn off more generalized auditing and enable auditing for just the roles you care about. The following example illustrates how to audit only when the user switches to a privileged desktop.

To audit only when the user switches to a privileged desktop:

1. Log in to the computer as the Administrator and open Access Manager.
2. Expand the console tree to the Authorization node for your evaluation zone.
3. Expand Role Definitions, select the `DesktopAdmin` role, right-click, then select **Properties**.
4. Click the Audit tab, select **Audit if possible** or **Audit required**.If auditing is required, users are prevented from using the role if auditing is not available or the agent is not running.
5. Log off and then log in as `amy.adams`.
6. Verify that you do not have elevated privileges by trying to change firewall settings in Control Panel.
7. Open a new desktop and select the `DesktopAdmin` role.
8. Perform operations, such as running the Firewall Control Panel and accessing the remote share on the Windows server, for which you need elevated privileges.
9. Switch back to your default desktop.

10. Open Audit Analyzer, select the Active Sessions node, and refresh the display.
11. Open the currently active session for the Windows client computer.

    You should find that only the portion of the session when you were using the `DesktopAdmin` desktop was recorded.

Audit trail of privileged events

Even when the auditing and monitoring service is not recording a session, it keeps a record of every event in which the user selected a role that provides elevated privileges.

To view audit trail events for elevated privileges:

1. Log in using your administrator account and open Access Manager.
2. Expand the console tree to the Authorization node for your evaluation zone.
3. Select the `ControlPanelAdmin` role, right-click, then select **Properties**.
4. Click the Audit tab and select **Audit not requested/required**.
5. Log off and then log in as `amy.adams`.
6. Verify that you do not have elevated privileges by trying to change firewall settings in Control Panel.
7. Right-click your Control Panel shortcut, select the `ControlPanelAdmin` role, and verify that you now have the rights to change firewall settings.
8. Close Control Panel and perform several more operations.
9. On the Windows client computer, open Audit Analyzer, select Active Sessions, and refresh the display.
10. Open the currently active session for your Windows client computer. You should find that none of your recent operations were recorded.
11. Right-click the Audit Events node, then select **Query Audit Events**.
12. In the dialog box, enter your search criteria, such as a role name, event time, or the type of event you are interested in locating, then click **OK**. All of the events that match the criteria you specify are listed. If the event

involved an audited role and you are capturing video records of audited activity, you can right-click an event to **Replay** the activity recorded.

All of the events that match the criteria you specify are listed. If the event involved an audited role and you are capturing video records of audited activity, you can right-click an event to **Replay** the activity recorded.

Additional auditing tools

Because the evaluation computer has the complete auditing infrastructure, you have several additional tools available for managing different components of that infrastructure. For example, computers that have the Centrify agent for Windows installed also have the following Centrify Auditing and Monitoring Service Settings. You also have access to the Audit Collector Control Panel, Audit Management Control Panel, and Audit Manager console. All of these programs are available from the Windows Start menu.

You use the control panels to configure and troubleshoot the component operations. Audit Manager provides a overview of all audit-related components. From Audit Manager, you can view the status of components, modify component properties and relationships, and manage audit store databases. You can also use Audit Manager to create audit roles, assign users to the audit roles, and manage permissions.

Audit Manager includes one Master Auditor role with full control over the installation. As the Master Auditor, you can manage and control all permissions for the installation.