Centrify Server Suite 2017

User's Guide for Windows

February 2017

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.

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 User Suite, and Centrify Server Suite are registered trademarks and Centrify for Mobile, Centrify for SaaS, Centrify for Mac, DirectManage, Centrify Express, DirectManage Express, Centrify Identity Platform, Centrify Identity Service, and Centrify Privilege Service are 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 B2; 9,112,846; 9,197,670; 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 *Centrify Server Suite User's Guide for Windows* describes how you select and use the roles you have been assigned to get privileged access to applications and network resources. If your organization has deployed Centrify software and installed agents on Windows computers, an administrator should have prepared your computer and any remote servers you use and assigned one or more roles with specific access rights to your account.

Intended audience

The *User's Guide for Windows* provides basic information for users who have been granted specific rights and role assignments by an administrator. If you are an administrator responsible for installing and configuring software or defining access rules and audit requirements, see the *Administrator's Guide for Windows* for information about how you create, manage, and assign access rights and roles.

Conventions used in this guide

The following conventions are used in this guide:

- `Fixed-width font` is used for sample code, program names or output, file names, and commands that you type at the command line. When *`italicized`*, the fixed-width font is used to indicate variables.
- **Bold** text is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- ***Italics*** are used for book titles and to emphasize specific words.

Finding more information

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. 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.

To get to the documentation portal, go to docs.centrify.com or https://www.centrify.com/support/documentation.

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 to 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.

Introduction to Centrify software

This chapter provides an overview of Centrify features for Windows computers and how you can use Centrify to temporarily elevate your privileges to perform administrative tasks locally on your computer or remotely on a network server.

The following topics are covered:

What is Centrify Server Suite?

Centrify Server Suite is a multi-tier software solution that enables administrators to centrally manage access to on-premise servers and workstation, mobile devices, and applications across a broad range of platforms. With Centrify Server Suite, administrators can accomplish the following:

- Manage local and remote access to computers with Linux, UNIX, Mac OS X, and Windows operating systems.
- Enforce security policies and control access to applications on mobile devices such as iPhone and Android smart phones and tablets.
- Enable single sign-on and role-based rights for on-site and cloud-based applications.

- Capture detailed information about user activity and the use of administrative privileges.

Using Centrify software, an Active Directory administrator creates **zones** to organize the enterprise's on-premise computers, mobile devices, and applications into groups. For each group, the administrator then defines rights, roles, and group policies to control access to the computers and applications in that zone. By using zones and role assignments, the administrator can establish fine-grain control over who is authorized to perform administrative tasks and when user activity should be audited.

With Centrify, your organization can reduce the risk of unauthorized access to critical resources, ensure accountability and regulatory compliance for users with access to privileged accounts or sensitive information, and simplify the management of shared accounts and role-based access rights.

Using Centrify to manage access to Windows computers

Centrify provides a cross-platform solution that relies on the deployment of a **Centrify agent**. To manage access to Windows servers and workstations, an administrator installs the Centrify agent for Windows and identifies the zone the computer should use. If an administrator has installed the agent and added your computer to a zone, the computer is a **Centrify-managed computer**. When you log on, the agent will check that you have been assigned a role that allows a local or remote logon. As long as you have a role assignment that allow you to log on, logging on proceeds normally. If you have not been assigned a role that allows you to log on, you will be denied access to the computer.

In most cases, an Active Directory administrator or another delegated administrator will also define rights and roles that enable you to run as another account that has elevated privileges. For example, the administrator might create a role that allows you to manage a Microsoft SQL Server instance using administrative privileges and another role that enables you to run an Exchange management tool using a shared service account.

The administrator is responsible for defining the specific rights that are available in different roles and for assigning those roles to the appropriate Active Directory users and groups. The administrator can also assign selected roles to local Windows users and groups.

As a user logging on to a **Centrify-managed computer**, you have the option to select from and switch between the roles you have been assigned. For example, you begin the day by logging on to your computer using your Active Directory credentials. In most cases, this account does not have elevated privileges. In your work queue, you find that you need to add a new database to the SQL Server instance you manage. Because this change requires administrative privileges not available in your logon account, you select the role that has elevated privileges that you have been assigned for managing SQL Server instances. When you are done adding the database in Microsoft SQL Server Management Studio, you switch back to your default logon account.

The administrator determines whether the elevated privileges in your role are limited to a specific application, for example, Microsoft SQL Server Management Studio, any application on your desktop, or only allowed on a remote server. You are responsible for selecting the appropriate role to do the work required from the list of roles available to you.

Auditing role-based activity

The administrator can also define an auditing requirement for each role. If you switch to a role that is audited, the switch is recorded in the local Windows event log. If the computer you are using is configured to audit session activity, all of the actions you take during the session are captured in a video recording until you end the session or log out. If session activity is audited, the agent on your computer captures everything displayed on the screen, including your keystrokes and the windows you have open while you are using an audited role on an audited computer. If you switch from a role that requires auditing to one that has no audit requirement, the recording stops until you resume the role that requires auditing.

The administrator determines which roles and computers require auditing of user activity and can enable auditing notification to inform you if your actions might be audited.

Roles grant different types of access rights

There are three types of access rights that an administrator can add to any role you might be assigned:

Type of access right	What a role with this type of right allows you to do
Desktop	If you have been assigned a role that grants a desktop right, you can create a separate desktop on your computer to run applications as yourself but with the elevated privileges associated with a specific Active Directory or built-in group. In most cases, an administrator assigns you a role with a desktop right if you have more than one local application for which you need elevated privileges and you need to use those privileges frequently. For example, if you use several administrative applications on a daily basis, you are likely to be assigned a role that has a desktop right.
Application	If you have been assigned a role that grants an application right, you can run a specific application with the elevated privileges associated with a specific user account or as yourself but with the elevated privileges associated with a specific Active Directory or built-in group. In most cases, an administrator assigns you a role with an application right if you have only occasional administrative responsibilities for a specific application or only need temporary use of the elevated privileges.
Network access	If you have been assigned a role that grants a network access right, you can connect to a remote computer as an account with privileges on that computer. In most cases, an administrator assigns you a role with a network access right if you need to take administrative action on a remote server. This access right does not change any of your privileges on your local computer.

Every role includes one or more rights. Depending on the roles you have been assigned, you might have one or more of these access rights available.

Computers must be in a zone for roles to be available

The administrator can define different rights and different roles for every zone. Your computer must be joined to a zone for those rights and roles to be available. In addition, a computer can be joined to only one zone at a time. The rights you have in any zone are based on the roles assigned to you in that zone and its parent zone. If the administrator has not added your computer to a zone, no local or network roles will be available for you to use.

After a computer is added to a zone, it is possible that your role assignments might enable you to access remote computers in zones other than the local computer's zone. Roles that enable access to remote computers do not require you to have any local roles available in your local computer's zone.

In most cases, the administrator should add your computer to the appropriate zone. Changing the zone assignment requires local administrative privileges. If you have administrative privileges on your local computer, you can use the Centrify DirectAuthorize Agent Control Panel to view information about your current configuration and perform administrative tasks, if required. For example, if the administrator notifies you that you should join a zone they have prepared, you can use the Centrify DirectAuthorize Agent Control Panel to complete the operation for your local computer.

Using the dzjoin command line program

You can use the `dzjoin` command line program to automatically join the zone where your rights and roles are assigned, or specify a zone to join by zone name upon logging on. The `dzjoin` command line program is particularly useful for organizations that use non-persistent virtual desktop infrastructures.

The syntax for the `dzjoin` command is:

```
dzjoin [/z] [/s] [/v] [/f] [/c]
```

Use this option	To do this
/z	Join to a zone using the zone name. If the zone name is not unique, use the canonical name instead.
/s	Join to the zone where the user's roles and rights are assigned. You must be a member of the zone, or have previously been joined to the zone.
/v	Display the agent version.
/f	Suppress any warnings.
/c	Specify a domain controller to connect to.

Why you should use roles for administrative tasks

Roles give the administrator complete flexibility for delegating control and limiting risk. For example, the administrator can define a role that lets you do specific administrative functions on your local or a remote computer without giving you the administrator's password. By eliminating the use of a shared password for the administrator's account, you can prevent an audit finding that could be costly for your organization. Using a role also limits your authority on the computer, ensuring appropriate accountability, and limits the potential damage a compromised password might cause.

In addition, roles enable targeted auditing of user activity, so that only the actions when you have elevated privileges or access certain computers are recorded. In many cases, these activities must be recorded for regulatory or industry compliance. With roles, you can go about your normal activity, such as reading and responding to email, without auditing, then capture detailed information about the use of

SQL Server Management Studio or the Exchange Management Console.

What gets installed on a managed computer

The Centrify agent for Windows includes components for access management and auditing. These components can be installed together or separately on any supported Windows computer. Depending on the selections made during installation, your computer might include the following:

- DirectAuthorize Agent service manages your access rights, including your ability to log on locally, connect to a remote server, and access applications using administrative privileges.
- Centrify DirectAuthorize desktop applet that enables you to select roles, open new desktops, switch between open desktops, and view details about our role assignments. The applet is visible on your computer as the Centrify icon in the system tray.
- Centrify DirectAuthorize Agent Control Panel that enables an administrator to join, change, or leave the zone, run diagnostics, and configure and view logged activity.

If you are assigned roles that define application and desktop rights on your local computer, or access rights on remote computers, the Centrify agent for Windows must be installed on your local computer and on the remote computer.

The administrator can deploy the Centrify agent for Windows from a central location on the network to your computer or you can install it directly on your local computer.

Getting started

This chapter describes how to use Centrify to access applications with privileges on a Windows computer that has the Centrify agent for Windows installed.

The following topics are covered:

- Verify you can log on
- Setting up the offline passcode (multi-factor authentication)
- Checking your rights and role assignments
- Working with desktop access rights
- Running a specific application with privileges
- Selecting roles with network access rights
- Role-based auditing of session activity

Verify you can log on

The Centrify agent for Windows can be centrally deployed by a system administrator or deployed locally directly on a computer. If an administrator has installed a Centrify agent on a computer you use, the next step is to verify that you can log on successfully and locate the Centrify applet on your computer. The Centrify agent does not change how you log on your computer. However, you must be assigned at least one role that allows you to log on locally, remotely, or both.

When you are prompted for a user name and password, type your domain or local credentials as you normally would. If your administrator has enabled multi-factor authentication for log in, you will be asked to perform one or more authentication challenges, such as responding to a text message or email message, answering a security question, or answering an automated phone call. If you provide valid credentials and have been assigned a role with permission to log on, you should see your default desktop as it normally displays with the addition of a Centrify applet that is added to

the system tray notification area. By left-clicking on the Centrify applet, you can view your current desktop and assigned roles.

As part of the deployment, your computer may or may not have been joined to a zone. If the administrator has not specified a zone for your computer to join as part of the deployment process, you can specify a zone using the Centrify DirectAuthorize Agent Control Panel on your local computer. Contact your system administrator to find out which zone you should join.

You can check whether the agent is installed and running, and whether you are connected to a zone using the Services Control Panel or the Centrify DirectAuthorize Agent Control Panel. For example, click **Start > Centrify Server Suite 2017 > Agent for Windows Control Panel > DirectAuthorize** to view the control panel.

If the agent is installed but not connected to a zone, you should contact your system administrator to determine the zone to use. You should note, however, that setting or changing the zone assignment requires local administrative privileges. If the agent is not installed on the local computer, you should contact your administrator to find out if you are responsible for deploying the Centrify agent for Windows on your computer.

If the zone information for the agent is configured, but the agent status is not Connected, your current rights, roles, and role assignment privileges should still be available, in most cases, from the local authorization cache. If you are unable to perform administrative tasks that you normally can perform, contact your system administrator to determine whether the authorization cache needs to be refreshed.

If you cannot log on, see "What to do if you cannot log on" on page 10.

What to do if the Centrify icon is not displayed

By default, the Windows system tray notification area is the located to the right of the task bar on the bottom of your screen. You can customize this area to display icons for different applications.

If the Centrify icon is not displayed by default, you can click the up arrow in the notification area to add it.

To display the Centrify icon if it is not displayed by default:

1 Click the up arrow in the notification area.

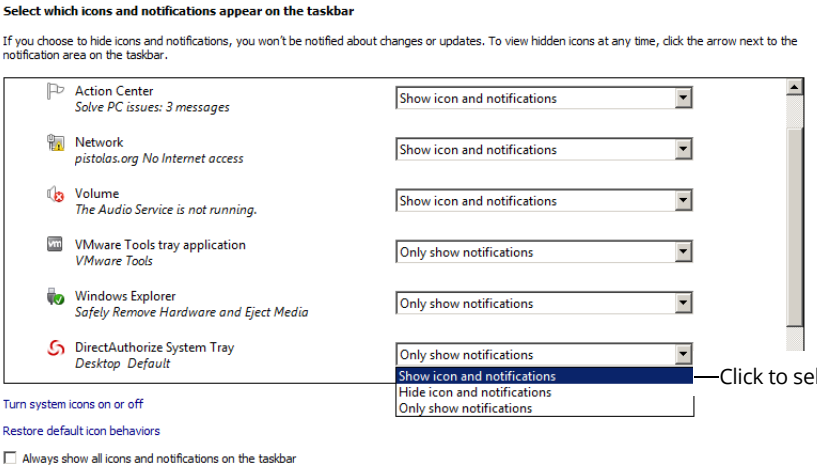
For example:

Click the arrow in the notification area to customize the icons displayed to include the

2 Click **Customize** to change the icons displayed.

3 Scroll to the DirectAuthorize System Tray icon, then select **Show icon and notifications** to display the Centrify icon at all times.

For example:



Click to select when the icon

4 Click **OK**.

What to do if you cannot log on

There are several reasons why an attempt to log on can fail. If you are denied access to a computer:

- Verify that the computer you trying to log on to allows the type of access you are attempting. For example, most users cannot log on locally on computers that are Active Directory domain controllers. Similarly, a computer's properties must be configured to allow remote access for you to be able to connect remotely. These

settings are Windows policies and properties and are not related to the Centrify agent for Windows.

- Check whether you are attempting to log on using a local account or a domain account. The administrator can assign a role that allows you to log on to your local account, your domain account, or both. It is possible that only one of those accounts has been assigned a role with access to the computer. For example, your administrator may have your account configured so you can log on using your local account credentials but not with your domain credentials.
- Verify that the computer where you are trying to log on has access to an Active Directory domain controller. If an Active Directory domain controller is not available or the local computer is not a member of an Active Directory domain, you might be prevented from logging on because the agent cannot verify you have authority to access the computer.
- Determine whether you are attempting to log on to a remote computer with an appropriate role. The administrator can assign a role that allows you to log on locally, log on remotely, or both. It is possible that only one of those rights has been configured for the role you have been assigned. For example, your administrator may have configured the role you are assigned to allow you to log on to your local computer but not allow remote connections.

After the Centrify agent has been installed, you must have a role assigned to your account that gives you log on privileges. If an attempt to log on fails, contact your Active Directory administrator or helpdesk to determine the roles you have been assigned, the type of access your roles grant, and any limitations associated with your role assignment. For example, roles can have time constraints with specific periods of availability. If you attempt to log on, but the role is not available, you will be denied access.

For more information about the steps you can take, see "Troubleshooting" on page 36.

Setting up the offline passcode (multi-factor authentication)

If you are required to use multi-factor authentication, you may be prompted to set up an offline passcode so that you can access your computer in the event that the Centrify authentication server cannot be reached.

If your administrator has enabled offline multi-factor authentication, you will see a notification message each time you log on which will prompt you to set up your offline passcode. Depending on the configuration settings, you may not be able to access your machine in the event that you are unable to connect to the authentication server if you do not set up the offline passcode.

To set up an offline passcode

1. Right click the Centrify notification icon in the system notification area, and select “Setup Offline Passcode”
2. Click **Next** to begin the Offline Authentication Wizard.
3. Select one of the following methods to create a authenticator account profile on your mobile device:
   - Scan barcode

     If you select this option, a QR code is displayed for you to scan using your mobile authenticator application. You can use either the Centrify application or a third-party authenticator application.
   - Manual entry

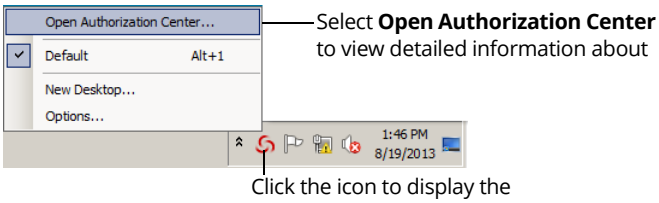
     If you select this option, you must manually enter the displayed account profile information into your authenticator application.
4. Enter the passcode that is generated after you have created your authenticator profile. Click **Next**.
5. Click **Finish** to exit the Wizard.

After you have set up your offline passcode, you will be prompted to enter the mobile passcode generated by your authentication application as the second form of authentication when you attempt to

log on to your machine if it cannot connect to the Centrify authentication server.

Checking your rights and role assignments

The roles you are assigned control your access rights and the accounts you can use to log on. You can look up detailed information about your rights and role assignments by clicking the Centrify icon, then selecting Open Authorization Center. For example:



You can then click the tabs to see information about your current role and any other roles you have been assigned. For example, from Authorization Center, click the following tabs to see more detailed information about how the roles you have been assigned are configured:

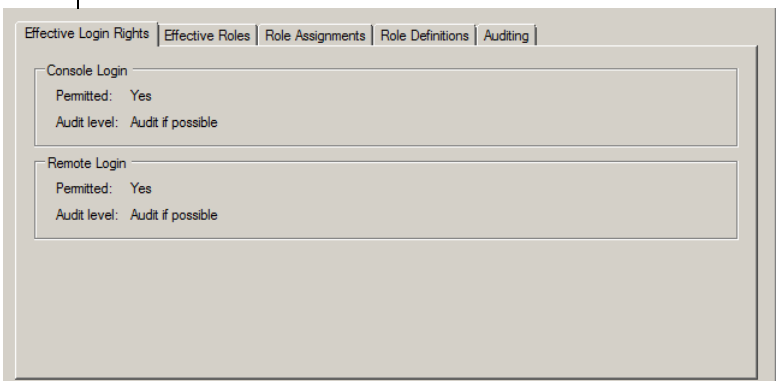
- Click **Effective Login Rights** to see information about your local and remote login rights and whether auditing is requested, required, or not applicable.
- Click **Effective Roles** to see information about the roles you have been assigned and the current status of each role. For any roles, you can right-click a role, then select Role Properties to view additional details. For example, if any of your roles are Inactive, you can right-click to see the time constraints defined for the role. You can also view the specific type of rights granted by each role.
- Click **Role Assignments** to see detailed information about your role assignments, including where the assignment was made, whether the role is a local or network role, and the start and end times that are in effect for the role. You can right-click a role assignment, then select Assignment Properties or Role Properties to view additional details.
- Click **Role Definitions** to see detailed information about the login rights and audit requirements that have been defined for the roles

you have been assigned. You can right-click a role definition, then select Properties to view additional details.

- Click **Auditing** to see information about the auditing status for each desktop started in a session.

You can only view information about your own access rights and role assignments in the Authorization Center. Click **Close** when you are finished viewing authorization information.

Click the tabs to see more information about your rights, role assignments, role definitions, and



After you review information about your access rights and role assignments using Authorization Center, you should have a basic understanding of the roles you have been assigned, any restrictions on when they are available, and what the roles allow you to do. Your role assignments control where you can log on, the type of account you use to log on, the specific access rights you have on local or network computers. As discussed in "Roles grant different types of access rights" on page 4, there are three categories of access rights for Windows computers:

- Desktop
- Application
- Network access

Depending on the details of how roles are defined in your organization and the specific roles you have been assigned, you might have some or all of the access rights described in the next sections.

Working with desktop access rights

When you first log on, the default desktop is your only desktop. Depending on whether you logged on using a local user account or an Active Directory domain user account, you have the default privileges associated with that account. If you have been assigned a role with a desktop access right, the Centrify agent enables you to run individual applications using a selected role from your default desktop or create one or more new desktops to run multiple applications using the administrative privileges associated with your roles.

If you have one or more roles with desktop rights, you can create, select, and switch between desktops on computers that have a traditional Windows desktop.

Note If the computer you are using is running Windows 8 or 8.1, or 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.

Running an individual application using a role

If you have a role assignment with a desktop access right, you don't have to create a new desktop to run a local application using your administrative privileges. You can select any local application directly from your default desktop, then select a role you have been assigned without creating a new desktop or switching from one desktop to another. This is often the best solution if you only run one application using your administrative privileges or rarely need to invoke those privileges.

To run a local application using a selected role:

1 Navigate to and select the application you want to run.

2 Right-click the executable or shortcut for the application.

If you want to open the 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 If the Select Role dialog box opens, select a role from the list of available roles, then click **OK**.

Note If there is only one role assigned to you that allows you to run the application, the application will automatically run using that role, and the dialog box does not open. If you would like to access the Select Role dialog box, press the Shift key when you select **Run with Privilege**.

5 Type the password for your login account if you are prompted for it, then click **OK**.

If your administrator has enabled multi-factor authentication, complete the additional authentication challenges after entering your password.

After you select a role, you have the rights associated with that role. The application opens with the privileges associated with a specific user account or with the members of a particular administrative group and an audit trail event is recorded in the Windows Application event log. When you close the application, you resume working with your normal account privileges and group membership.

Creating a new desktop

Desktop access rights enable you to create a separate desktop working environment for each role the administrator has assigned to you. You might have multiple role assignments with different desktop access rights so that you can run applications with elevated privileges. For example, you might be assigned two separate roles—one for running

applications as a member of the domain administrators group and another for running applications as a member of the local administrators group.

If you have been assigned roles that have desktop access rights, you can create a desktop for each role.

To create a new desktop:

1 Click the Centrify icon in the notification area.

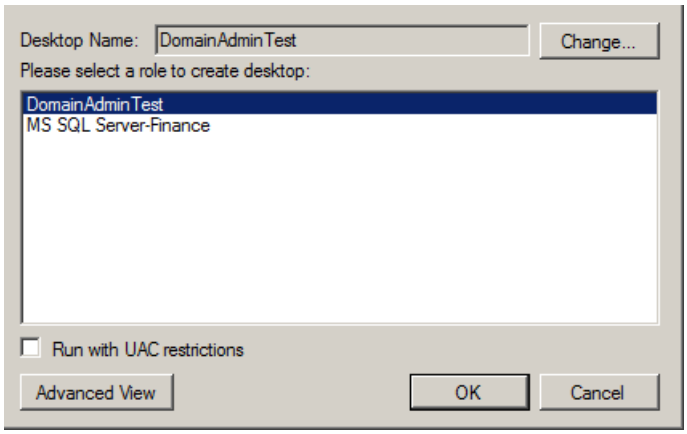
2 Select **New Desktop**.

If you have not been assigned to any role that has a desktop access right, a message is displayed to inform you that you are not a member of any role that permits opening a new desktop.

If you have been assigned to any roles that have desktop access rights, you can continue to the next step.

3 Select a role from the list of your available roles, then click **OK**.

For example, if you are assigned multiple roles that include desktop access rights, you can select from these role assignments to control which account privileges are in effect for the new desktop.



Note that the roles listed might allow you to run as you own account locally, but grant access to remote servers. To see more information about the context associated with your roles, click **Advanced View**.

When you select a role, you also have the option to run the desktop with User Account Control (UAC) restrictions enforced. Selecting this option gives you filtered privileges, prompting you to confirm

actions before continuing with operations that require elevated privileges. You can leave this option unselected to use a desktop with full privileges and without being prompted to confirm your actions. You should note, however, that when you run a desktop without enforcing UAC restrictions, no warnings are displayed, even if you have configured User Account Control Settings on the local computer.

4 Type the password for your login account, if you are prompted for it, then click **OK**.

If your administrator has enabled multi-factor authentication, complete the additional authentication challenges after entering your password.

After you select a role and click **OK**, the new desktop becomes your working environment. You can view the local and network roles you are using for the new desktop by left-clicking on the Centrify icon in the system Notification Area on the taskbar.

If the role is only applicable on a remote computer, the local role is displayed as Self. If the role does not have network access rights, the network role is displayed as Self.

To see complete information about the desktop, application, and network access rights for each of your roles, open the Authorization Center as described in "Checking your rights and role assignments" on page 13.

Setting a desktop name

By default, new desktops uses the name of the role you select as the desktop name. You can click **Change** if you want to change the name of desktop. For example, you might want to add your name, a computer name, or other information to the information displayed when you left-click the Centrify icon in your system Notification Area to help identify the context when switching from one desktop to another.

After you click **Change**, select **Use the following desktop name**, type the name you want displayed for the desktop, then click **OK**.

Switching from one desktop to another

To switch desktops, click the Centrify icon and select the desktop you want. You can also set up hot keys to switch between desktops using a keystroke combination.

Setting hot keys for switching between desktops

Hot keys are keystroke combinations that enable you to switch between desktops without clicking the Centrify icon or accessing the applet menu. By selecting hot key combinations, you can move from one desktop to another more quickly when you have more than one desktop open at a time.

To set up hot keys for switching between desktops:

1. Click the Centrify icon.
2. Select **Options**.
3. Click the **Hotkey** tab.
4. Select the **Enable Hotkey** option, then select a key or key combination from the list of Modifiers and whether to use a number, function key, or letter from the list of Specifiers.

   For example, if you want to switch from one desktop to another using the ALT and a number, ALT+1 and ALT+2, select Alt from the list of Modifiers and Number from the list of Specifiers.
5. Click **OK**.

Using a desktop with network access rights

When you open a desktop and select a role, you get all of the access rights associated with that role. Depending on how the role is configured, those access rights may be limited to running applications with locally elevated privileges or include access to remote servers on the network. The Centrify icon in the system Notification Area always displays the current Local and Network roles you are using. However, it is up to the administrator to decide whether network access rights should be included in roles that grant desktop access rights.

If roles granting network access rights are defined separately from roles that include desktop access rights, you might have to select your local and network roles separately. In some cases, you might also need to select more than one network role to work with multiple remote computers. To handle these more complex situations, you can use the Advanced View to select the appropriate combination of local and network roles.

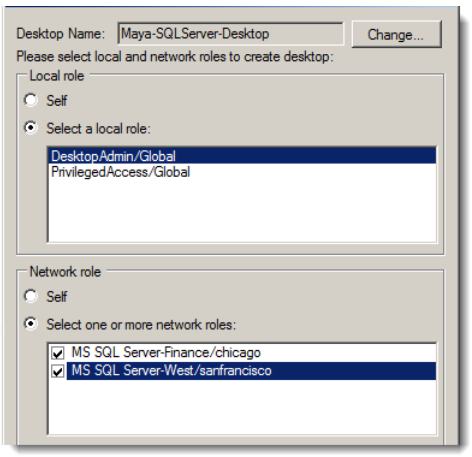
To view and select your local and network roles for a desktop:

1 Open a new desktop.

2 In the Select Role dialog box, click **Advanced View**.

If there are any network roles listed, those roles grant network access rights for specific remote computers. For example, if you are assigned separate roles with network access rights to two separate SQL Server instances, you might see the roles with network access rights listed separately from your roles with local desktop access rights.

Click Advanced View to select network roles



In this example, the `DesktopAdmin` role is a local role that has desktop access rights but does not include any network access rights. By selecting both `MS SQL Server-Finance` and `MS SQL Server-West` network roles, you can create a single local desktop that has remote network access to both SQL Server instances. Alternatively, you could create separate desktops for accessing each SQL Server instance. You can left-click on the Centrify icon in the system Notification Area to view the roles you have selected so that you know whether you have network access rights for one SQL Server instance or both.

3 For the local role, select a role that grants desktop access rights or application access rights on the local computer.

4 Type the password for your login account, if you are prompted for it, then click **OK**.

If your administrator has enabled multi-factor authentication, complete the additional authentication challenges after entering your password.

Closing a desktop

In some cases, you might have multiple desktops open at the same time to allow you to switch between several different roles quickly. If you have more than one desktop open at a time, you can selectively close the desktops you are no longer using.

To close a desktop:

1 Switch to the desktop you want to close.

2 Click the Centrify icon.

3 Select **Close Desktop**.

The agent removes that desktop from your list and returns you to the default desktop. You cannot close your default desktop.

Running a specific application with privileges

With desktop access rights, you can run any application using one of the roles assigned to you. Application access rights are assigned on an application-by-application basis.

If you have a role assignment with application access rights, you can run one or more specific applications using the administrative privileges defined for your role. The administrator defines the specific application rights that you have in each role you are assigned. If you have a role assignment with application access rights, the administrator specifies the location of the application executable, the arguments you can use when running the application, and the account

used when you run application. You can only select a role to run a local application for which you have application rights.

To run a local application using a selected role:

1 Navigate to and select the application you want to run.

2 Right-click the executable or shortcut for the application.

If you want to open the application from the Start menu, press the Shift key when you right-click.

3 Select **Run with Privilege**.

If you have not been assigned to any role that has application access rights for the application you are trying to open, a message is displayed to inform you that you are not a member of any role associated with the selected application.

4 If the Select Role dialog box opens, select a role from your list of available roles, then click **OK**.

Note If there is only one role assigned to you capable of running the application, the application will automatically run using that role. If you would like to access the Select Role dialog box, press the Shift key when you select **Run with Privilege**.

If the application requires network access rights for a remote server, click **Advanced View** to see if you have a role with network access rights available.

5 Type the password for your login account, if you are prompted for it, then click **OK**.

If your administrator has enabled multi-factor authentication, complete the additional authentication challenges after entering your password.

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.

By default, the account a role is configured to use controls the environment variables used when you run applications with the

selected role. You can select **Use current environment variables instead of the "Run As" user's** if you want to use current environment variable settings.

After you select one or more roles, the application opens and an audit trail event is recorded in the Windows Application event log. You can use the application with the privileges granted to the specific user account or administrative group defined for your role. You have the privileges associated with the role or roles you selected until you exit the application. When you close the application, you resume working with your normal account privileges and group membership.

Using the runasrole command line

As an alternative to selecting Run with Privilege from the right-click menu for an application, you can use the `runasrole` command-line program. The `RunAsRole` program enables you to run a specified Windows application in a Command Prompt windows using a specified Centrify access role. You can use command line options to control whether the role is used as a local role, a network role, or both, and whether to use the current environment or the environment variables associated with the "Run As" user account. The `runasrole` command line program is equivalent to selecting the Run with Privilege menu option when right-clicking an application shortcut or executable.

The syntax for the `runasrole` command is:

`runasrole /role:`*`role[/zone]`* `[options]` *`application`* `[`*`argument`*`]`
`runasrole /localrole:`*`role[/zone]`* `[options]` *`application`* `[`*`argument`*`]`
`runasrole /networkrole:`*`role[/zone]`* `[options]` *`application`* `[`*`argument`*`]`

You must specify the role to use in the *`rolename`*/*`zonename`* format. You must also specify an appropriate path to the *`application`* you want to access, including any required or optional arguments.

You can use the following command line arguments with the `runasrole` command:

Use this option	To do this
/role	Use the role name you specify as both a local role and a network role. You can specify this option to run an application locally and access a remote server using the same role, if applicable. You should only use this option if the role you are assigned and want to use has both local and network access rights defined.
/localrole	Use the role name you specify as a local role.
/networkrole	Use the role name you specify as a network role.
/env	Use the current environment variables instead of the environment variables associated with the "Run As" user account.

Use this option	To do this
/netdrives	Use mapped network drives when running an application with the selected role. By default, you cannot use mapped network drives that are associated with you logged-on user account when running applications using a role with elevated privileges. If you want to use a mapped network drive when accessing an application using a selected role, include the /netdrives option in the command line.
/wait	Prevents the `runasrole` program from exiting immediately after opening the specified application. If you specify this option, the `runasrole` program starts the specified application and waits until the application session ends before exiting. When the application session ends, the `runasrole` program exits and returns the same result code as the application. If you specify this option and the application is a command line utility, the `runasrole` program redirects the application's input and output to the command line console. You should note that some applications use a Microsoft API that does not support redirection of standard input and output. For applications that don't support redirection, the `/wait` option has no effect and is ignored.

Examples

To use the same role to open the Computer Management application locally and access a remote server in `zone1`, you might run a command similar to the following:

```
runasrole /role:role1/zone1 mmc.exe
c:\windows\system32\compmgmt.msc
```

To use the role named `SQLdba` from the `finance` zone as a local role to open the Services application, you might run a command similar to the following:

```
runasrole /localrole:SQLdba/finance mmc.exe
c:\windows\system32\services.msc
```

To use `role1` from `zone1` as a local role to open the Computer Management application and use network access rights from `role2` in `zone2`, you might run a command similar to the following:

```
runasrole /localrole:role1/zone1 /networkrole:role2/
zone2 mmc.exe compmgmt.msc
```

To open the Services application using the role named `SQLdba` from the `finance` zone and have the `runasrole` program remain open until you close the Services application, you might run a command similar to the following:

```
runasrole /wait /role:SQLdba/finance mmc.exe
c:\windows\system32\services.msc
```

Running an application from a shortcut

In most cases, you can use the `runasrole` program to run specified Windows applications using the application shortcut. However, there are many different types of application shortcuts and the `RunAsRole` program does not support all of them. You can use the `RunAsRole` program to execute applications with the following recognized shortcut target extensions:

```
.bat
.cmd
.cpl
.exe
.msc
.msi
.msp
.ps1
.vbs
.wsf
```

How to determine whether RunAsRole supports an application shortcut

You can determine whether you can use the `RunAsRole` program to execute an application from the application shortcut by checking the file extension for the target application in the application's shortcut properties dialog box.

To check the file extension for a target application shortcut

1. Select an application shortcut.
2. Right-click the shortcut, then click **Properties** to display the file properties.
3. Click the Shortcut tab and check the target field.

   If the target file extension displayed is a supported file extension, you can use `RunAsRole` to execute the application from the application shortcut. You should note that a shortcut target field might include both the file name for the application executable and one or more arguments. As long as the application executable has a supported file extension, you can use `RunAsRole` to execute the application with the specified arguments from the shortcut. For example, if the shortcut target is `C:\Windows\System32\control.exe printers`, the application executable `C:\Windows\System32\control.exe` is a supported file extension with `printers` supplied as an argument. Therefore, you would be able use `RunAsRole` to run the application from its shortcut.

Selecting roles with network access rights

As discussed in "Using a desktop with network access rights" on page 19 network access rights can be included in roles with other rights or defined separately. Therefore, it is not always possible to see where your rights apply or the scope of your role assignment.

If you are assigned multiple roles, you should work with the administrator to identify which roles grant local and network access rights and the computers where the roles apply. You can see detailed information about the rights associated with each role you are

assigned and the zones where different roles are defined using the Authorization Center. You have less visibility, however, of which computers are in scope for your network access rights.

Selecting a role that is not applicable on a local computer

In some cases, you might have roles that are visible on your local computer in the list of roles you have been assigned that are not applicable on the local computer. You can select the role, but the privileges associated with the role are only granted when you access computers over the network where the assignment applies.

For example, an administrator might create an Exchange Admin role that contains a network access right, and assign you to that role in a zone that only contains Exchange servers or assign you to that role explicitly on the computers that host Exchange.

When you log on to your laptop, the Exchange Admin role is included in your list of available roles even though the assignment is out of scope for the laptop. You can select the Exchange Admin role and continue working on the laptop without elevated privileges.You know that the Exchange server requires maintenance and you are planning to get to it later in the day.

When you are ready to do maintenance on the Exchange server, you connect to the server over the network. At that point, the elevated privileges associated with the Exchange Admin role are applied. The Exchange server you are accessing from your laptop is in scope for where you have been assigned the Exchange Admin role. You complete the maintenance required on the Exchange server with your elevated privileges, then resume working on your laptop where the Exchange Admin role does not apply.

Role-based auditing of session activity

The Centrify agent for Windows can be installed with or without auditing features. Depending on whether auditing features are activated on your computer and whether your role requires auditing or not, your session activity might be captured and stored in a database. You can check whether session-level auditing is requested or required

for the roles you are assigned using Authorization Center. You are only notified that your session activity might be audited if the administrator has enabled notification. If you select a role that requires auditing but auditing features are not available on computer you attempt to use, you will be denied access to that computer until auditing is available.

If session-level auditing is activated, everything you do on your computer is captured, including all of your keystrokes and the screens displayed on the desktops you use. At a minimum, any time you use a role that elevates your privileges on a computer, an audit trail event is recorded in the Windows Application event log.

Working with Server Core computers

Centrify agents can be installed on Windows computers that are configured to run the Server Core operating environment. Server Core is a Windows installation option that provides a low-maintenance server environment with limited functionality.

Most Centrify agent operations are not affected by running on Server Core. However, there are specific features that are not available or not applicable because of the limitations of the Server Core environment itself. For example, the Run with Privilege menu option is not available on Server Core computers because Server Core does not support Windows Explorer and other graphical user interface applications. However, you can use the `runasrole` command line utility to run specific applications using a specified role.

Similarly, there's no Centrify notification area applet or desktop rights available on Server Core computers. However, you can access the Authorization Center, agent control panels, and agent command-line utilities from the Server Core command prompt.

The following list summarizes the Centrify agent for Windows features that are not supported on Server Core computers:

- You cannot create, select, or switch desktops or use any desktop-related features because the Windows desktop is not available on Server Core.
- You cannot select Run with Privilege as a right-click menu option for applications because Windows Explorer is not available on Server Core.
- You cannot open the Authorization Center or access the Centrify notification area applet because the Windows desktop and Windows Explorer are not available on Server Core.
- You cannot open applications such as the DirectAuthorize Agent Control Panel or DirectAudit Agent Control Panel from Start menu shortcuts because the Windows desktop and Windows Explorer are not available on Server Core.

You should note that only Centrify agents for Windows are supported for the Server Core environment. A small number of other Centrify Server Suite components for Windows support a command line interface, but are not configured to support a Server Core environment.

Server Core supported platforms

Centrify supports the following versions of the Server Core environment:

- Windows Server 2008 R2 Server Core
- Windows Server 2012 Server Core
- Windows Server 2012 Minimal Server Interface
- Windows Server 2012 R2 Server Core
- Windows Server 2012 R2 Minimal Server Interface

You should note that Server Core is not supported on Windows Server 2008 because Windows Server 2008 Server Core does not support any version of the .NET Framework. The Centrify agent for Windows requires the .NET Framework. For more information about the supported libraries and .NET functionality on Server Core, see the reference material available on the Microsoft Developer Network website for the operating system you have deployed.

Joining a zone

One of the first tasks after installing the Centrify agent is to join a zone. You can do by launching the DirectAuthorize Agent Control Panel from the command prompt.

To open the DirectAuthorize Agent Control Panel to join a zone:

1. Navigate to the Centrify agent installation directory.

   By default, the agent files are installed in the `C:\Program Files\Centrify\Centrify Agent for Windows` directory.

2. Run `Centrify.DirectAuthorize.Agent.Config.exe`.

3 Click **Join zone**.

4 Type all or part of the zone name, click Find Now, then select the zone to join and click **OK**.

5 Click **Close** to close the control panel.

If you later need to change the zone, run diagnostics, refresh the authorization cache, or view or modify log settings, you can run `Centrify.DirectAuthorize.Agent.Config.exe` to perform those tasks.

Viewing authorization details

By default, access control, privilege management, and auditing features are enabled after you install and configure the Centrify agent for Windows. To see details about your rights, role definitions, role assignments, and auditing status, you can launch the Authorization Center from the command prompt.

To open the Authorization Center on a computer with the Server Core operating system:

1 Navigate to the Centrify agent installation directory.

By default, the agent files are installed in `C:\Program Files\Centrify\Centrify Agent for Windows` directory.

2 Run `Centrify.DirectAuthorize.Auth.Center.exe`.

Configuring auditing options

By default, access control, privilege management, and auditing features are enabled when you install the Centrify agent for Windows. To configure auditing options and specify the audit installation for the agent, you can launch the DirectAudit Agent Control Panel from the command prompt.

To open the DirectAudit Agent Control Panel to configure auditing features:

1 Navigate to the Centrify agent installation directory.

By default, the agent files are installed in the `C:\Program Files\Centrify\Centrify Agent for Windows` directory.

2. Run `agent.configure.exe`.
3. Click **Configure**.
4. Select a color quality, then click **Next**.

   Because the Server Core operating system uses very few graphical elements, in most cases you should accept the default setting of Low for the color quality. This setting minimizes the storage requirements for auditing if you have enabled video capture auditing.
5. Accept the default offline data location and maximum size or type a different location, then click **Next**.

   You can also drag the slider to change the maximum percentage of the drive the offline data can consume. In most cases, however, you should leave the default setting unchanged.
6. Select the audit installation, then click **Next**.
7. Review your configuration settings, then click **Next**.
8. Click **Finish** to close the configuration wizard.
9. Click **Close** to close the control panel.

Running command line programs

The Centrify agent for Windows includes several command line programs for performing administrative tasks. The following command line programs are supported on Server Core computers:

- dzinfo
- dzdiag
- dzrefresh
- dzflush
- dzdump

- runasrole

For more information about the command line options or output for these commands, see the *Administrator's Guide for Windows* or run the command with the `/help` option.

Working with PowerShell cmdlets

If you want to use the Centrify DirectManage Access Module for Windows PowerShell on a Server Core computer, you must have Windows PowerShell, version 2.0 or later, installed before attempting to install the Access module.

To check whether Windows PowerShell is installed

1. Log on to the Server Core computer.
2. Run a command similar to this:

```
DISM /Online /Get-FeatureInfo /
FeatureName:MicrosoftWindowsPowerShell
```

This command returns information similar to the following:

```
...
Feature Name : MicrosoftWindowsPowerShell
Display Name : Windows PowerShell
Description : Adds or Removes Windows PowerShell
Restart Required : Possible
State : Enabled
...
ServerComponent\DisplayName : Windows PowerShell 4.0
...
```

If you have Windows PowerShell, version 2.0 or later, available, you can install the Centrify DirectManage Access Module for Windows PowerShell.

To install the Access Module for Windows PowerShell

1. Copy the Access Module for Windows PowerShell .msi files to the Server Core computer.

   For example:

```
copy D:\DirectManage64\PowerShell\*.msi C:\CentrifyAgent
```

2 Install the Access Module for Windows PowerShell using the `.msi` file.

For example, you might run the following command:

```
msiexec.exe /i "CentrifyDC_PowerShell-5.2.0-win64.msi" /qn /
norestart
```

Troubleshooting

This chapter describes how to resolve issues with logging on, find log files, set the level of detail recorded in log files, and use diagnostic tools to retrieve information about the operation of the Centrify agent for Windows.

The following topics are covered:

- Solving problems with logging on
- Accessing network computers with privileges
- Running diagnostics and viewing logs for the agent
- Refreshing cached information
- Check your rights and roles using dzinfo

Solving problems with logging on

Once you have the Centrify agent installed on your computer, you cannot log on without a role assignment. The role, however, may be assigned to your local account, your domain account, or a remote computer. Consequently, you might encounter problems logging on after the agent is deployed. For example, you might find that you can log on to your computer using your local account but cannot log on using your domain account or have trouble connecting to a remote server.

You have no control over the roles assigned to your local, domain, or remote server accounts. These are all set by the administrator. There are a couple of things you can try if you cannot log on:

- ❑ Try to log on using a local user account or using a different domain account if you have more than one account available.
- ❑ Determine whether the computer you are using is connected or disconnected from the network. In rare cases, authorization information might not be available when a computer disconnected from the network.

- ❑ If you cannot log on to a remote computer, confirm that you have role that has the remote logon system right and that the computer is configured to allow users to log on remotely. Open the Authorization Center to see details about your roles and their rights.

Your administrator is the only person who can correct any log on problems. You should contact an administrator for your organization to proceed.

Accessing network computers with privileges

Depending on how your administrator has defined the roles you are assigned, it is possible for you to see potentially misleading information in certain applications or be unable to perform administrative tasks as you expect. For example, if you select a role with administrative privileges to access an application such as SQL Server Configuration Manager or Microsoft SQL Server Management Studio and connect to a remote SQL Server instances, it might appear as if you have permission to start and stop services or perform other tasks. However, if your role does not include network access rights for the remote SQL Server instance, you will not have the appropriate permission to perform those tasks.

You can check whether your selected role includes network access rights using the Authorization Center. If the role you are using does not include network access rights, you should click **Advanced View** to see if you have additional network roles available to use in conjunction with your local role. If the role you are using includes network access rights, you should contact your administrator to find out if those rights are applicable on the network computer you are attempting to manage.

Running diagnostics and viewing logs for the agent

If you are a local administrator on a managed computer, you can generate diagnostic information about the operation of the Centrify agent and view and save the current content of the log file from the Troubleshooting tab in the Centrify DirectAuthorize Agent Control Panel.

Refreshing cached information

If you are a local administrator on a managed computer, you can refresh the authorization information stored in the cache to ensure the agent has the most up-to-date information about your current rights and roles. For example, if you are assigned a new role or been granted new application rights, you can refresh the cache to get the new assignment or application rights.

Check your rights and roles using dzinfo

You can use the `dzinfo` command line program in a Command Prompt window to view detailed information about your rights, roles, and role assignments. The `dzinfo` command line utility provides the same functionality as the Authorization Center described in "Checking your rights and role assignments" on page 13, but allows you to view and capture the output from the command in a single window.

The syntax for the `dzinfo` program is:

```
dzinfo
```

The command returns detailed information about your rights, roles, and role assignment similar to the following:

```
Effective roles for AJAX\rey.garcia:
   weblogic2/portland
      Zone:
CN=portland,CN=mainoffice,CN=Zones,OU=Centrify,DC=ajax,D
C=org
      Status:  Active

   Domain Admin/portland
      Zone:
CN=portland,CN=mainoffice,CN=Zones,OU=Centrify,DC=ajax,D
C=org
      Status:  Active

   Windows Login/mainoffice
```

```
      Zone:
CN=mainoffice,CN=Zones,OU=Centrify,DC=ajax,DC=org
      Status:  Active

Effective Login Rights for AJAX\rey.garcia:
   Console Login: Permitted
      Audit Level: Audit if possible

   Remote Login: Permitted
      Audit Level: Audit if possible

Role Assignments for AJAX\rey.garcia:
   weblogic2/portland
      Status:        Active
      Account:       AJAX\rey.garcia
      Scope:         Zone
      Zone:          ajax.org/Centrify/Zones/mainoffice/
portland
      Local Role:    No
      Network Role:  Yes
      Effective:     Immediate
      Expires:       Never

   Domain Admin/portland
      Status:        Active
      Account:       AJAX\rey.garcia
      Scope:         Zone
      Zone:          ajax.org/Centrify/Zones/mainoffice/
portland
      Local Role:    No
      Network Role:  Yes
      Effective:     Immediate
      Expires:       Never

   Windows Login/mainoffice
      Status:        Active
      Account:       AJAX\Domain Admins
      Scope:         Zone
      Zone:          ajax.org/Centrify/Zones/mainoffice
```

```
      Local Role:    Yes
      Network Role:  No
      Effective:     Immediate
      Expires:       Never

Role Definitions:
   weblogic2/portland
      Status:          Active
      Description:     None
      Zone:
CN=portland,CN=mainoffice,CN=Zones,OU=Centrify,DC=ajax,D
C=org
      Login Permitted: No
      Audit Level:     Audit if possible
      Rescue Right:    No
      Require MFA:     No
      Available Hours:
                  12  2   4   6   8   10  12  2   4   6
8   10
         Sunday    X X X X X X X X X X X X X X X X X X X X
X X X X X
         Monday    X X X X X X X X X X X X X X X X X X X X
X X X X X
         Tuesday   X X X X X X X X X X X X X X X X X X X X
X X X X X
         Wednesday X X X X X X X X X X X X X X X X X X X X
X X X X X
         Thursday  X X X X X X X X X X X X X X X X X X X X
X X X X X
         Friday    X X X X X X X X X X X X X X X X X X X X
X X X X X
         Saturday  X X X X X X X X X X X X X X X X X X X X
X X X X
      Rights:
         weblogic Network Access/portland
            Type:                    Network Access
            Description:             None
            Priority:                0
            Run As:                  AJAX\wladmin
            Require Authentication: No
```

```
            weblogic Desktop/portland
               Type:                    Desktop
               Description:             None
               Priority:                0
               Run As:                  AJAX\wladmin
               Require Authentication: No

      Domain Admin/portland
         Status:          Active
         Description:     None
         Zone:
CN=portland,CN=mainoffice,CN=Zones,OU=Centrify,DC=ajax,D
C=org
         Login Permitted: No
         Audit Level:     Audit if possible
         Rescue Right:    No
         Available Hours: All
         Rights:
            ADUC/portland
               Type:                    Application
               Description:             Active Directory
Users and Computers as Admin
               Priority:                0
               Run As:                  AJAX\Administrator
               Application:             mmc.exe
               Path:                    C:\Windows\system32
                                        C:\Windows
                                        C:\Program Files
                                        C:\Program Files
(x86)
                                        C:\Windows\SysWOW64
               Arguments:
"C:\Windows\system32\dsa.msc"
               Match Case:              No
               Require Authentication: No

               Application Criteria:
                  None
```

```
            Domain Admin Network Access/portland
               Type:                    Network Access
               Description:             None
               Priority:                0
               Run As:                  AJAX\Administrator
               Require Authentication: No

      Windows Login/mainoffice
         Status:          Active
         Description:     Predefined system role for general
Windows login users.
         Zone:
CN=mainoffice,CN=Zones,OU=Centrify,DC=ajax,DC=org
         Login Permitted: Console and Remote
         Audit Level:     Audit if possible
         Rescue Right:    No
         Available Hours: All
         Rights:
            None

Computer is joined to zone ajax.org/Centrify/Zones/
mainoffice

Auditing for AJAX\rey.garcia:
   Session ID 2:
      Desktops:
         Default: Not currently auditing.

Auditing is not available on this computer.
```

Index

Z