



Server Suite

Windows Evaluation Guide

Version: 2024.x

Publication Date: 7/26/2024

Server Suite Windows Evaluation Guide

Version: 2024.x, Publication Date: 7/26/2024

© Delinea, 2024

Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

Table of Contents

Windows Evaluation Guide	i
Evaluation Guide for Windows	1
Setting up the Evaluation Environment	1
Preview of Tasks	1
Basic Requirements for the Evaluation	2
Preparing an Active Directory Domain Controller	2
Selecting a Windows Domain Computer	3
Downloading Delinea Software for Windows Evaluations	3
Downloading Server Suite Software for Windows Evaluations	4
Creating an Active Directory User and Group	4
Preparing to Evaluate Access Management	5
Configuring Active Directory Using Access Manager	5
Creating the First Zone	6
Assigning Yourself the Default Windows Login Role	6
Preparing to Evaluate Auditing	7
Identifying a Microsoft SQL Server Instance	7
Installing the Auditing Components	8
Installing the Agent for Windows	9
Configuring the Agent	10
Configuring Agent Settings for Audit and Monitoring Service	11
Selecting the Maximum Color Quality for Recorded Sessions	12
Configuring Agent Settings for Offline Audit and Monitoring Service Storage	12
Configuring Agent Settings for the Identity Platform	12
Configuring Agent Settings for Privilege Elevation	13
How Authentication Works for Windows	14
Providing Access Control and Accountability	14
Organizing Computers and Access Rights	15
Restricting Access to Administrative Privileges	15
Auditing User Activity on a Managed Computer	16
Creating and Using Roles and Desktops	17
Verifying that your Account is Assigned Basic Login Rights	17
Assigning the Windows Login Role to a Group	18
Adding Predefined Rights to a Zone	19
Creating an Application Right	20
Creating a Desktop Right	23
Switching Among Active Desktops	25
Creating a Network Right	25
Reviewing Rights and Roles in the Authorization Center	27

Table of Contents

Auditing Sessions	27
Using Audit Analyzer to Replay a Session	27
Magnifying the Recorded Session	28
Controlling Playback Speed or Session Location	28
Marking Sessions for Review or Action	28
Using the Indexed Event List	29
Creating Custom Queries	30
Creating a Quick Query	31
Auditing Only Specific Events	31
Specifying which Roles or Desktops to Audit	31
Audit Trail of Privileged Events	32
Additional Auditing Tools	32

Evaluation Guide for Windows

December 2021 (release 2021.1)

- [Setting Up the Evaluation Environment](#)
- [How Authentication Works for Windows](#)
- [Creating and Using Roles and Desktops](#)
- [Auditing Sessions](#)

Setting up the Evaluation Environment

This section describes how to prepare for an evaluation of Server Suite on a Windows computer. It includes instructions for installing Server Suite components and the Agent for Windows to enable a full evaluation of access control, privilege management, and auditing on Windows computers.

Installing and configuring Server Suite 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 Tasks

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 solution for Windows computers.

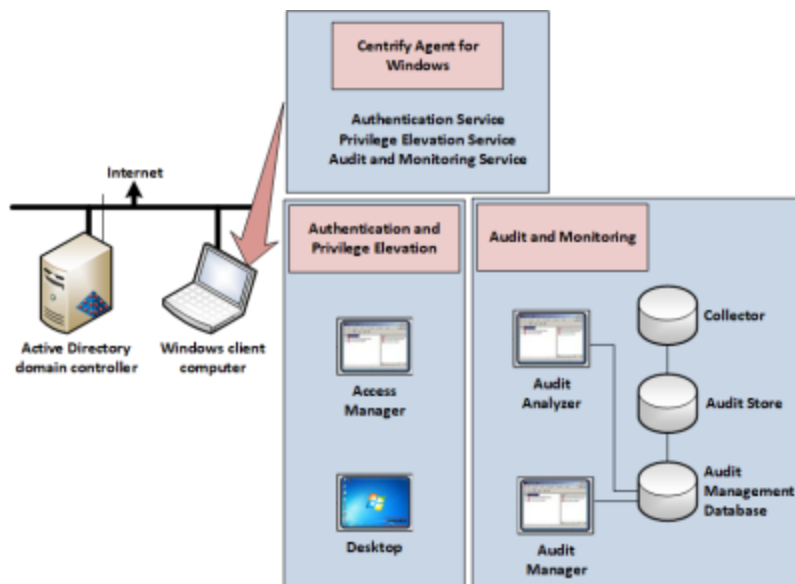
1. Ensure you have at least one Active Directory *domain controller* and one Windows *domain computer*—also referred to as the Windows *client computer*.
See [Basic Requirements for the Evaluation](#) for details about the system requirements for these computers.
2. Acquire Delinea software for the Windows client computer.
See [Downloading Delinea Software for Windows Evaluations](#) for details about acquiring Delinea software.
3. On the Active Directory domain controller, create an Active Directory user and group to be used in the evaluation.
See [Creating an Active Directory User and Group](#) for details about this procedure.
4. Install Access Manager and administrative tools on the Windows client computer.
See [Preparing to Evaluate Access Management](#) for details about installing these features.
5. Use Access Manager to configure Active Directory on the domain controller.
See [Configuring Active Directory Using Access Manager](#) for details about configuring Active Directory from Access Manager.
6. Use Access Manager to create a zone.
See [Creating the First Zone](#) for details about creating a zone.

Setting up the Evaluation Environment

7. Use Access Manager to assign the Windows Login role to your Active Directory account.
See [Assigning Yourself the Default Windows Login Role](#) for details about this procedure.
8. If you are evaluating auditing features, you need access to an instance of Microsoft SQL Server and an audit installation, which consists of several auditing-specific components.
See [Identifying a Microsoft SQL Server Instance](#) for details about installing a SQL Server Express instance for demonstration purposes.
See [Preparing to Evaluate Auditing](#) for details about installing audit components.
9. Install the Agent for Windows on the Windows client computer.
See [Installing the 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 Delinea-managed computer (the *Windows client computer*) and one 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.

Preparing 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.

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



In the configuration illustrated in the previous topic, no software is installed on the domain controller. However, because this is just an evaluation environment, you could install all of the software on the domain controller. In a production environment it is not recommended to install this software on domain controllers.

Selecting 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 or a Windows server platform. Please consult the release notes for supported platform versions.
.NET Framework	.NET Framework 4.6.2 or later If .NET is not installed, the 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 Agent for Windows provides a custom start menu. The Delinea start menu allows you to open and run applications as you would on Windows 7 or Windows Server 2008 R2. The Delinea start menu is installed on the left side of the taskbar and displays the Delinea logo. This start menu is only available if you are using a role with Delinea desktop rights and cannot be modified.

Delinea 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.

Downloading Delinea Software for Windows Evaluations

You can go to the [this website](#) to sign up for a free trial. Once you're signed up with an account, you can download the software.

To register for a free trial:

Setting up the Evaluation Environment

1. Navigate to <https://www.delinea.com/free-trial/>.
2. Enter your contact and company information, click the checkbox to indicate that you agree to the terms of use and privacy policy, and then click **Start My Trial**.



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

Downloading Server Suite Software for Windows Evaluations

You can download all of the components for Server Suite from the Delinea website to your Windows computer. Before you begin, be sure you have the email address and password you used to register for your trial.

To download the Windows software for Server Suite:

1. Open a browser on the Windows computer you plan to use for the evaluation and go to <https://www.delinea.com>.
2. In the upper area of the web page, click **Login**.
3. Enter your email address and your account password, then click **Login**.
4. Go to **Support > Downloads**.
5. Select **Zero Trust Privileges - Enterprise** to locate the latest software bundles.
6. Next to the latest version for 64-bit Windows systems, click either the **ISO** or **ZIP** button to download the software in that format.

The latest version of the Windows software bundle is called Server Suite.

7. Close the window when the download is complete.

Creating 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.

Preparing 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 Agent for Windows on the Windows client computer as described in [Installing the 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 Delinea CD or directory that has Delinea software, open **autorun**.
3. On the Getting Started page, click **Authentication & Privilege** to start the setup program for Authentication Service and Privilege Elevation Service.
4. Follow the prompts displayed and select Administration as the components to install.
For a Windows-only evaluation, none of the Utilities components are applicable.
5. Accept the defaults for the remaining selections, then click **Finish** to close the setup program.

Configuring 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 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 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 profile property pages.
9. Review the summary, click **Next**, then click **Finish**.

Setting up the Evaluation Environment

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**.

Creating 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**.



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.

Assigning Yourself the Default Windows Login Role

After you install the 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 Delinea-managed Windows computers.

To assign the Windows Login role to your account:

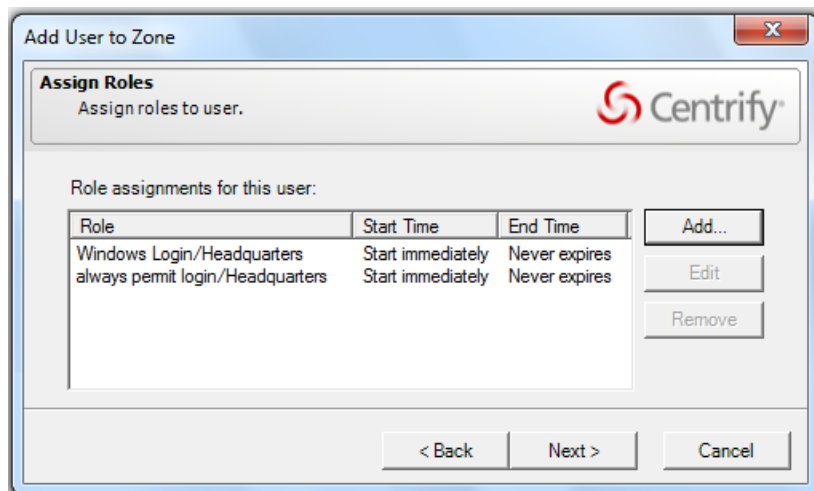
Setting up the Evaluation Environment

1. In Access Manager, expand Zones and select the zone you created in [Creating 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:



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

If you are evaluating auditing features, go on to [Preparing to Evaluate Auditing](#). If you are only evaluating access-related features, skip to [Installing the Agent for Windows](#).

Preparing 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.

Identifying 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.

Setting up the Evaluation Environment

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 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.

Installing the Auditing Components

In this section, you run the 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 Audit & 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 Delinea CD or directory that has Delinea software, open **autorun**.
3. On the Getting Started page, click **Audit & Monitor** to start the setup program for the audit and monitoring service.
4. At the Welcome page, click **Next**.
5. Review the terms of the license agreement, click **I accept the terms in the license agreement**, then click **Next**.
6. Select **Administration** and **Services** to install both Audit Manager and Audit Analyzer, then click **Next**.
7. 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 Audit 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.

8. In the Welcome page for the audit configuration wizard, click **Next**.
9. 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.

10. Select **Install a new SQL Server Express instance on this computer** and specify the instance name, then click **Next**.
11. 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**.



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

12. 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 Agent for Windows and join the computer to the zone you created.

Installing the Agent for Windows

You are now ready to install the Agent for Windows on the 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.



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 [Assigning 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.

To install the Agent for Windows using the setup program:

1. Insert the Delinea distribution CD into the computer on which you wish to install the agent or browse to the location where you have saved downloaded Delinea files.
2. On the Getting Started page, click **Agent** to start the setup program for the agent.
If the Getting Started page is not displayed, open the autorun.exe file to start the software installation.
3. If a previous version of the agent is installed, click **Yes** when prompted to upgrade the Agent for Windows.
4. At the Welcome page, click **Next**.
5. Review the terms of the license agreement, click **I accept the terms in the License Agreement**, then click **Next**.
6. Accept the default location for installing components, or click **Change** to select a different location, then click **Next**.
7. In the Ready to install Agent for Windows page, click **Install**.
8. Click **Finish** to complete the installation and start the agent configuration panel.

You must restart the computer after you configure the 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 Delinea 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.

Configuring the Agent

By default, when you click **Finish**, the setup program opens the agent configuration panel. In the agent configuration panel, you can enable the agent to connect to Delinea services that are installed on the main administrative computer as described in [Installing the Agent for Windows](#). After a service is enabled, you can use the agent configuration panel to configure settings that define how the agent will interact with each service.

The first time the agent configuration panel opens, it does not display any services for you to enable. Services display in the agent configuration panel only after you manually instruct the configuration panel to check for services and display those that are eligible to be enabled.

Only services that are installed and configured as required are eligible to be enabled. For example, if you installed the Privilege Elevation Service earlier (as described in [Preparing to Evaluate Access Management](#)) but did not create a zone, the Privilege Elevation Service does not display on the list of services that you can enable.

To enable services using the agent configuration panel:

1. If the agent configuration panel is not open, open it by clicking **Agent Configuration** in the list of applications in the Windows Start menu.
2. In the agent configuration control panel, click **Add service**.
All services that are available to be enabled are displayed.
3. In the list of services, highlight a service and click **OK**.
4. Provide additional information about the service that you are enabling:

- **Audit & Monitoring Service:**

In the Select an Audit Installation page, select an audit store from the list of available audit stores. Click **Next**, and the computer is connected to the audit store.

- **Identity Platform Settings:**

- a. In the Connect to Identity Platform page, type the URL of the identity platform instance to connect to, or select an instance from the list of registered platform instances in the forest. Click **Next**.
- b. In the Multi-factor authentication for Windows Login page, ensure that the check box to enable multi-factor authentication is selected. Next, use the **All Active Directory accounts** button or **Accounts below** button to specify which Active Directory accounts are enabled for multi-factor authentication login. If you select **Account below**, use the **Add** and **Remove** buttons to select accounts. Click **Next** when you are finished.

- **Privilege Elevation Service:**

Setting up the Evaluation Environment

- a. In the Join to a zone page, type a zone or select a zone from the list of available zones. You can also choose to select the option to retrieve the zone data before the computer restarts. This option can be helpful in situations where you might lose connection to the domain after restarting, such as when you're using a VPN connection.

Click **Next**, and the computer is joined to the zone.

- b. After the computer is joined to a zone, you must reboot the computer to activate all privilege elevation service features on the computer.

If the zone that you select is already configured with a Privileged Access Service tenant, the message **Identity Platform enabled** displays after the computer joins the zone. In this situation, the instance is managed by the zone, and is shown as read-only.

5. To add additional services, click **Add service** and repeat the preceding steps.

When you are done, the services that you enabled are shown in the **Enabled services** section of the agent configuration panel.

6. If necessary, continue to configure services after their initial configuration during enablement as described in these sections:

- [Configuring Agent Settings for the Audit and Monitoring Service](#)
- [Configuring Agent Settings for Offline Audit and Monitoring Service Storage](#)
- [Configuring Agent Settings for the Identity Platform](#)
- [Configuring Agent Settings for Privilege Elevation](#)

Configuring Agent Settings for Audit and Monitoring Service

If you want to reconfigure agent settings for auditing on a Windows computer after initially configuring them during enablement (or if you did not use the agent configuration panel when you enabled the service), you can open the agent configuration panel manually and configure the agent as described in this section.

To configure agent settings for audit and monitoring service:

1. In the Windows Start menu, click **Agent Configuration** in the list of applications.

The agent configuration panel opens, and displays the services that are currently enabled. You can configure any service listed in the **Enabled services** section.

2. Click **Audit & Monitoring Service**, and then click **Settings**.

3. In the General tab, click **Configure**.

4. Select the maximum color quality for recorded sessions, then click **Next**.

See [Selecting the Maximum Color Quality for Recorded Sessions](#) for more information on the configuration of this setting.

5. Specify the offline data location and the maximum percentage of disk that the offline data file should be allowed to occupy, then click **Next**.

See [Configuring Agent Settings for Offline Audit and Monitoring Service Storage](#) for more information on the configuration of this setting.

Setting up the Evaluation Environment

6. Select the installation that the agent belongs to, then click **Next**.
7. Review your settings, then click **Next**.
8. Click **Finish**.
9. Click **Close** in the General tab to save your changes.

For information about using the Troubleshooting tab, see the *Administrator's Guide for Windows*.

Selecting the Maximum Color Quality for Recorded Sessions

Because auditing Windows computers captures user activity as video, you can configure the color depth of the sessions to control the size of data that must be transferred over the network and stored in the database. A higher color depth increases the CPU overhead on audited computers but improves resolution when the session is played back. A lower color depth decreases network traffic and database storage requirements, but reduces the resolution of recorded sessions.

The default color quality is low (8-bit).

Configuring Agent Settings for Offline Audit and Monitoring Service Storage

The “Maximum size of the offline data file” setting defines the minimum percentage of disk space that should be available, if needed, for audit and monitoring service. It is intended to prevent audited computers from running out of disk space if the agent is sending data to its offline data storage location because no collectors are available.

For example, if you set the threshold to 10%, auditing will continue while spooling data to the offline file location as long as there is a least 10% of available disk space on the spool partition. When the available disk space reaches the threshold, auditing will stop until a collector is available.

The agent checks the spool disk space by periodically running a background process. By default, the background process runs every 15 seconds. Because of the delay between background checks, it is possible for the actual disk space available to fall below the threshold setting. If this were to occur, auditing would stop at the next interval. You can configure the interval for the background process to run by editing the HKLM\Software\Centrify\DirectAudit\Agent\DiskCheckInterval registry setting.

Configuring Agent Settings for the Identity Platform

If you want to reconfigure agent settings for Privileged Access Service on a Windows computer after initially configuring them during enablement (or if you did not use the agent configuration panel when you enabled the service), you can open the agent configuration panel manually and configure the agent as described in this section.

To configure agent settings for the Identity Platform:

1. In the Windows Start menu, click **Agent Configuration** in the list of applications.

The agent configuration panel opens, and displays the services that are currently enabled. You can configure any service listed in the **Enabled services** section.

2. Click **Identity Platform**, and then click **Settings**.
3. In the General tab, review the Status field in the Features area:

Setting up the Evaluation Environment

- If the status is **Enabled**, the computer is not joined to a zone, and you can configure all Identity Platform settings that are shown in the General tab.
 - If the status is **Enabled per zone settings**, the computer is joined to a zone, and most Identity Platform settings are based on the zone configuration. In this situation, the **Browse** and **Details** buttons in the General tab are disabled, because those features are controlled by the zone configuration. The only configuration that you can perform in the General tab is to change the proxy server settings.
4. To change proxy server settings:
 - a. Click **Change**.
 - b. Specify a new proxy server address.
 - c. Click **OK**.
 5. To change to a different Identity Platform instance (only configurable if the computer is not joined to a zone):
 - a. Click **Browse**.
 - b. Select an instance from the list of registered platform instances in the forest.
 - c. Click **OK**.
 6. To specify which Active Directory accounts require multi-factor authentication (only configurable if the computer is not joined to a zone):
 - a. Click **Details**.
 - b. Use the **All Active Directory accounts** button or **Accounts below** button to specify which Active Directory accounts are enabled for multi-factor authentication login. If you select **Account below**, use the **Add** and **Remove** buttons to select accounts.
 - c. Click **OK**.
 7. Click **Close** in the General tab to save your changes.

For information about using the Troubleshooting tab, see the *Multi-factor Authentication Quick Start Guide*.

Configuring Agent Settings for Privilege Elevation

If you want to reconfigure agent settings for privilege elevation on a Windows computer after initially configuring them during enablement (or if you did not use the agent configuration panel when you enabled the privilege elevation service), you can open the agent configuration panel manually and configure the agent as described in this section.

To configure agent settings for privilege elevation:

How Authentication Works for Windows

1. In the Windows Start menu, click **Agent Configuration** in the list of applications.

The agent configuration control panel opens, and displays the services that are currently enabled. You can configure any service listed in the **Enabled services** section.

2. Click **Privilege Elevation Service**, and then click **Settings**.
3. In the General tab, click **Change**.
4. In **Change the zone for this computer**, click **Browse**.
5. Click **Find Now** to search for an appropriate zone for the agent.
6. Select a zone from the list of search results, then click **OK**.
7. Click **OK** to use the zone you selected.
8. Click **Close** in the General tab to save your changes.

For information about using the Troubleshooting tab, see the *Administrator's Guide for Windows*.

How Authentication Works for Windows

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

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.

Delinea 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, Delinea 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, Delinea relies on the following:

- **Authentication Service** and **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 zone technology to limit the scope of a role to limited sets of computers. You can, also, configure roles with start

How Authentication Works for Windows

and expiration dates or to be active on specific days of the week and hours of the day.

- **Audit & Monitoring Service** enables you to collect and store an audit trail of user activity and provides a console for searching and replaying captured sessions.
- **Agent for Windows** enables you to deploy access and auditing features on the Windows computers you want to manage.

You can use Privilege Elevation Service without auditing if you aren't interested in collecting and storing information about session activities. You can also deploy Server Suite without access and privilege management features if you are only interested in auditing activity on Windows computers. However, the real value of Delinea 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 Delinea software to manage access and administrative privileges for Windows computers and applications. However, Delinea 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. Delinea enables this cross-platform integration through the use of **Zones**.

A 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 be inherited or zone-specific.

As part of the evaluation, you will create a 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

How Authentication Works for Windows

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 an Agent for Windows installed on each computer you want to manage.

Auditing User Activity on a Managed Computer

When you install the 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 audit 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 audit 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 **audit and monitoring service installation**:

- **Audited computers** are the computers on which you want to monitor activity. To be audited, the computer must have the 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

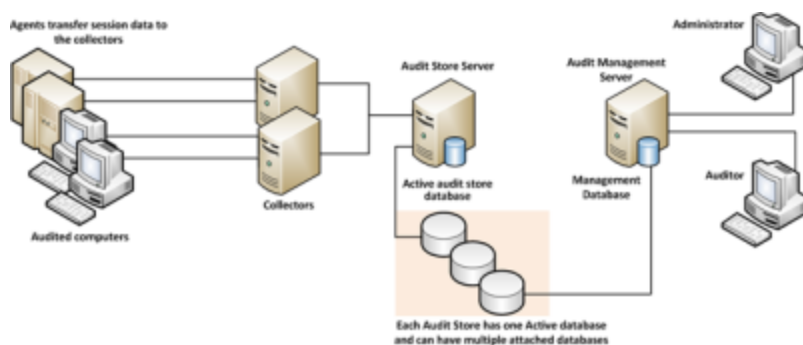
Creating and Using Roles and Desktops

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 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.



Creating and Using 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.

Verifying that your Account is Assigned Basic Login Rights

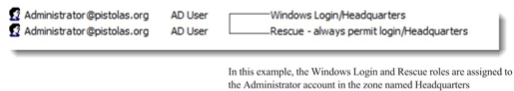
At this point, you should be logged on to the Windows client computer with an administrator account that has been assigned the “Windows Login” and “Rescue always permit login role” predefined roles as described in “Assigning Yourself the Default Windows Login Role” on page 6. Because the client computer has Access Manager and the 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 “Creating the First Zone” on page 6.
2. Expand Authorization and select Role Assignments.

Creating and Using Roles and Desktops

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



Assigning the Windows Login Role to a Group

After a computer joins a 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 `Eva1` 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 "Creating an Active Directory User and Group" on page 4.

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 `Eva1` to search for `Eva1` 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 `Eva1` 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 "Creating an Active Directory User and Group" on page 4, 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.

Adding 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.

Creating 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 [Creating 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:

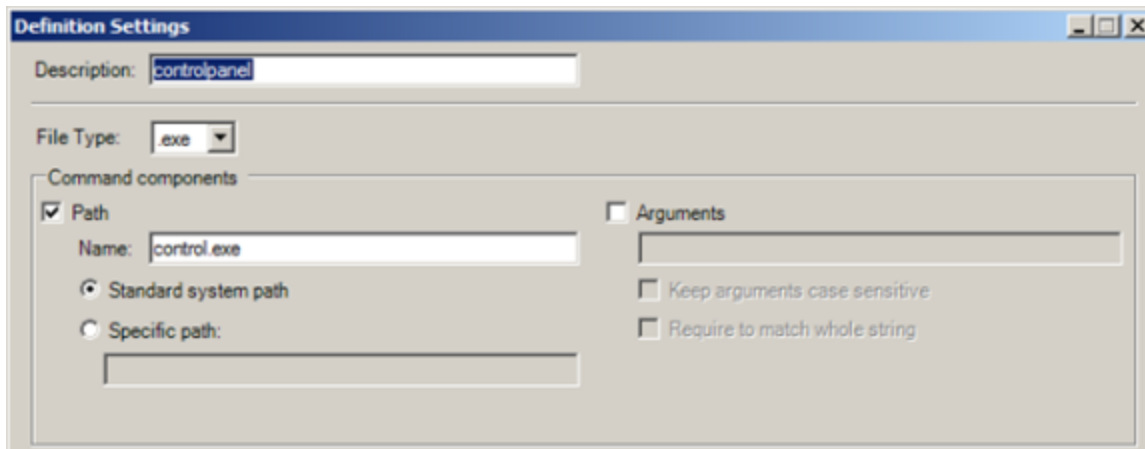
1. On the Windows client computer, open Access Manager and expand to display **Authorization > Windows Right Definitions**.
2. Select **Applications**, right-click, then select **New Windows Application**.
3. On the General tab, type Control Panel Right for the name of this application right and an optional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

Creating and Using Roles and Desktops

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:



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 ##-managed Windows computers relies on the infrastructure provided by Privileged Access Service. 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:

Creating and Using Roles and Desktops

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 > 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.

Creating 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 `Eva1` 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 Server Suite-managed Windows computers relies on the infrastructure provided by Privileged Access Service. 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**.

Creating and Using Roles and Desktops

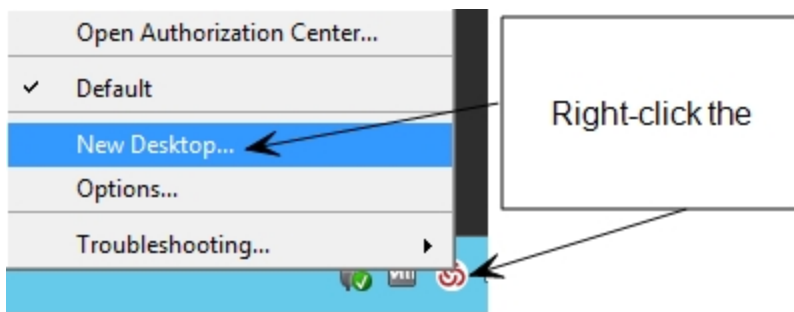
- Click **Add AD Account**.
- Change the **Find** filter from User to Group.
- Search for and select the group you created for the evaluation (for example, Eval Group), then click **OK**.
- Verify that the account is included in the Accounts list in the Assign Roles dialog box, then click **OK**.
- Open the **Privilege Elevation Service Settings** (from the Agent Configuration shortcut > 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 ## icon to display the applet options.
5. Select **New Desktop**.



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 ## 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.



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 Among 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 Server Suite 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 Server Suite icon, then select **Close Desktop**.

Creating 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 Agent for Windows on the remote computer and join that remote computer to the zone you created in "Creating the First Zone" on page 6.

You can use the domain controller or another computer as the remote computer for this exercise. Install the 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 Agent for Windows on the computer that you are using as the remote computer.
See *Installing the 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.

Creating and Using Roles and Desktops

- 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 ##-managed Windows computers relies on the infrastructure provided by the Privileged Access Service. 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 > 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 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.

Auditing Sessions

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.

Reviewing Rights and Roles in the Authorization Center

The Authorization Center is an option available from the 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 ## 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 audit 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.

Using Audit Analyzer to Replay a Session

If you selected both Privilege Elevation Service and Auditing and Monitoring Service features, the 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 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:

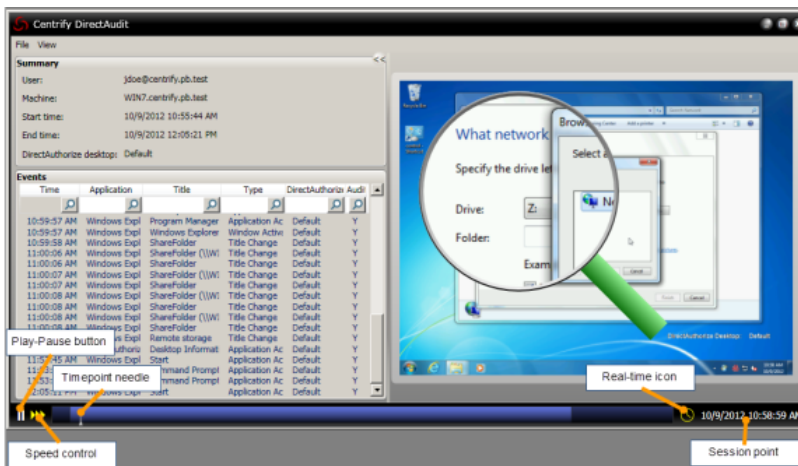
Auditing Sessions



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.



Controlling Playback 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:

Auditing Sessions

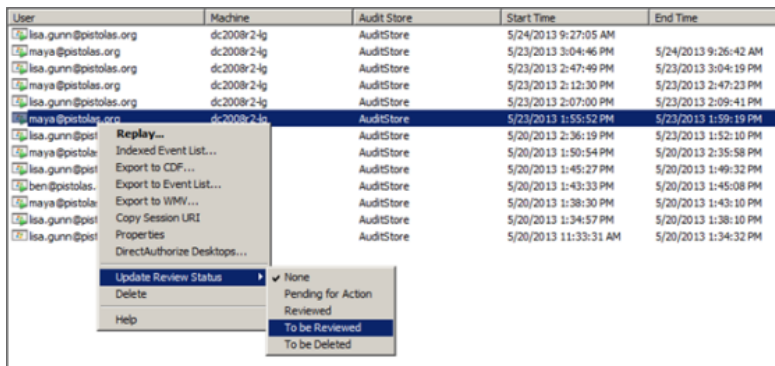
- To be Reviewed
- Reviewed
- Pending for Action
- To be Deleted

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**.



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**.

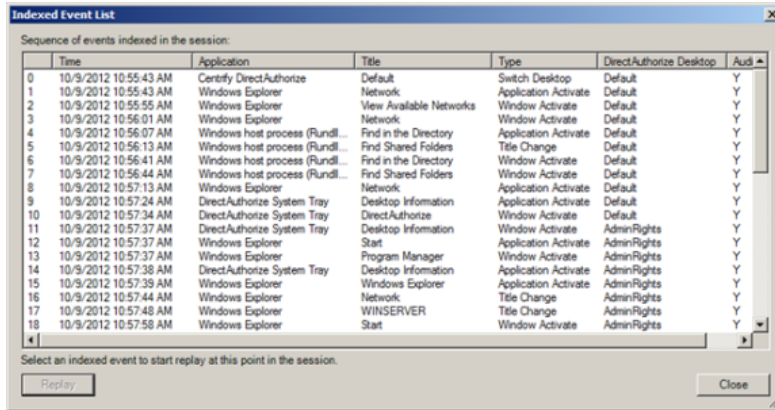
Using the Indexed Event List

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**.

Auditing Sessions



Indexed Event List

Sequence of events indexed in the session:

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

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

Replay Close

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

Creating Custom Queries

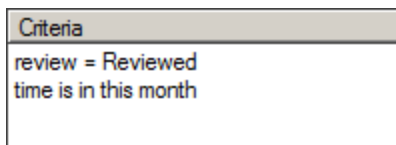
Predefined queries searches the audit store database for sessions that meet the specific criteria. To see the search criteria, right-click a query, select **Properties**, then click the Definition tab.

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.



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.

Specifying 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 Agent for Windows installed also have the following 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.