

Administrator's Guide for Windows

September 2020 (release 2020)

Centrify Corporation





Legal Notice

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

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

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

© 2004-2020 Centrifly Corporation. All rights reserved. Portions of Centrifly software are derived from third party or open source software. Copyright and legal notices for these sources are listed separately in the Acknowledgements.txt file included with the software.

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

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

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

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



Contents

| | |
|-------------------------------------------------------------------------------------------------------------------------------|-----------|
| About Centrify Management Services for Windows | 8 |
| Intended audience | 8 |
| Using this guide | 9 |
| Documentation conventions | 10 |
| Finding more information about Centrify products | 11 |
| Product names | 11 |
| Contacting Centrify | 14 |
| Getting additional support | 14 |
| | |
| Introduction to Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service | 15 |
| Managing Windows computers using Centrify software | 16 |
| Access control for Windows computers | 17 |
| How zones organize access rights and roles | 18 |
| How role-based access rights can be used | 19 |
| Auditing user activity on Windows computers | 20 |
| Using access and auditing features together | 21 |
| | |
| Centrify architecture and operation | 22 |
| Identity and privilege management | 22 |
| The audit and monitoring service infrastructure | 25 |
| Basic operation with identity and privilege management, and auditing | 30 |
| | |
| Planning a deployment | 33 |
| Why planning is important | 34 |
| Identify identity, privilege management, and auditing goals | 34 |
| Decide on the scope of the installation | 35 |
| Decide where to install the management database | 35 |



| | |
|----------------------------------------------------------------------------|----|
| Decide where to install collectors and audit stores | 36 |
| Decide where to install agents | 41 |
| Decide where to install consoles | 42 |
| Check SQL Server logins for auditing | 42 |
| What's involved in the deployment process | 43 |
| Authentication and Privilege Elevation services deployment checklist | 49 |
| Accounts and permissions for installation and deployment | 54 |

Installing Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service 62

| | |
|-----------------------------------------------------------------------------------------------------------------------|-----|
| Installation checklist | 63 |
| Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory | 65 |
| Installing and configuring Microsoft SQL Server for auditing | 69 |
| Installing Centrify Audit Manager and Centrify Audit Analyzer consoles | 71 |
| Creating a new installation | 71 |
| Installing and configuring Centrify audit collectors | 79 |
| Installing the Centrify Agent for Windows | 82 |
| Installing additional consoles | 105 |
| Installing group policy extensions separately from Centrify Access Manager | 106 |

Managing zones 109

| | |
|-----------------------------------------------------------|-----|
| Starting Centrify Access Manager for the first time | 109 |
| Preparing to use zones | 113 |
| Creating a new parent zone | 117 |
| Creating child zones | 120 |
| Opening and closing zones | 122 |
| Changing zone properties | 123 |
| Delegating control of administrative tasks | 124 |
| Adding Windows computers to a zone | 127 |



| | |
|-----------------------------------------------|-----|
| Preparing Windows computer accounts | 127 |
| Changing the zone for the computer | 128 |
| Leaving a zone | 128 |
| Renaming a zone | 129 |
| Working directly with managed computers | 131 |

Managing access rights and roles 133

| | |
|-----------------------------------------------------------------------------------------------------|-----|
| Basics of authorization and access rights | 134 |
| Adding predefined rights to a zone | 137 |
| Defining desktop access rights | 140 |
| Defining application rights | 142 |
| Defining network access rights | 159 |
| Defining custom roles with specific rights | 161 |
| Assigning users and groups to a role | 168 |
| Making rights and roles available in other zones | 169 |
| Viewing rights and roles | 171 |
| Scenario: Using a network access role to edit group policies | 173 |
| Scenario: Using multiple roles for network resources | 174 |
| Defining rights for Windows applications that encrypt passwords | 175 |
| Enabling access across multi-tiered application layers | 176 |
| Requiring users to justify privilege elevation | 177 |
| Working with computer roles | 178 |
| Assigning roles on multiple computers at once | 183 |
| Using the Authorization Center directly on managed computers | 185 |
| Working with the authorization cache on managed computers | 186 |
| Configuring PowerShell Remote Access | 190 |
| Authentication service enforcement | 191 |
| Configuring MFA with RADIUS for Centrify Privilege Elevation Service for Windows checklist | 191 |
| Adding remote users automatically | 197 |



| | |
|------------------------------------------------------------------|------------|
| Enabling users to run applications with alternate accounts | 197 |
| Managing local Windows users and groups | 199 |
| Adding local Windows accounts | 199 |
| Enabling Windows local account management | 202 |
| Creating and managing local Windows user passwords | 203 |
| Removing local Windows accounts | 205 |
| Managing auditing and audit permissions | 207 |
| Configuring selective auditing | 207 |
| Enabling audit notification | 209 |
| Managing audit roles and auditors | 210 |
| How access roles and audit roles differ | 213 |
| Managing auditing for an installation | 216 |
| Securing an installation | 216 |
| Setting administrative permissions | 222 |
| Managing audit stores | 225 |
| Managing audit store databases | 227 |
| Managing the management database | 235 |
| Managing collectors | 237 |
| Managing audited computers and agents | 240 |
| Adding an installation | 242 |
| Removing or deleting an installation | 244 |
| Troubleshooting and common questions | 246 |
| Solving problems with logging on | 247 |
| Accessing network computers with privileges | 248 |
| Refreshing cached information on managed computers | 249 |



| | |
|-----------------------------------------------------------------------------|-----|
| Analyzing information in Active Directory | 249 |
| Running diagnostics and viewing logs for the agent | 251 |
| Enabling detailed logging for audit and monitoring service components | 255 |
| Tracking database activity | 258 |
| Controlling audit trail events | 261 |
| Offline MFA profile authentication | 263 |
| Centrify Authentication Service known issues | 263 |

Using Windows command line programs265

| | |
|-------------------------------------------|-----|
| Using CopyGroup and CopyGroupNested | 265 |
| Using dzinfo | 266 |
| Using dzjoin | 270 |
| Using dzleave | 271 |
| Using dzdiag | 271 |
| Using dzrefresh | 273 |
| Using dzflush | 274 |
| Using dzdump | 274 |
| Using runasrole | 276 |

Working with Server Core and Windows Server 2012 280

| | |
|--------------------------------------------------------------|-----|
| Server Core supported platforms | 281 |
| Installing the agent on a computer running Server Core | 282 |
| Opening consoles on Server Core computers | 283 |
| Joining a zone | 283 |
| Viewing authorization details | 284 |
| Configuring auditing options | 284 |
| Running command line programs | 285 |
| Unsupported Windows Server 2012 features | 286 |



About Centrify Management Services for Windows

The *Administrator's Guide for Windows* describes how to install and configure Centrify software to manage access rights granted through the authentication service, elevated permissions granted through the privilege elevation service, and role-based audit and monitoring service for Windows computers. This guide focuses exclusively on the management of rights, roles, role assignments, privileges for application and network resources, and audit and monitoring service requirements that apply to Windows computers. If you manage a heterogeneous environment that includes Linux, UNIX, and Mac OS X computers, you should check for additional information in the other guides that make up the Centrify documentation set.

Intended audience

The *Administrator's Guide for Windows* provides information to ensure a successful installation of Centrify components and describes how to use Centrify to manage access to desktop, application, and network resources, and audit user activity on Windows computers. The guide is intended for administrators who are responsible for installing and configuring software on Windows computers, and for administrators who manage access to and monitor user activity on Windows servers. The guide also includes information intended for security administrators and auditors who are responsible for identifying audit requirements, querying the audit store databases, examining user activity, and flagging sessions for follow-up.

This guide is not intended for end-users or administrators who have been granted specific rights or role assignments by a senior administrator. If you are



a user who has been assigned one or more roles, see the *User's Guide for Windows* for information about how you can select and use the roles you have been assigned.

For information about planning a deployment and installing Centrify in a heterogeneous environment that includes Linux, UNIX, and Mac OS X computers in addition to Windows computers, see the *Planning and Deployment Guide*

Using this guide

Depending on your role and responsibilities, you may want to read portions of this guide selectively. For example, if you are only interested in deploying components for authentication and privilege elevation, you can skip all of the chapters and sections about configuring and managing an installation for audit and monitoring service.

The guide is organized into the following sections:

- **Introduction to Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service** provides an overview of the key features and benefits of using Centrify software to manage privileged access on Windows computers.
- **Centrify architecture and operation** describes the Centrify architecture and how components of authentication, privilege elevation, and audit and monitoring services provide audit and monitoring service, authentication and privilege elevation services for Windows computers.
- **Planning a deployment** describes the decisions and tasks involved in a typical deployment project that includes audit and monitoring service, authentication and privilege elevation.
- **Installing Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service** describes how to install Centrify on the Windows computers you plan to use for administration and on the computers you plan to manage.
- **Managing zones** describes how to create and use zones to control access to the computers in your organization.
- **Managing access rights and roles** describes how to define access rights with elevated privileges for users in different roles in the organization and



how to assign users and groups to the appropriate roles to enforce the rules you define.

- **Managing auditing and audit permissions** explains how to configure audit and monitoring service and define audit roles.
- **Managing auditing for an installation** describes how to manage the multi-tiered audit and monitoring service infrastructure.
- **Troubleshooting and common questions** describes where to find log files and how to generate diagnostic information.
- **Using Windows command line programs** describes the command line programs you can use to perform administrative operations on managed computers.
- **Working with Server Core and Windows Server 2012** describes support for Windows Server 2008 R2 and Windows Server 2012 Server Core environments and unsupported features.

In addition to these chapters, an index is provided for your reference.

Documentation conventions

The following conventions are used in Centrify documentation:

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



Finding more information about Centrify products

Centrify provides extensive documentation targeted for specific audiences, functional roles, or topics of interest. If you want to learn more about Centrify and Centrify products and features, start by visiting the [Centrify website](#). From the Centrify website, you can download data sheets and evaluation software, view video demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.

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

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

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

Product names

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

| Current Overall Product Name | Current Services Available |
|-------------------------------------|--------------------------------------|
| Centrify Identity-Centric PAM | Privileged Access Service |
| | Gateway Session Audit and Monitoring |
| | Authentication Service |
| | Privilege Elevation Service |
| | Audit and Monitoring Service |
| | Privilege Threat Analytics Service |

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



| Previous Product Offering | Previous Product Offering | Description | Current Product Offering |
|-------------------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Centrify Privileged Service (CPS) | | Privileged Access Service |
| DirectControl (DC) | | | Authentication Service |
| DirectAuthorize (DZ or DZwin) | | | Privilege Elevation Service |
| DirectAudit (DA) | | | Audit and Monitoring Service |
| | Infrastructure Services | | Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service, and Privilege Threat Analytics Service |
| DirectManage (DM) | Management Services | Consoles that are used by all 3 services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service | |
| DirectSecure (DS) | Isolation and Encryption Service | | Still supported but no longer being developed or updated |
| | User Analytics Service | | Privilege Threat Analytics Service |
| Deployment Manager | | Deployment Manager provided a centralized console for discovering, analyzing, and managing remote computers. This feature is no longer included starting with Infrastructure Services release 19.6. | |

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



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



Contacting Centrify

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

Getting additional support

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

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



Introduction to Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service

Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service is an IT management solution that provides three main services:

- Access control, provided through the Centrify Authentication Service.
- Privilege management, provided through the Centrify Privilege Elevation Service.
- Auditing, provided through Centrify Audit & Monitoring Service.

These services can be used together or independently, depending on the requirements of your organization.

The following topics are covered:

| | |
|----------------------------------------------------------|----|
| Managing Windows computers using Centrify software | 16 |
| Access control for Windows computers | 17 |
| How zones organize access rights and roles | 18 |
| How role-based access rights can be used | 19 |
| Auditing user activity on Windows computers | 20 |
| Using access and auditing features together | 21 |



Managing Windows computers using Centrify software

Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service is a security platform that includes multiple components for managing Windows computers. The components fall into two broad categories of features:

- Access-related components for managing access, including administrative privileges.
- Audit-related components for managing and analyzing audited activity.

Access-related features

Access-related features are provided by the Centrify Authentication Service and the Centrify Privilege Elevation Service. Together, these services enable you to manage access and administrative privileges for the computers in your organization. The primary tool for managing access-related features is Access Manager.

Access Manager provides a central console for defining and managing role-based access control rules and applying them to specific users, groups, or computers. For example, you can use Access Manager to delegate specific administrative tasks to a particular user or group. As an administrator, you can also use Access Manager to configure roles with start and expiration dates or limit the availability of a role to specific days of the week or hours of the day.

Audit-related features

Audit-related features are provided by the Centrify Audit & Monitoring Service. This service enables you to collect and store audit trails that capture detailed information about user activity. The primary tool for managing audit-related features is Audit Manager.

Audit Manager provides a central console for configuring and managing audited computers, audit store databases, and the permissions granted to specific auditors. There is also a separate Audit Analyzer console for searching and replaying captured activity.



Choosing access and auditing features

In addition to the management tools for access-related or auditing-related features, each computer you want to manage must have a Centrify agent installed. After you install the agent, you choose whether to enable access features, auditing features, or both feature sets.

If you enable access features, the agent enforces the role-based privileges that enable users to run applications locally with administrative privileges without using the Administrator password and with their activity traceable to their own account credentials. You can also use role-based privileges to secure access to network services on remote computers.

If you enable auditing features, the agent captures detailed information about what users do when they access applications or network resources with administrative privileges.

You can use access features and components without auditing if you aren't interested in collecting and storing information about session activities. You can also deploy auditing features and components without access control and privilege elevation features if you are only interested in auditing activity on Windows computers. However, the real value of using Centrify to manage Windows computers comes from using all of the services as an integrated solution for managing elevated privileges and ensuring accountability and regulatory compliance across all platforms in your organization.

Access control for Windows computers

By using Access Manager and deploying the Centrify agents for Windows, you can develop fine-grained control over who has access to the Windows computers in your organization. You can also limit the use of administrative accounts and passwords. For example, you can restrict access to computers that host administrative applications or data center services and ensure that users accessing those computers can log on locally or connect remotely only when appropriate.

In a Windows environment without Centrify, the primary way you secure access to Windows computers is by granting a limited number of users or groups local or domain administrator privileges. The main drawback of this approach is that the rights associated with group membership don't change. A user who has domain administrator rights has those rights on any computer in the domain at



all times. In other cases, users who aren't administrators or members of an administrative group need administrative privileges to perform specific tasks that would require them to have an administrator and service account password. Shared passwords reduce accountability and are often flagged by auditors as a security issue.

Through the use of zones and roles, Centrify provides granular control over **who** can do **what**, and over **where** and **when** those users should be granted elevated privileges.

One way trust environments

Windows agent supports one-way trust in the following scenarios:

- When the zone belongs to the resource forest.
- When the logon account belongs to the account forest.
- When the RunAs account or group belongs to the resource forest (RunAs group can be a built-in group).
- When the role assignment is at the zone, computer, or computer role level.

How zones organize access rights and roles

One of the most important aspects of managing computers with Centrify software is the ability to organize computers, users, groups and other information about your organization into **Centrify zones**. A Centrify zone is a logical object created using Access Manager that is stored in Active Directory. You use zones to organize computers, rights, roles, security policies, and other information into logical groups. These logical groups can be based on any organizing principle you find useful. For example, you can use zones to describe natural administrative boundaries within your organization, such as different lines of business, functional departments, or geographic locations.

Zones provide the first level of refinement for access control, privilege management, and the delegation of administrative authority. For example, you can use zones to create logical groups of Windows computers to achieve these goals:

- Control who can log on to specific computers.
- Grant elevated rights or restrict what users can do on specific computers.



- Manage role definitions, including availability and auditing rules, and role assignments on specific computers.
- Delegate administrative tasks to implement “separation of duties” management policies.

You can also create zones in a hierarchical structure of parent and child zones to enable the inheritance of rights, roles, and role assignments from one zone to another or to restrict local or remote access to specific computers for specific users or groups.

Because zones enable you to grant specific rights to users in specific roles on specific computers, you can use zones as the first level of refinement for controlling who has access to which computers, where administrative privileges are granted, and time restrictions on when administrative privileges can be used.

You can also use zones to establish an appropriate separation of duties by delegating specific administrative tasks to specific users or groups on a zone-by-zone basis. With zones, administrators can be given the authority to manage a given set of computers and users without granting them permission to perform actions on computers in other zones or giving them access to other Active Directory objects.

How role-based access rights can be used

Role-based access rights are more flexible than Active Directory group membership because Active Directory groups provide static permissions. For example, if Jonah is a member the Active Directory Backup Operators group, he has all of the permissions defined for members of that group regardless of when or where he logs on to computers in the forest. In contrast, role assignments can be scheduled to start and end, apply only during specific hours, or only be available on specific computers. For example, Jonah may only be in the Backup Operators role on a specific computer or only on weekends.

Role-based access rights also prevent password sharing for privileged accounts, helping to ensure accountability. Users who need to be able to launch applications with elevated privileges can log on with their regular account credentials but run the application using an appropriate role without being prompted to provide the administrative password. For example, if Angela is assigned a role that enables her to run Disk Defragmenter using elevated privileges, she can log on with her normal credentials and select the role that



enables her to run Disk Defragmenter without being prompted to provide an administrator user name and password.

Auditing user activity on Windows computers

Just as it is important to protect assets and resources from unauthorized access, it is equally important to track what users who have permission to access those resources have done. For users who have privileged access to computers and applications with sensitive information, auditing helps ensure accountability and improve regulatory compliance. With Centrify audit and monitoring service, you can capture detailed information about user activity and all of the events that occurred while a user was logged on to an audited computer.

If you choose to enable audit and monitoring service on Windows computers, the Centrify agent starts recording user activity when a user selects a role or logs on to a computer. The agent continues recording until the user logs out or the computer is locked because of inactivity. The user activity captured includes an audit trail of the actions a user has taken and a video record of the applications opened, any text that was entered, and the results that were displayed on the screen. Because information about user activity, called a **session**, is collected as it happens, you can monitor computers for suspicious activity or troubleshoot problems immediately after they occur.

When users start a new session on an audited computer, they can be notified that their session is being audited and they cannot turn off auditing except by logging off. The information recorded is then 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 that may have led to a service degradation or outage.

In addition to saving video record of user activity, sessions provide a summary of actions taken so that you can scan for potentially interesting or damaging actions without playing back a complete session. After you select a session of interest in the Audit Analyzer, the console displays an indexed list of actions taken in the order in which they occurred. You can then select any entry in the list to start viewing the session beginning with that action. For example, if a user opened an application that stores credit card information, you can scan the list of actions for the launch of that application and begin reviewing what happened in the session from that time until the user closed that application.



If users change their account permissions to take any action with elevated privileges, the change is recorded as an audit trail event. You can search for these events to find sessions of interest.

Using access and auditing features together

If you use Centrify access and audit and monitoring service features together, you can define role-based access rights, restrict when and where roles are available, identify roles that should be audited, trace activity when roles with elevated permissions are selected and used, and play back session activity based on the criteria you choose. However, audit and monitoring service requires database storage for the audited sessions and management of network communication for collecting and transferring audited sessions from computers being audited to one or more databases where the sessions are stored. You also need to decide which roles should require audit and monitoring service and the computers you want to audit.



Centrify architecture and operation

This chapter provides an overview of the Centrify architecture for identity management, privilege elevation, and auditing on Windows computers.

The following topics are covered:

| | |
|----------------------------------------------------------------------------|----|
| Identity and privilege management | 22 |
| The audit and monitoring service infrastructure | 25 |
| Basic operation with identity and privilege management, and auditing | 30 |

Identity and privilege management

In Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service, the authentication service and privilege elevation service provide role-based access control and privilege management for Windows computers. For administration, the services provide tools that help you define and manage access rights and roles for Active Directory users and groups. To enforce the rights and roles you define, you install an agent on each server or workstation to be managed.

Defining rights and roles using Access Manager

When you install authentication, privilege elevation, and audit and monitoring services, you choose the components you want to enable. For identity and privilege management, the key component for administration is the Access Manager console. Although there are other ways to define and manage access rights, roles, and role assignments, Access Manager is the primary tool for



Access Manager, you can:

- Create and manage zones to control access to all of the computers you support, including Windows, UNIX, Linux, and Mac OS X computers.
- Set and modify specific types of access right for users and groups.
- Add and customize the role definitions available in different zones, including any time restrictions on when roles are available or cannot be used.
- Assign and manage roles for individual Active Directory user or Active Directory groups.
- Associate groups of computers that share a common function or attribute with users who have a specific role assignment.
- Generate and view reports describing the users, groups, computers, and applications you are managing and which users and groups have access to which computers.
- View and manage licenses for servers and workstations.

Enforcement of rights and roles by the agent

For identity and privilege management, the key component for deployment is the Centrify agent for Windows. After you install the agent on a server or workstation and identify a zone for the computer to join, the computer becomes a **Centrify-managed computer**. If you have enabled access management features for the agent, you can then define access rights and role-based policies to control what different sets of users can do on those computers in each zone.

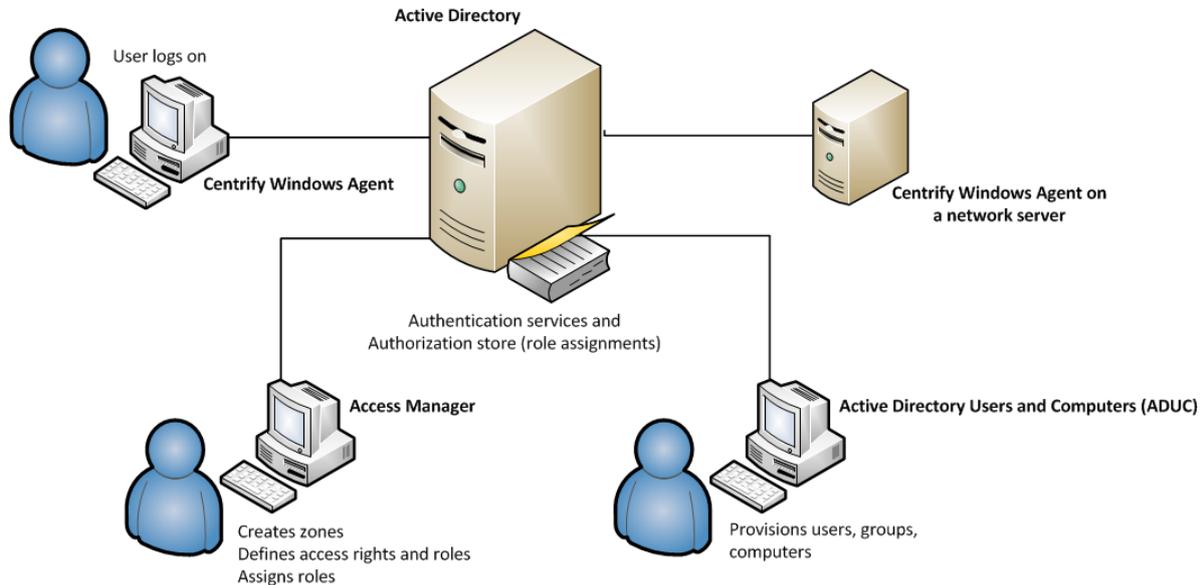
After you deploy the Centrify agent for Windows and select access management on a computer, the agent provides the following identity and privilege management features:

- Users logging on to the computer must be assigned to a role that allows them to log on.
- Users who are assigned to a role with **application rights** can run a specific application with elevated privileges.
- Users who are assigned to a role with **desktop rights** can create new Windows desktops that enables them to run all local applications with elevated privileges.



- Users who are assigned to a role with **network access rights** can connect to network resources with elevated privileges.

The following illustration provides a simplified view of the components for identity and privilege management.



In this illustration, a Centrify agent is installed on an individual user's workstation and on a server accessed remotely. The administrative consoles that you use to manage zones, access rights, role definitions, and Active Directory accounts are installed on two separate computers. As shown in the illustration, all of these computers are part of an Active Directory domain and have access to an Active Directory domain controller. If you work with other platforms, the architecture is the same but you would have additional platform-specific agents.

To ensure that you can centrally manage access to Windows computers with the privilege elevation service and the Centrify agent for Windows, you should check that your network meets a few basic requirements:

- You have at least one Active Directory forest and domain controller.
- All of the computers you want to manage must be joined to an Active Directory domain and can communicate with an Active Directory domain controller over the network or through a firewall.
- You have a basic deployment plan in place that identifies your primary goals, team members and responsibilities, and a target set of computers.



The audit and monitoring service infrastructure

The Centrify Audit & Monitoring Service is part of Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service. The service captures detailed information about user activity on the computers you choose to audit.

Auditing captures user activity

After you deploy audit and monitoring service, the Centrify agent for Windows captures all of the user activity on the computers you choose to audit. Depending on whether you enable identity and privilege management together with audit and monitoring service, or just audit and monitoring service on a computer, the agent starts recording user activity when a user selects a role or logs on to a computer and continues recording until the user logs out or the computer is locked because of inactivity. If you enable identity and privilege management together with audit and monitoring service on a computer, the agent records user activity when a role without audit and monitoring service is used. If you only enable audit and monitoring service on a computer, all user activity is captured by default.

Each record of continuous user activity is called a **session**, and starts as soon as users log on, whether they log on locally, using a Windows Remote Desktop connection, through a virtual network connection such as Citrix or VNC, or using any other type of remote access software. A session ends when the user logs out, disconnects, or is inactive long enough to lock the desktop. If the user reconnects to a disconnected desktop or unlocks the desktop, the agent resumes recording the user's activity as a new session. Each session is a video record of everything that takes place on the user's desktop during a period of user activity.

Auditing requires a scalable architecture

To ensure scalability for large organizations and fault tolerance, audit and monitoring service has a multi-tier architecture that consists of the following layers:

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



features enabled, and be joined to an Active Directory domain.

- **Collectors** are intermediate services that receive and compress the captured activity from the agents on audited computers as it occurs. You should establish at least two collectors to ensure that audit and monitoring service is not interrupted. You can add collectors to your installation at any time, and it is common to have multiple collectors to provide load balancing and redundancy.
- **Audit stores** define a scope for audit and monitoring service and include the audit store databases that receive captured activity and audit trail records from the collectors and store it for querying and playback. Audit store databases also keep track of all the agents and collectors you deploy. For scalability and network efficiency, you can have multiple audit stores each with multiple databases.
- A **management database server** is a computer that hosts the Microsoft SQL Server instance with the audit management database. The management database stores information about the overall installation, such as the scope of each audit store, which audit store database is active, where there are attached databases, the audit roles you create, and the permissions you define. The management database enables centralized monitoring and reporting across all audit stores, collectors, and audited computers.
- **Audit Manager** and **Audit Analyzer consoles** are the graphical user interfaces which administrators can use to configure and manage the deployment of audit components, such as agents and collectors, or query and review captured user sessions.
- A **reporting database** collects data from audit stores and the management database and saves the data in a format that is optimized for reporting. With the reporting database, you can generate event notifications, such as when an audited system goes offline.

To ensure that audit data transferred over the network is secure, communication between components is authenticated and encrypted.

In addition to these core components of the audit and monitoring service infrastructure, there is a separate Windows service that is optional to collect audit trail events when there are audit store databases that are not accessible, for example, because of network issues or the database server is shut down. This audit management service pools the events on the management database, then sends them to the audit store database when the inaccessible database comes back online.

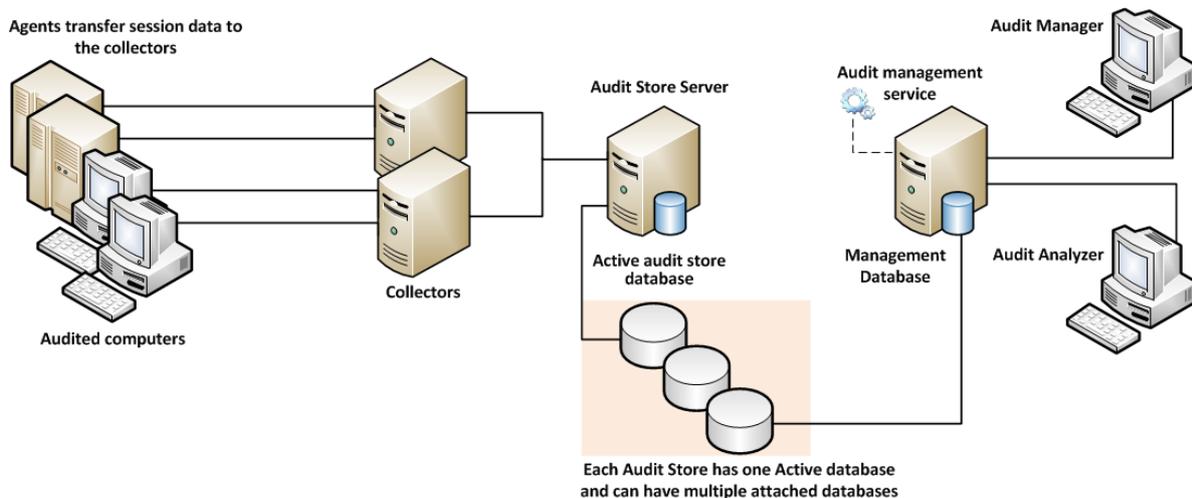


How audited sessions are collected and stored

The agent on each audited computer captures user activity and forwards it to a collector on a Windows computer. If the agent cannot connect to a collector—for example, because all of the computers hosting the collector service for the agent are shut down for maintenance—the agent spools the session data locally and transfers it to a collector later. The collector sends the data to an audit store server, where the audit data is stored in the Microsoft SQL Server database that you have designated as the **active audit store**. As you accumulate data, you can add more SQL Server databases to the audit store to hold historical information or to change the database designated as the active audit store database.

When an administrator or auditor uses the Audit Analyzer console to request session data, the audit management server retrieves it from the appropriate audit store.

The following figure illustrates the basic architecture and flow of data with a minimum number of audit and monitoring service components installed.



In the illustration, each agent connects to one collector. In a production environment, you can configure agents to allow connections to additional collectors for redundancy and load balancing or to prevent connections between specific agents and collectors. You can also add audit stores and configure which connections are allowed or restricted. The size and complexity of the auditing infrastructure depends on how you want to optimize your network topology, how many computers you are audit and monitoring service, how much audit data you want to collect and store, and how long you plan to retain audit records.



Deploying the audit and monitoring service infrastructure

The multi-tiered architecture of audit and monitoring service requires that you deploy an audit and monitoring service infrastructure to transfer and store the information captured by agents on the audited computers. This auditing infrastructure is referred to collectively as an **Auditing installation**. The audit and monitoring service installation represents a logical boundary similar to an Active Directory forest or site. It encompasses all of the audit and monitoring service components you have installed—agents, collectors, audit stores, management database, and consoles—regardless of how they are distributed on your network. The installation also defines the scope of audit data available. All queries and reports are against the audit data contained within the installation boundary.

The most common deployment scenario is to have a single audit and monitoring service installation for an entire organization so that all audit data and management of the audit data is centralized. Within a single audit and monitoring service installation, you can have components wherever they are needed, as long as you have the appropriate network connections that allow them to communicate with each other. The audit data for the entire installation is available to users who have permission to query and view it using a console. For most organizations, having a single audit and monitoring service installation is a scalable solution that allows a “separation of duties” security model through the use of audit roles. If you establish a single audit and monitoring service installation, there will be one Master Auditor role for the entire organization, and that Master Auditor can control the audit data that others users and groups can see or respond to by defining roles that limit access rights and privileges.

However, if you have different lines of business with different audit policies, in different geographic locations, or with different administrative groups, you can configure them as separate audit and monitoring service installations. For example, if you have offices in North America and Hong Kong managed by two different IT teams—IT-US and IT-HK—you might want to create two installations to maintain your existing separation of duties for the IT-US and IT-HK teams.

Planning where to install audit and monitoring service components

Before you install audit and monitoring service components, you should develop a basic deployment plan for how you will distribute and manage the components that make up an installation. For example, you should decide how many collectors and audit stores to create and where to put them. You should



also consider the network connections required and how many computers you plan to audit. For example, you can have multiple agents using the same set of collectors, but you should keep the collectors within one hop of the agents they serve and within one hop of the audit stores to which they transfer data.

By planning where to install components initially, you can determine the number of collectors you should have for load balancing or redundancy. After the initial deployment, you can add collectors and audit stores whenever and wherever they are needed.

Using multiple databases in an audit store

Each audit store uses Microsoft SQL Server to provide database services to the installation. When you configure the first audit store, you identify the database instance to use for audit and monitoring service and that database becomes the active database for storing incoming audit data. A single audit store, however, can have several databases attached to it. Attached databases store historical information and respond to queries from the management database. You can use the Audit Manager console to control the databases that are attached and to designate which database is active. Only one database can be active in an audit store at any given time.

Although the audit store can use multiple databases, the presentation of session data is not affected. If a session spans two or more databases that are attached to the audit store, the Audit Analyzer console presents the data as a single, unbroken session. For example, if you change the active database during a session, some of the session data is stored in the attached database that is no longer active and some of it stored in the newly activated database, but the session data plays back as a single session to the auditor.

Using multiple consoles in an installation

A single audit installation always has a single audit management server and database. In most cases, however, you use more than one console to request data from the audit management database. The two most important consoles in an installation are the Audit Manager console and the Audit Analyzer console.

- As an installation owner, you use the Audit Manager console to configure and manage the audit installation. In most organizations, there is only one Audit Manager console installed.
- Auditors and administrators use the Audit Analyzer console to search, retrieve, play back, and delete sessions. The auditor can use predefined

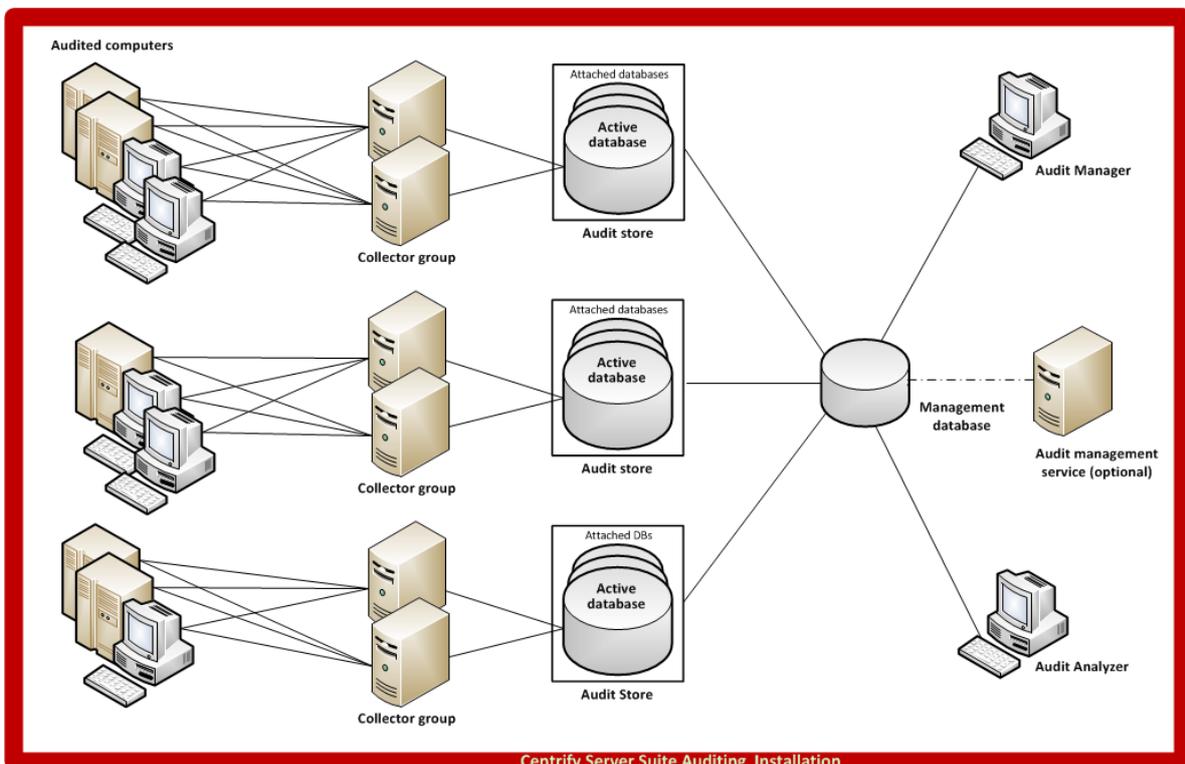


queries to find sessions or define new queries. Auditors can also choose whether to share their queries with other auditors or keep them private. In most organizations, there are multiple Audit Analyzer consoles installed.

In addition to the Audit Manager and Audit Analyzer consoles, audit and monitoring service includes a settings control panel and a collector control panel.

- As an administrator, you can use the Centrifys Audit & Monitoring Service Settings control panel to configure the agent on Windows. Normal users who log on and run applications on the audited computer cannot stop, pause, restart, or configure the agent.
- You can use the collector control panel to configure a collector.

The following illustration is an example of the architecture of a medium-size installation.



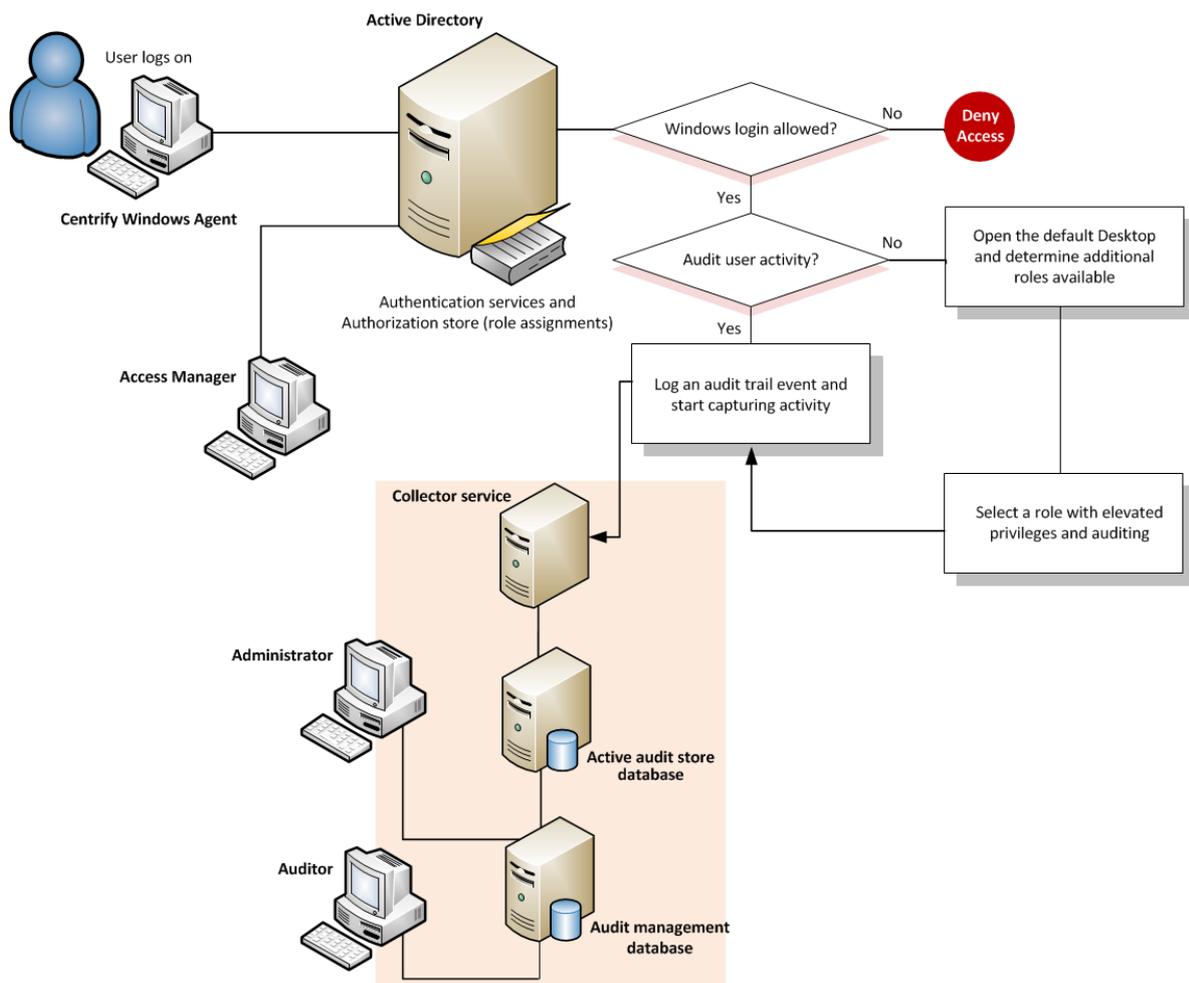
Basic operation with identity and privilege management, and auditing

When you combine identity and privilege management together with auditing on the same computer, you have an audit trail and video record of actions



performed with elevated privileges. For example, when you deploy identity and privilege management features, users must be assigned to a role with permission to log on. If they are allowed to log on and audit and monitoring service is deployed, the agent begins auditing their activity. If a user creates a new desktop, opens a protected application, or connects to services on a remote network server with administrative or service account privileges, the action is recorded and can be traced back to the account used to log on.

The following illustration provides a simplified view of the architecture and flow of data when you deploy components for identity management, privilege management, and auditing.



Although it is not depicted in the illustration, the audit trail records every successful or failed attempt to use a role, including the login role. You do not have to enable audit and monitoring service for a role to record this information. Every computer that has the Centrify agent for Windows records the use of elevated privileges by default. If you do enable audit and monitoring service for a role, however, you can record all of the user activity after the user switches to the audited role. With audit and monitoring service enabled, the audit trail and



the user activity are stored in the database and available for display and analysis anywhere you install the Audit Analyzer console. Without audit and monitoring service, the audit trail is only available in the Windows event log on the local computer where the activity took place.



Planning a deployment

This chapter describes the decisions you need to make during the planning phase of a deployment and summarizes what's involved in deploying identity management, privilege management, audit and monitoring service, and Centrify agents. It includes simplified diagrams that highlight the steps involved.

Because of its multi-tier architecture and storage requirements, most of the information in this chapter applies to planning a deployment of audit and monitoring service. If you are only interested in deploying identity and privilege management without auditing, you should scan [What's involved in the deployment process](#) for relevant topics and continue to [Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory](#).

The following topics are covered:

| | |
|----------------------------------------------------------------------------|----|
| Why planning is important | 34 |
| Identify identity, privilege management, and auditing goals | 34 |
| Decide on the scope of the installation | 35 |
| Decide where to install the management database | 35 |
| Decide where to install collectors and audit stores | 36 |
| Decide where to install agents | 41 |
| Decide where to install consoles | 42 |
| Check SQL Server logins for auditing | 42 |
| What's involved in the deployment process | 43 |
| Authentication and Privilege Elevation services deployment checklist | 49 |
| Accounts and permissions for installation and deployment | 54 |



Why planning is important

Deploying Centrify software on Windows affects how users access local applications and remote services. These changes will become a critical part of your IT infrastructure and the management of your organization's resources. Therefore, it is important that you plan and test your deployment strategy and validate the results before placing Centrify components into a production environment.

After you deploy Centrify in a production environment, the rights and roles you define will control whether users can log on and what they can do on specific computers if they are allowed to log on. Because preventing users from accessing critical resources or services can affect business operations, you should analyze the requirements of your environment as thoroughly as possible before moving from a pilot deployment into production.

Identify identity, privilege management, and auditing goals

As discussed in [Managing Windows computers using Centrify software](#), you have the option of focusing your deployment on identity and privilege management, or on audit and monitoring service, or on a combination of the two. If you plan to install components for identity and privilege management together with audit and monitoring service, you can use roles and role assignments to control which users and groups are audited and under what circumstances auditing takes place. You can also capture detailed information about what happened after a user selected a role with domain administrator privileges or started an application using a service account.

During the planning phase, you should decide on the goals of your deployment—identity and privilege management, audit and monitoring service, or both—because that decision affects all of the other decisions you need to make. If you plan to include audit and monitoring service, you should also start to identify who and what you want to audit, any roles where no auditing should be done, and any roles that will require auditing.



Decide on the scope of the installation

Before you deploy any of the audit and monitoring service infrastructure, you should decide on the scope of the installation and whether you want to use a single installation for your entire Active Directory site, or separate installations for different geographical areas or functional groups.

The most common deployment is a single audit and monitoring service installation for each Active Directory forest, so that auditors can query and review information for the entire organization. However, if your Active Directory site has more than one forest, you might want to use more than one audit and monitoring service installation. If you want to use more than one audit and monitoring service installation, you should determine the subnetwork segments that will define the scope of each installation.

In Active Directory, a site represents the collection of Internet Protocol (IP) addresses that describe the physical structure of your network. If you are not familiar with how Active Directory sites are defined, you should consult Microsoft documentation for more information.

Decide where to install the management database

Each installation has a single audit management server and database. The management database is a Microsoft SQL Server database that stores information about the installation such as the Active Directory sites or subnets associated with each audit store.

The computer you use for the audit management database should have reliable, high-speed network connectivity. The management database does not store the captured sessions, and is, therefore, much smaller than the audit store databases. There are no specific sizing requirements or recommendations for the management database.

You can use the following guideline as the recommended hardware configuration for the computer you use as the management database:

| Computer used for | Number of concurrent sessions | CPU cores | CPU speed | Memory |
|--------------------------|--------------------------------------|------------------|------------------|---------------|
| Management database | Any | 1 to 2 | 2.33 GHz | 8 GB |



Decide where to install collectors and audit stores

Although a collector and an audit store database can be installed on the same computer for evaluation, you should avoid doing so in a production environment. As part of the planning process, therefore, you need to decide where to install collectors and audit store databases. In designing the network topology for the audit and monitoring service installation, there are several factors to consider. For example, you should consider the following:

- Database load and capacity
- Network connectivity
- Port requirements
- Active Directory requirements

The next sections provide guidelines and recommendations to help you decide where to install the collectors and audit store databases required to support the number of computers you plan to audit.

Use separate computers for collectors and audit store databases

To avoid overloading the computers that host collectors and audit store databases, you should install collectors and audit store SQL Server databases on separate computers. Because SQL Server uses physical memory to store database information for fast query results, you should use a dedicated computer for the audit store database, and allocate up to 80% of the computer's memory to SQL Server. In most installations, you also need to plan for more than one audit store database and to periodically rotate from one database to another to prevent any one database from getting too large. For more information about managing audit store databases, see [Managing audit store databases](#).

Plan for network traffic and data storage

You should minimize the distance network packets have to travel between an agent and its collector. You should also minimize the distance between collectors and their audit stores. If possible, you should not have more than one gateway or router hop between an agent and its collector.



Default ports for network traffic and communication

To help you plan for network traffic, the following provides an overview of the network communications and ports used when a user logs on and the ports used in the initial set of network transactions.

When a user logs on, the Centrify agent for Windows connects to Active Directory to begin the lookup process, then the agent and the domain controller exchange messages as follows:

- Directory Service - Global Catalog lookup request on port 3268.
- Authentication Services - LDAP sealed request on port 389.
- Kerberos – Ticket Granting Ticket (TGT) request on port 88.
- Network Time Protocol (NTP) Server – Time synchronized for Kerberos on port 123.
- Domain Name Service (DNS) – Host (A), Pointer (PTR), Service Location (SRV) records on port 53.
- RPC over TCP - For inbound RPC endpoint mapper connections to support network discovery or if password management and validation uses RPC over TCP on port 135.

Depending on the specific components you deploy and operations performed, you might need to open additional ports. The following table summarizes the ports used for different editions of Centrify software.

| This port | Is used for | Centrify software and operation requiring this port |
|-----------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 22 | Encrypted TCP communication for OpenSSH connections | Centrify authentication service and privilege elevation service for secure shell connections on remote clients. |
| 23 | TCP communication for Telnet connections | Centrify authentication service, privilege elevation service, and audit and monitoring service. By default, telnet connections are not allowed because passwords are transferred over the network as plain text. |
| 53 | TCP/UDP communication | Centrify authentication service and privilege elevation service, clients use the Active Directory DNS server for DNS lookup requests. |
| 88 | Encrypted UDP communication | Centrify authentication service and privilege elevation service, Kerberos ticket validation and authentication, agents, Centrify PuTTY |



| This port | Is used for | Centrify software and operation requiring this port |
|-----------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 123 | UDP communication for simple network time protocol (NTP) | Centrify authentication service and privilege elevation service, keeps time synchronized between clients and Active Directory for Kerberos ticketing. |
| 389 | Encrypted TCP/UDP communication | authentication service and privilege elevation service, Active Directory authentication and client LDAP service. |
| 443 | Cloud proxy server to Centrify cloud service | Centrify for mobile device management. |
| 445 | Encrypted TCP/UDP communication for delivery of group policies | Centrify authentication service and privilege elevation service, adclient and adgpupdate use Samba (SMB) and Windows file sharing to download and update group policies, if applicable. |
| 464 | Encrypted TCP/UDP communication for Kerberos password changes | Centrify authentication service and privilege elevation service, Kerberos ticket validation and authentication for agents, Centrify PuTTY, adpasswd, and passwd. |
| 500 | Internet Key Exchange (IKE) for UDP | Centrify authentication service, privilege elevation service, and audit and monitoring service; isolation and encryption service to protect data-in-motion. |
| 1433 | Encrypted TCP communication for the collector connection to Microsoft SQL Server | Centrify authentication service, privilege elevation service, and audit and monitoring service; collector service sends audited activity to the database. |
| 3268 | Encrypted TCP communication | Centrify authentication service and privilege elevation service, Active Directory authentication and LDAP global catalog updates. |
| 4500 | Internet Key Exchange (IKE) for NAT-T | Centrify authentication service, privilege elevation service, and audit and monitoring service; isolation and encryption service to protect data-in-motion. |
| 5063 | Encrypted TCP/RPC communication for the agent connection to collectors | Centrify authentication service, privilege elevation service, and audit and monitoring service; auditing service records user activity on an audited computer. |
| none | ICMP (ping) connections | Centrify authentication service and privilege elevation service, to determine whether if a remote computer is reachable. |

Auditing requires database management

If you are planning a deployment with just audit and monitoring service or with identity management, privilege management, and auditing, you must plan how you will create and manage the databases that receive and store audit data. You should also consider your data archiving and retention policies, who should be given auditor permissions, and other details because these decisions affect



your storage and maintenance requirements. For more information about managing an installation for auditing, see [Managing auditing for an installation](#).

For audit and monitoring service, you should plan a pilot deployment of 20 to 25 agents to determine how much audit data your organization would generate and how fast the database can increase in size as you add agents. For more information about monitoring a pilot deployment for audit and monitoring service and guidelines for sizing the database, see [Estimating database requirements based on the data you collect](#).

Identify an Active Directory site or subnets

Depending on the size and distribution of your Active Directory site, an audit store might cover an entire site or specific subnet segments. If you have a large, widely distributed site, you should consider network connectivity and latency issues in determining which subnets each audit store should serve. In addition, you should always place collectors in the same site as the agents from which they receive data. Collectors and agents must always be in the same Active Directory forest. If possible, you should put collectors and agents in the same domain.

Note: If you deploy agents in a perimeter network, such as a demilitarized zone (DMZ), that is separated from your main network by a firewall, put the collectors in the same Active Directory domain as the audited computers. The collectors can communicate with the audit store database through a firewall.

Determine how many collectors and audit stores to install

Although you can add collectors and audit stores to your audit and monitoring service installation after the initial deployment, you might want to calculate how many you will need before you begin deploying components. You should always have at least two collectors to provide redundancy. As you increase the number of agents deployed, you should consider adding collectors.

Estimate the number of agents and sessions audited

If you plan to use more than the minimum number of collectors, the most important factor to consider is the number of concurrent sessions you expect to



monitor on audited computers. The number of concurrent sessions represents the number of interactive users that the agent is actively capturing for at the same time.

You can use the following guidelines as a starting point and adjust after you have observed how much audit data you are collecting and storing for Windows computers:

| Number of concurrent sessions | Recommended number of collectors | Recommended number of audit stores |
|-------------------------------|----------------------------------|------------------------------------|
| up to 100 agents | 2 | 1 |
| more than 100 agents | 2 for every 100 agents | 1 for every 100 agents |

Determine the recommended hardware configuration

The hardware requirements for collectors and audit store servers depend on the size of the installation and where the components are installed on the network. For example, the requirements for a computer that hosts the collector service are determined by the number of audited computers the collector supports, the level of user activity being captured and transferred, and the speed of the network connection between the agents and the collector and between the collector and its audit store.

You can use the following guidelines as the recommended hardware configuration for the computers you use as collectors and audit store servers when auditing Windows computers:

| Computer used for | Number of concurrent sessions | CPU cores | CPU speed | Memory |
|-------------------|-------------------------------|-----------|-----------|--------|
| Collectors | Up to 100 active agents | 2 | 2.33 GHz | 8 GB |
| Audit store | Up to 200 active agents | 2 | 2.33 GHz | 8 GB |
| | 200 to 500 active agent | 4 | 2.33 GHz | 32 GB |

Guidelines for storage

Because audit and monitoring service collectors send captured user sessions to the active SQL Server database, you should optimize SQL Server storage for fast data logging, if possible. For the active database, you get the most benefit from improvements to disk write performance. Read performance is secondary. Fibre Attached Storage (FAS) and Storage Area Network (SAN) solutions can provide 2 to 10 times better performance than Direct Attached Storage (DAS),



but at a higher cost. For attached databases that are only used to store information for queries, you can use lower cost storage options.

Guidelines for disk layout

The following table outlines the recommended disk arrays:

| Application | Disk configuration | Use the disk for |
|----------------------|-----------------------|------------------------------------------------------------------|
| Operating system | C: RAID 1 | Operating system files, page file, and SQL Server binaries. |
| Microsoft SQL Server | D: RAID 10 (1+0) | Audit store database. |
| | E: RAID 10 (1+0) | Audit database log files. |
| | F: RAID 1 or 10 (1+0) | Temporary database space (tempdb) for large queries for reports. |
| | G: RAID 1 | Database dump files. |

The size of disk needed depends on the number, length, and types of sessions recorded each day, the selected recovery model, and your data retention policies. For more information about managing audit store databases, see [Managing audit store databases](#).

Decide where to install agents

The Centrifify agent for Windows must be installed on all of the computers you want to audit. Therefore, as part of your planning process, you should decide whether you want to audit every computer on the network or specific computers, such as the computers used as servers or used to run administrative software.

Before installing the agent, verify the following:

- The computer is joined to Active Directory.
- The computer has Windows security update KB3033929 installed if it is running Windows 7 with Service Pack 1 or Windows Server 2008 R2 with Service Pack 1.
- The computer has .NET 4.6.2 or later installed.
- The computer has Windows Installer version 4.5 or newer.
- Agents can communicate with a collector only if the agents and collector are in the same Active Directory forest.



Decide where to install consoles

You can install and run the Audit Manager console and the Audit Analyzer console on the same computer or on different computers. The computers where you install the consoles must be joined to the Active Directory domain and be able to access the management server and the database that serves the installation.

You can also use the Audit Analyzer console to run queries from any additional computers with network access to the management database. Therefore, you should decide where it would be convenient to have this capability.

Check SQL Server logins for auditing

An audit installation requires at least two Microsoft SQL Server databases: one for the management database and at least one for the first audit store database. To successfully connect to these databases, you must ensure that the appropriate users and computers have permission to read or to read and write for the databases that store audit-related information.

The simplest way to manage SQL logins for auditors and administrators is to do the following:

- Ensure you have a SQL login account for the NT Authority\System built-in account.
- Add the NT Authority\System account to the system administrator role.
- Use Audit Manager to grant Manage SQL Logins permissions to the Active Directory users and groups that require them.

If you use Audit Manager to manage SQL logins, you can use Active Directory membership to automatically add and remove the permissions required for auditing activity. There is no requirement to use the SQL Server Management Studio to manage logins or permissions. Because it is recommended that you have a dedicated SQL Server instance for auditing, giving the NT Authority\System account a SQL login and system administrator role is an acceptable solution for most organizations.



Create security groups for auditing

Depending on whether you configure Microsoft SQL Server to use Windows only authentication or Windows or SQL Server authentication, your SQL Server login credentials might be a Windows account or a SQL Server login account that is not associated with a Windows account.

To facilitate communication and the management of SQL logins, you can create Active Directory security groups for the following users and computers:

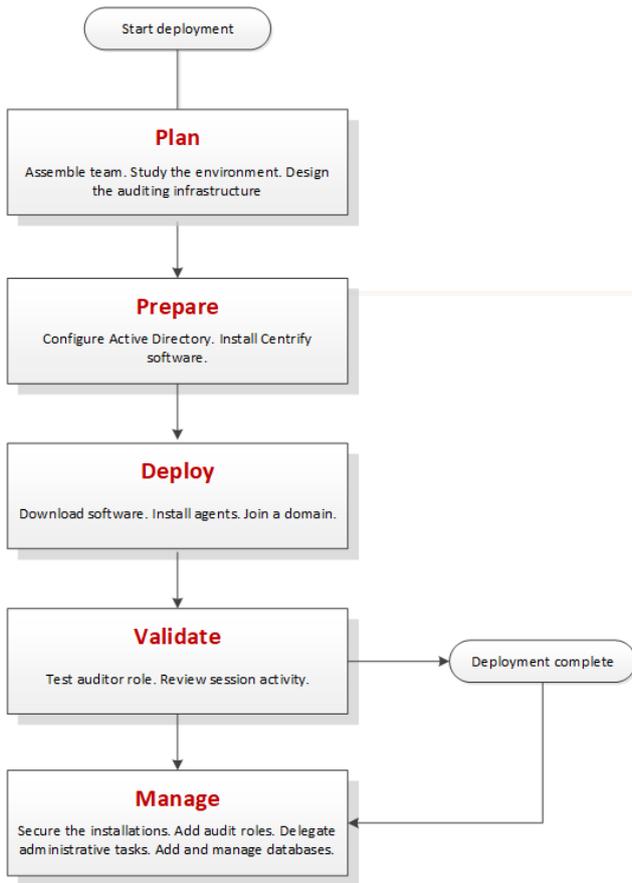
- **Centrify-Admins** for the user accounts that perform administrative tasks using Audit Manager.
- **Centrify-Auditors** for the user accounts that use Audit Analyzer.
- **Centrify-TrustedCollectors** for the computers accounts that host the collector service.

If you create these Active Directory security groups, you can then use Audit Manager to grant Manage SQL Login permissions for each group to allow its members to connect to the appropriate SQL Server database. Creating Active Directory security groups with SQL Server logins enables you to manage access to the databases required for auditing through Active Directory group membership without the help of the database administrator.

Any time you want to add an administrator, auditor, or collector computer to the installation, you simply add that user account or computer object to the appropriate Active Directory group. If an administrator or auditor leaves or if you want to stop using the collector on a particular computer, you can remove that user or computer from its Active Directory security group to prevent it from accessing the database.

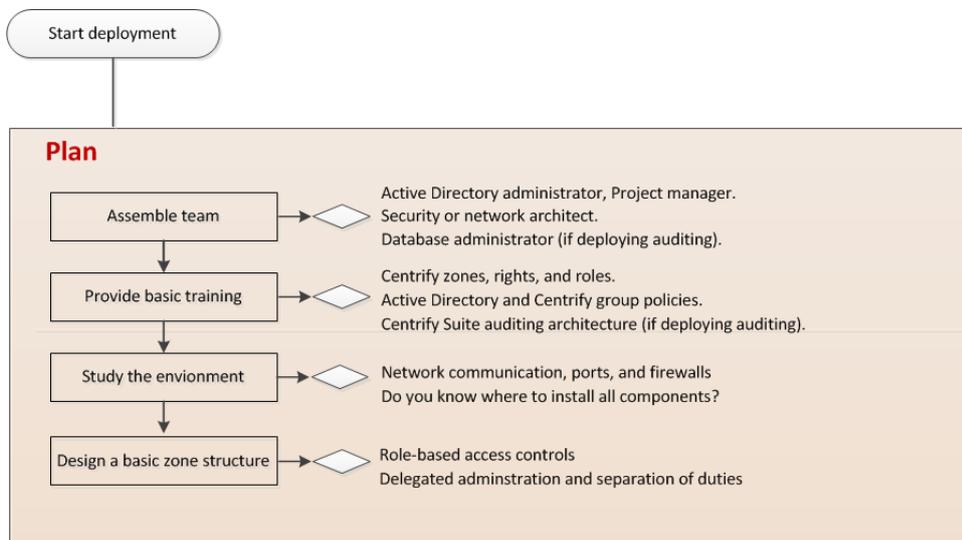
What's involved in the deployment process

Most of the planning in this chapter has focused on designing the audit and monitoring service infrastructure and deciding where to install components. The following illustration provides a visual summary of the complete deployment process and highlights the keys to success. The sections after the flowchart provide additional details about what's involved in each phase or the decisions you will need to make, such as who should be part of the deployment team, where to install the software, and who has permission to do what.



Plan

During the first phase of the deployment, you collect and analyze details about your organization's requirements and goals. You can then also make preliminary decisions about sizing, network communication, where to install components, and what your zone structure should look like.





Here are the key steps involved:

- Identify the goals of the deployment.
 - Is identity and privilege management or audit and monitoring service a primary goal?
 - Are identity and privilege management and audit and monitoring service equally important to the organization?
 - Is audit and monitoring service important for specific computers?
 - Is audit and monitoring service important for computers used to perform administrative tasks?
 - Is audit and monitoring service important for computers that host specific applications or sensitive information?
 - Should audit and monitoring service be required for users in specific groups or with specific roles?

For example, if audit and monitoring service is important, are you primarily interested in auditing Windows servers, such as SQL Server, Exchange, and IIS, administrative workstations, or computers that host specific applications or sensitive information?

- Assemble a deployment team with Active Directory and other expertise.
 - People with specific knowledge, such as Exchange, IIS, or Sharepoint administrators.
 - If auditing, at least one Microsoft SQL Server database administrator.
- Provide basic training on Centrify architecture, concepts, and terminology.
- Study the existing environment to identify target computers where you plan to install Centrify components.
 - Plan for permissions and the appropriate separation of duties for your organization.
 - Review network connections, port requirements, firewall configuration.

For more information about network communication and the ports used, see [Plan for network traffic and data storage](#).



- Identify computers for administration.
 - **Basic deployment**—Access Manager
 - **Auditing**—Audit Manager and Audit Analyzer consoles
- Identify computers to be used as collectors, audit stores, and the management database.
 - Verify that you have reliable, high-speed network connections between components that collect and transfer audit data.
 - Verify you have sufficient disk storage for the first audit store database.
- Identify the initial target group of computers to be managed and audited.
- Design a basic zone structure that suits your organization.
 - Single or multiple top-level parents.
 - Initial child zones, for example, separate zones for different functional departments or administrative groups.

Prepare

After you have analyzed the environment, you should prepare the Active Directory organizational units and groups to use. You can then install administrative consoles and the audit and monitoring service infrastructure, and prepare initial zones.

Here are the key steps involved:

- (Optional) Create organizational units or containers to define a scope of authority.

The deployment team should consult with the Active Directory enterprise administrator to determine whether any additional containers or organizational units would be useful, who should be responsible for creating Licenses and Zones container objects, and who will manage the objects in those containers.
- (Optional) Create the additional Active Directory security groups for your organization.

Groups can simplify permission management and the separation of duties.



- Install Access Manager on at least one administrative Windows computer.
- Open Access Manager for the first time to run the Setup Wizard for the Active Directory domain.
- Create a parent zone and the appropriate child zones as identified in your basic zone design.

The hierarchical zone structure you use depends primarily on how you want to use inheritance and roles.

- Prepare Windows computer accounts in the appropriate zones and assign the default Windows Login role to the appropriate Active Directory users and groups.
- Install Audit Manager and Audit Analyzer together or separately.
- Create an installation and a management database on one computer.
- Create an audit store and audit store database on at least one computer.
- Install a collector on at least two computers.

Deploy

After you have prepared Active Directory, installed administrative consoles on at least one computer, created at least one zone, and prepared the audit and monitoring service infrastructure, you are ready to deploy on the computers to be managed.

Here are the key steps involved:

- Create Desktop, Application, and Network Access rights.
- Add Desktop, Application, and Network Access rights to custom role definitions.
- Assign custom roles to the appropriate Active Directory users and groups.
- Install the Centrify agent for Windows on a target set of computers.
- Join the appropriate zones.
- Prepare a Group Policy Object for deploying agents remotely using a group policy.
- Assign the appropriate permissions to the users and groups who should have access to audit data.



Validate

After you have deployed agents on target computers, you should test and verify operations before deploying on additional computers.

Here are the key steps involved:

- Log on locally to a target computer using an Active Directory user account and password to verify Active Directory authentication and Windows Login role assignment.
- Open a Remote Desktop Connection to a target computer to verify Active Directory authentication and Windows Login role assignment on a remote computer.
- Create a new desktop that gives you administrative rights and verify that you can start and stop Windows services or perform other administrative tasks.
- Right-click an application, select Run using selected roles, then select an available role for running the application.
- Open Audit Analyzer and query for your user session if audit and monitoring service is enabled.

Manage

After you have tested and verified identity management, privilege management, and audit and monitoring service operations, you are ready to begin managing the installation and refining on-going operations.

Here are the key steps involved if you deploying identity management, privilege management, and auditing for Windows computers:

- Secure the installation.
- Add roles and assign roles and permissions to the appropriate users, groups, and computers.
- Delegate administrative tasks to the appropriate users and groups for each zone.
- Deploy additional group policies on the appropriate organizational units.
- Create new databases and rotate the active database.
- Archive and delete old audit data.

- Automate key administrative tasks using Centrify-defined Powershell-based cmdlets and scripts.

Authentication and Privilege Elevation services deployment checklist

The following checklist provides an overview of each of the main steps that are involved when you deploy Centrify Authentication Service and Centrify Privilege Elevation Service. For any tasks related to Centrify software, there are links to more information and procedures.

For auditing deployment steps, please see the [Audit & Monitoring Service deployment checklist](#).

| Step# | Authentication and Privilege Elevation services installation step | Notes | Link to Details |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|---------------------------------------|
| PREPARATION AND PLANNING | | | |
| 1 | Analyze your network topology to determine where to install components and services and any hardware or software updates required. | | Planning a deployment |
| 2 | Create a list of the computers where you plan to install different components. | | Planning a deployment |
| 3 | Determine how you plan to install the software onto your computers. | | Planning a deployment |
| PRE-INSTALL TASKS | | | |
| 4 | Prepare a domain account that has permissions to create Active Directory containers and child objects. | You'll need this account to create the OU using the Installation wizard. | |
| 5 | Prepare an Active Directory group to be zone administrators. | | |
| 6 | Create the Zone Provisioning Agent (ZPA) service account. | Requires Active Directory domain admin privileges | |
| 7 | Apply group policy to allow the ZPA to run as a service. | Requires Active Directory domain admin privileges | |



| Step# | Authentication and Privilege Elevation services installation step | Notes | Link to Details |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| INSTALL TASKS | | | |
| 8 | Install the Access Manager console, ZPA, group policies, create the OU in Active Directory, and so forth. | | Installing Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service "Installing Zone Provisioning Agent" topic in the Planning and Deployment Guide |
| 9 | (Optional) Configure ZPA – this is only needed if you plan on automatically provisioning users. | | "Configure the Zone Provisioning Agent" topic in the Planning and Deployment Guide |
| 10 | Run adcheck on any UNIX computer that you want to manage and fix any issues until adcheck produces no issues. | | "Perform administrative tasks using commands" topic in the Administrator's Guide for Linux and UNIX |
| 11 | Install a Centrify agent for Windows on each Windows computer that you want to manage. | | Installing the Centrify Agent for Windows |
| 12 | Install a Centrify agent for UNIX on each UNIX or Linux computer that you want to manage. | | "Installing agents on computers to be managed" topic in the Planning and Deployment Guide |
| 13 | Install additional Access Manager consoles on any Windows computer that you want to use for the Authentication and Privilege Management services. | | Installing additional consoles |



| Step# | Authentication and Privilege Elevation services installation step | Notes | Link to Details |
|----------------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 14 | Verify that agents are working correctly. Run <code>adinfo</code> on managed UNIX computers. | | Troubleshooting and common questions "Perform administrative tasks using commands" topic in the Administrator's Guide for Linux and UNIX |
| POST-INSTALL HOUSEKEEPING | | | |
| 15 | Identify UNIX users who do not have an Active Directory account. | Automatically done by <code>adimport</code> | adimport man page |
| 16 | Identify service accounts. | | "Identifying service accounts to migrate to Active Directory" topic in the Planning and Deployment Guide |
| 17 | Collect and analyze sudoers files. | | "Converting sudoers aliases and user specifications" topic in the Administrator's Guide for Linux and UNIX |
| 18 | Create a list of Roles in sudoers that will be migrated to Centrify Privilege Elevation Service. | | "Identifying accounts that should not be migrated" topic in the Planning and Deployment Guide |
| 19 | Create a list of users and groups to be migrated to Active Directory. | | "Migrating existing users to hierarchical zones" topic in the Planning and Deployment Guide |
| 20 | Create missing Active Directory user accounts. | | |
| SETUP AND CONFIGURATION | | | |
| 21 | Create list of computers that will be joined to each Zone. | | |



| Step# | Authentication and Privilege Elevation services installation step | Notes | Link to Details |
|-------|-------------------------------------------------------------------|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 22 | Create parent and child zones. | | Creating a new parent zone Creating child zones |
| 23 | Delegate control to zones. | | Delegating control of administrative tasks |
| 24 | Import UNIX users and groups into Active Directory. | | "Migrating existing users to hierarchical zones" topic in the Planning and Deployment Guide |
| 25 | Create Zone Provisioning groups and add users and groups to them. | | "Adding new users to a provisioning group and a role group " topic in the Planning and Deployment Guide |
| 26 | Pre-create computer objects in zones. | | "Prepare a computer object before joining" topic in the Planning and Deployment Guide |
| 27 | Create Role Groups . | | "Create role groups for child zones" topic in the Planning and Deployment Guide |
| 28 | Assign roles and users to role groups. | | "Adding new users to a provisioning group and a role group" topic in the Planning and Deployment Guide |
| 29 | Create ComputerRoles and ComputerRole groups. | | Create a new computer role "Working with computer roles" topic in the Planning and Deployment Guide "Working with computer roles" topic in the Administrator's Guide for Linux and UNIX |



| Step# | Authentication and Privilege Elevation services installation step | Notes | Link to Details |
|--------------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 30 | Assign roles, users, and computers to ComputerRole groups. | | Add role assignments to the computer role |
| 31 | Use "Show Effective Users" to check that profiles and roles are correct. | | "Verifying effective users on each zone" topic in the Planning and Deployment Guide |
| 32 | Start the ZPA agent. | You configured ZPA in a previous step. | "Configure the Zone Provisioning Agent" topic in the Planning and Deployment Guide |
| 33 | Configure the ZPA provisioning rules for the parent zone. | | "Configure the Zone Provisioning Agent" topic in the Planning and Deployment Guide |
| 34 | Join UNIX servers to Zones. | | "Joining a domain" topic in the Administrator's Guide for Linux and UNIX |
| 35 | Change the UID/GID of files for those users who have been assigned a new UID/GID in the Zone. Run adfixid on servers. | * Critical task that must be carefully coordinated with the users. Can be done at time of join to Active Directory with a script. | "Perform administrative tasks using commands" topic in the Administrator's Guide for Linux and UNIX |
| FINAL TASKS | | | |
| 36 | Check the status of the join and roles on the servers. | Run adflush, adinfo and dzinfo | "Perform administrative tasks using commands" topic in the Administrator's Guide for Linux and UNIX "Migrating existing users to hierarchical zones" topic in the Planning and Deployment Guide |
| 37 | Back up passwd, shadow, and group files. | | |



| Step# | Authentication and Privilege Elevation services installation step | Notes | Link to Details |
|-------|-------------------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------|
| 38 | Remove the users and groups (that have been migrated to Active Directory) from the local files. | Run admlocal on servers | "Perform administrative tasks using commands" topic in the Administrator's Guide for Linux and UNIX |

Accounts and permissions for installation and deployment

Below is a summary of the account permissions that you need to install and deploy Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service.

The following topics are included:

| | |
|----------------------------------------------------------------------------|----|
| Centrify Authentication and Privilege Elevation Services permissions | 55 |
| Zone Provisioning Agent permissions | 55 |
| Report Services permissions | 56 |
| Audit & Monitoring permissions | 60 |



Centrify Authentication and Privilege Elevation Services permissions

Access Manager account permissions

| Account name (suggested) | Type of account | Required permissions | Notes |
|--------------------------|--------------------------------------------------------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| n/a | Domain administrator (when running Access Manager for the first time) | domain admin (in most cases) | Because the Setup Wizard creates container objects, you might need to use a domain administrator account. This requirement depends on the specific permissions your organization has configured for different classes of users. For example, if your organization only permits Domain Admins to create parent and child objects in Active Directory, you need to use an account with those permissions to run the Setup Wizard. |

For more information, see:

- "Running Access Manager for the first time" and "Permissions required to use the Setup Wizard" in the Planning and Deployment Guide

Zone Provisioning Agent permissions

Zone Provisioning Agent account permissions

| Account name (suggested) | Type of account | Required permissions | Notes |
|--------------------------|--------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cfy_SVC_ZPA | Active Directory account | Log on as a service | The Zone Provisioning Agent requires permission to create UNIX profiles-- that is, the service connection points in each zone where it needs to perform provisioning operations. The service account that runs the Zone Provisioning Agent requires the Log on as a service right set as a local computer security policy, or in the default domain policy. |

For more information, see:

- "About Zone Provisioning Agent and its requirements" in the Planning and Deployment Guide



Report Services permissions

Report services account permissions

| User type | Required Active Directory permissions | Required security policy permissions (group policy, or local policy) | Required SSRS permissions | Required SQL Server or PostgreSQL permissions |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| report service account to run the Reporting Service | For domain-based reporting: Replicating directory changes at the domain level (ADUC) and replicate directory changes in ADSI | Log on as a service | | |
| | For zone-based reporting: Read permission | | | |
| SQL Server service account to run SQL Server | n/a | Log on as a service | | |
| PostgreSQL service account | | | | the account must have Create Database permission |
| report admin to run the Report Configuration wizard or the Upgrade & Deployment wizard and deploy reports to an existing SQL Server instance | needs to be a member of the domain | n/a | Folder Settings > Content Manager role | member of the securityadmin role (At the very least, the user needs permission to connect to SQL Server and create a database.) |



Report services account permissions

| User type | Required Active Directory permissions | Required security policy permissions (group policy, or local policy) | Required SSRS permissions | Required SQL Server or PostgreSQL permissions |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| report admin to modify the Reports Control Panel | Read permission to the domain root object of the selected domain. Read permission to all computer objects in the selected domain. | n/a | | |
| Report viewer to view reports from SSRS/Internet Explorer | | | Site settings > System user role Folder settings > browser (assign SSRS roles to Active Directory group or users) | |



Report services account permissions

| User type | Required Active Directory permissions | Required security policy permissions (group policy, or local policy) | Required SSRS permissions | Required SQL Server or PostgreSQL permissions |
|----------------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Report writer | read, write, edit access for reports, in addition to the permissions needed to view reports | | Site settings > System user role Folder settings > Content Manager role (assign SSRS roles to Active Directory group or users) | |



SQL Server permissions set by the Report Services Configuration wizard

| User type | Required SQL Server permissions |
|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| report services account to run the SQL Server Reporting Service | Snapshot Service (predefined role) |
| SQL Server service account to run SQL Server | <p>If you deploy to an existing SQL Server instance, the configuration wizard makes no changes to the SQL Server service account.</p> <p>If you deploy to a new SQL Server instance:</p> <p>--If the operating system is Windows 2008 and you're using a SQL Server version later than 2012, virtual accounts are used for various SQL Server components, as follows:</p> <p>SQL Server engine: NT SERVICE\MSSQL\$<InstanceName></p> <p>SQL Server Agent: NT SERVICE\SQLAgent\$<InstanceName></p> <p>Full text search: NT SERVICE\MSSQLFDLauncher\$<InstanceName></p> <p>SSRS: NT SERVICE\ReportServer\$<InstanceName></p> <p>--Otherwise, the SQL Server service accounts are configured as follows:</p> <p>SQL Server engine: NT Authority\Network Service</p> <p>SQL Server Agent: NT Authority\Network Service</p> <p>Full text search: NT Authority\Local Service</p> <p>SSRS: NT Authority\Local Service</p> |
| report admin to run the Report Configuration Wizard and deploy reports to an existing SQL Server instance | Connect SQL (cannot be revoked after setup) Create Database, Create any database, or Alter any database member of securityadmin role, or Alter any login permission |
| report admin to modify the Reports Control Panel | SnapshotAdmin (predefined role) |



| User type | Required SQL Server permissions |
|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Report viewer to view reports from SSRS/Internet Explorer | Login permission SnapshotViewer (predefined role) |
| Report writer read, write, edit access for reports, in addition to the permissions needed to view reports | Login permission SnapshotViewer (predefined role) |

Note: Microsoft SQL Server Reporting System (SSRS) affords only role-based security in their reports. Be sure to grant appropriate access to reports. For example, if a user has access to only some data in the specified domain but all reports, they will be able to view all reports on all data from Active Directory.

For more information, see:

- "Required user permissions for report services" and "SQL Server permissions that are set by the Configuration Wizard" in the Report Administrator's Guide

Audit & Monitoring permissions

Auditing permissions for SQL Server

| SQL Server account | Type of account | Required permissions | Notes |
|---------------------|-----------------|----------------------------------------------|-------|
| NT Authority\System | machine account | SQL Server Roles: <code>sysadmin</code> role | |



Auditing security groups

| Active Directory security groups | Type of account | Required SQL Server permissions | Notes |
|-----------------------------------------------------------------------------------------------------|------------------------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Centrify-Admins for the user accounts that perform administrative tasks using Audit Manager. | | no explicit SQL Server permissions needed — | Creating Active Directory security groups with SQL Server logins enables you to manage access to the databases required for auditing through Active Directory group membership without the help of the database administrator. |
| Centrify-Auditors for the user accounts that use Audit Analyzer. | Active Directory | Audit Manager handles the SQL Server permissions | |
| Centrify-Collectors for the computer accounts that host the collector service. | | | |

For more information, see:

- "Checking SQL Server logins for auditing" and "Creating security groups for auditing" in the Auditing Administrator's Guide



Installing Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service

This chapter describes how to install Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service software on Windows computers in a production environment. It includes instructions for installing all identity and privilege management, audit and monitoring service, and multi-factor authentication components. It also describes how to install the Centrify agent on Windows computers, and how to enable services on agent-managed Windows computers.

If your deployment plan includes identity and privilege management, as well as audit and monitoring service, you should review the details in [Planning a deployment](#) before installing any components.

The following topics are covered:

| | |
|-----------------------------------------------------------------------------------------------------------------------|----|
| Installation checklist | 63 |
| Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory | 65 |
| Installing and configuring Microsoft SQL Server for auditing | 69 |
| Installing Centrify Audit Manager and Centrify Audit Analyzer consoles | 71 |
| Creating a new installation | 71 |



| | |
|-------------------------------------------------------------------------------------|-----|
| Installing and configuring Centrify audit collectors | 79 |
| Installing the Centrify Agent for Windows | 82 |
| Installing additional consoles | 105 |
| Installing group policy extensions separately from Centrify Access Manager | 106 |

In a production environment, you should use separate computers for different components to ensure scalability and performance. For information about setting up an evaluation environment on a single computer for testing, see the *Evaluation Guide for Windows*.

Installation checklist

As a preview of what's involved in the installation process, the following steps summarize what you need to do and the information you should have on hand for a successful deployment of authentication, privilege elevation, and audit and monitoring services.

To prepare for installation:

1. Analyze your network topology to determine where to install components and services and any hardware or software updates required.

For a review of the decisions to make and recommended hardware configuration, see [Planning a deployment](#).

2. Create a list of the computers where you plan to install different components.

For example, list the computers where you plan to install agents, collectors, audit store databases, consoles, and group policy extensions.

If you are installing the audit and monitoring service infrastructure, you should use a dedicated computer for each component, so that the audit collector service, audit store database, and audit management database are on separate computers with high-speed and reliable network connectivity.

For a review of the requirements associated with each component, see [Planning a deployment](#).



3. Determine the scope of the audit installation.

The most common deployment scenario is a single installation for an Active Directory site, but you can have more than one installation, if needed, and use subnets to limit the scope of the installation. If you are only implementing access management, you can skip this step, Step 4, and Step 7 through Step 10.

For a review of what constitutes an installation, see [Deploying the audit and monitoring service infrastructure](#) and [Decide on the scope of the installation](#).

4. Create Active Directory security groups for managing the permissions required for the audit and monitoring service infrastructure.

For a review of the Active Directory security groups to create, see [Create security groups for auditing](#). If you are only implementing identity and privilege management, you can skip this step.

5. Install Access Manager on at least one computer that can connect to the Active Directory forest.

6. Open Access Manager and add containers for licenses and zones to the Active Directory forest.

7. Install Microsoft SQL Server.

If you are not a database administrator in your organization, you should submit a service request or contact an administrator who has permission to create databases for assistance. For more information about preparing a SQL Server database engine for auditing, see [Installing and configuring Microsoft SQL Server for auditing](#). If you are only implementing access management, you can skip this step.

8. Install Audit Manager and Audit Analyzer.

For more information about installing these products, see [Installing Centrify Audit Manager and Centrify Audit Analyzer consoles](#). If you are only implementing identity and privilege management, you can skip this step.

9. Open Audit Manager to create a new installation for auditing.

For more information about using Audit Manager to create a new installation and audit store, see [Creating a new installation](#). If you are only implementing identity and privilege management, you can skip this step.



10. Install the audit collector service on at least two Windows computers.
You can add collectors to the installation at any time. For more information about installing and configuring collectors, see [Installing and configuring Centrify audit collectors](#). If you are only implementing identity and privilege management, you can skip this step.
11. Install a Centrify agent for Windows on each Windows computer that you want to manage or audit.
For more information about installing and configuring Centrify agents for Windows, see [Installing the Centrify Agent for Windows](#).
12. Install additional consoles on any Windows computer that you want to use for identity and privilege management, or audit and monitoring service.

After the initial deployment, you can add new agents, collectors, audit stores, and audit store databases to the audit installation or create additional installations at any time.

Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory

When you install Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service, components for the following features are installed:

- The Centrify Identity Services Platform, which enables MFA login, endpoints, and other platform services.
- The Centrify Privilege Elevation Service, which enables users and zone-joined computers to have elevated privileges.
- The Centrify Audit & Monitoring Service, which enables audit and monitoring service data to be collected and stored.
- The Centrify Agent for Windows, which enables each computer where the agent is installed to be managed by Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service software.
- The Centrify Licensing Service, which works together with Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service components to monitor and report usage and activity for all types



of Centrify licenses. For more information about the licensing service, see the *License Management Administrator's Guide*

You can select which features to install from the Centrify setup program.

After authentication, privilege elevation, and audit and monitoring services are installed, you must enable some or all of them on each agent-managed computer. The enablement step lets you decide which services are available on each agent-managed computer.

Things to remember

- At least one zone must be created before an agent-managed computer can be enabled to use the identity and privilege management features that you install. If no zones are available, the agent-managed computer will not have the option of being joined to the authentication and privilege elevation services.
- When the Centrify agent is upgraded or when it adds the Centrify Identity Services Platform, a corporate endpoint enrollment is performed in the Privileged Access Service. The endpoint device moves into the endpoint category and the device is marked as corporate owned.

Running the setup program on a Windows computer

You can install components for all authentication, privilege elevation, and audit and monitoring services from the Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring ServiceCD or a downloaded ISO or ZIP file. After you access the distribution media, the setup or autorun program copies the necessary files to the local Windows computer. There are no special permissions required to run the setup or autorun program other than permission to install files on the local computer.

To install Centrify software on Windows:

1. Log on to the computer you have selected for administrative tasks and browse to the location where you have saved downloaded Centrify files. If you have a physical CD, the Getting Started page is displayed automatically. If the page is not displayed, open the `autorun.exe` file to start the installation of Centrify software.

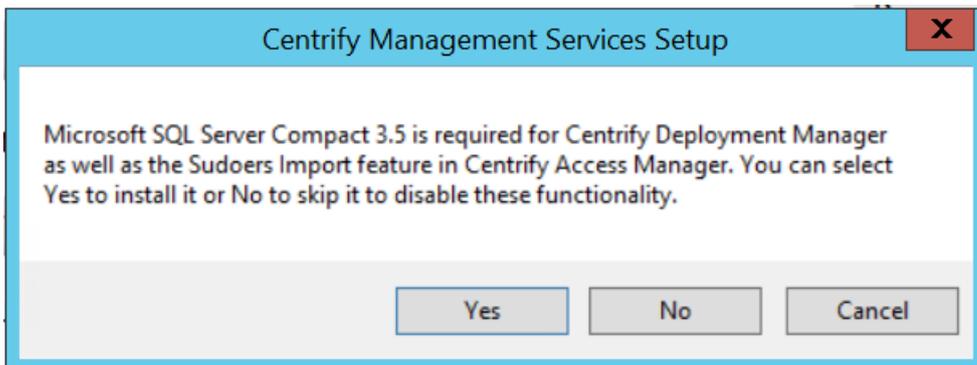


2. On the Getting Started page, click **Authentication & Privilege** to start the setup program for authentication and privilege elevation services.

Note: The **Authentication & Privilege** components are the recommended first components to install so that Access Manager is available for you to use to create zones. At least one zone must be created before you can enable the authentication and privilege elevation services on an agent-managed computer.

If any programs must be updated before installing, the setup program displays the updates required and allows you to install them. After updates are complete, you can restart the setup program.

3. At the following screen, select **Yes** to install Microsoft SQL Server Compact. The Access Manager console uses the Microsoft SQL Server Compact for storage.



If you select No, Microsoft SQL Server Compact is not installed and some features of Access Manager are not available.

4. At the Welcome page, click **Next**.
5. Review the terms of the license agreement, click **I agree to these terms**, then click **Next**.
6. Type your name and company name, then click **Next**.
7. Expand and select the Centrify Administration and Centrify Utilities components you want to install, then click **Next**.

If you are only managing identity and privileges for Windows computers, you can install a subset of the components. For a Windows-only deployment, select the following components:

- **ADUC property page extension** if you want to include Centrify profiles when displaying properties in Active Directory Users and



Computers.

- **Access Manager console (all)** if you want to use an administrative console to manage Centrify zones and roles.
- **Group Policy Management Editor extension** if you want to deploy Centrify group policies.

Installing Centrify Report Services is optional. If you select this option, see [Installing and configuring Microsoft SQL Server for auditing](#) for additional details.

For a Windows-only deployment, you can deselect Centrify Utilities to skip the installation of those components.

8. Accept the default location for installing components, or click **Browse** to select a different location, then click **Next**.
9. Review the components you have selected, then click **Next**.

The setup program begins installing the selected components.

10. Click **Finish** to complete installation.
11. Optionally install additional authentication, privilege elevation, and audit and monitoring services components as follows:
 - **Centrify Licensing Service.** This service is installed by default when you install the Authentication & Privilege components, and usually does not need to be installed separately. For more information about the licensing service, see the *License Management Administrator's Guide*.
 - **Audit & Monitor.** The Auditing and Monitoring Service is not installed automatically with any other components, and must be installed separately if you intend to use auditing and monitoring features. For installation details, see [Installing Centrify Audit Manager and Centrify Audit Analyzer consoles](#).
 - **Centrify Agent for Windows.** To install the agent on client Windows computers so that those computers can be managed by Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service, see [Installing the Centrify Agent for Windows](#).

Opening Centrify Access Manager to update Active Directory

The first time you start Access Manager, a Setup Wizard prepares the Active Directory forest with parent containers for licenses and zones. The Setup



Wizard also sets the appropriate permissions for the objects automatically. For more information about using the Setup Wizard to update Active Directory, see [Starting Centrify Access Manager for the first time](#).

Installing and configuring Microsoft SQL Server for auditing

If you want to audit user activity on Windows, you must have at least one Microsoft SQL Server database instance for the audit management database and audit store databases. Centrify recommends that you use a dedicated instance of SQL Server for the audit management database. A dedicated SQL Server instance is an instance that does not share resources with other applications. The audit store databases can use the same dedicated instance of SQL Server or their own dedicated instances.

There are three database deployment scenarios for your installation:

- **Evaluation**—Use the SQL Server Express with Advanced Services setup program (SQLEXPADV_x64_ENU.exe) to create a new instance of Microsoft SQL Server Express. *You should only use Microsoft SQL Server Express for evaluation or for limited use in a test environment. You should not use SQL Server Express databases in a production environment.*

If you choose to install a different version of Microsoft SQL Server Express for an evaluation and the version requires .NET version 3.5 SP1, you will need to manually install the .NET files yourself (the installer doesn't include these files).

- **Manual installation with system administrator privileges**—Install a Microsoft SQL Server database instance for which you are a system administrator or have been added to the system administrator role.
- **Manual installation without system administrator privileges**—Have the database administrator (DBA) install an instance of Microsoft SQL Server and provide you with system administrator credentials or information about the database instance so that you can create the management database and audit store databases.



Downloading and installing SQL Server manually

You can use an existing Microsoft SQL Server database engine or install a new instance. You can download Microsoft SQL Server software from the Microsoft website or through the [Centrify Support Portal](#). In selecting a version of Microsoft SQL Server to download, you should be sure it includes Advanced Services. Advanced Services are required to support querying using SQL Server full-text search.

After downloading an appropriate software package, run the setup program using your Active Directory domain account and follow the prompts displayed to complete the installation of the SQL Server database engine.

Configuring SQL Server to prepare for audit and monitoring service

After you install the SQL Server database engine and management tools, you should configure the SQL Server instance for audit and monitoring service by doing the following:

- Depending on the version of SQL Server you install, you might need to manually enable full-text search. For example, use SQL Server Surface Area Configuration for Services and Connections to start the full-text search service.
- Use SQL Server Configuration Manager to enable remote connections for TCP/IP.
- Use SQL Server Configuration Manager to restart the SQL Server and SQL Server Browser services.
- Verify whether SQL Server is using the default TCP port 1433 for network communications. If you use a different port, you should note the port number because you will need to specify in the server name when you create the management and audit store databases.



Installing Centrify Audit Manager and Centrify Audit Analyzer consoles

You can install Audit Manager and Audit Analyzer on the same computer or on different computers. The computers where you install the consoles must be joined to the Active Directory domain and be able to access the audit management database.

In most cases, the consoles are installed together on at least one computer.

To install Audit Manager and Audit Analyzer on the same computer:

1. Log on to the computer you have selected for administrative tasks and browse to the location where you have saved downloaded Centrify files. If you have a physical CD that you made from the ISO image file, the Getting Started page is displayed automatically. If the page is not displayed, open the `autorun.exe` file to start the installation of Centrify software.
2. On the Getting Started page, click **Audit & Monitor** to start the setup program for audit and monitoring service components. In the rare case where the administrator should not have access to the Audit Analyzer, select Audit Manager, then click **Next**.

After you install Audit Manager, you are prompted to create a new installation. If you want to create the installation at a later time, you can run the setup program again to create a new installation.

Creating a new installation

Before you can begin audit and monitoring service, you must create at least one installation and a management database. Creating the management database, however, requires SQL Server system administrator privileges on the computer that hosts the SQL Server instance. If possible, you should have a database administrator add your Active Directory domain account to the SQL Server system administrators role.

If you have not been added to the system administrators role, you should contact a database administrator to assist you. For more information about creating a new installation when you don't have system administrator



privileges, see [How to create an installation without system administrator privileges](#).

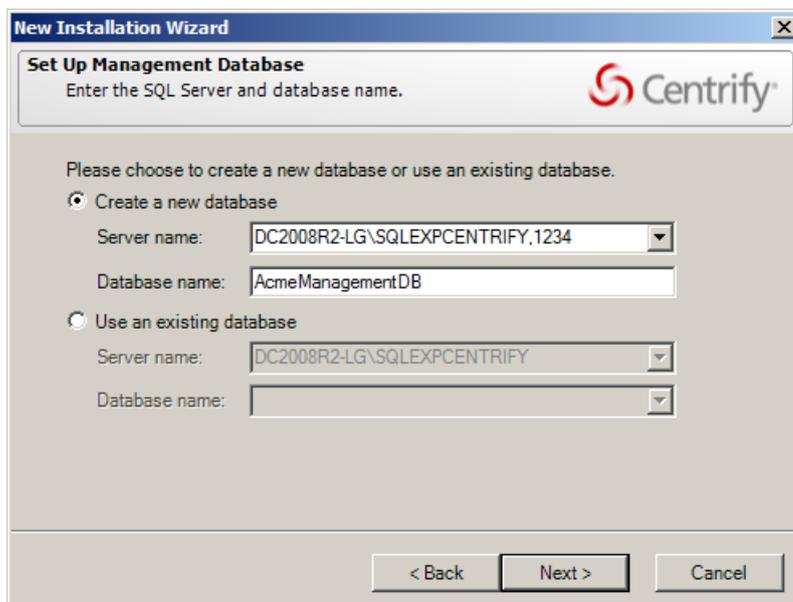
To create a new installation and management database as a system administrator:

1. Log on using an Active Directory account with permission to install software on the local computer.
2. Open the Audit Manager console to display the New Installation wizard. The New Installation wizard displays automatically the first time you start Audit Manager. You can also start it by clicking **Action > New Installation** or from the right-click menu when you select the Audit Manager node.
3. Type a name for the new installation, then click **Next**.

Tip: Name the installation to reflect its administrative scope. For example, if you are using one installation for your entire organization, you might include the organization name and All or Global in the installation name, such as AcmeAll. If you plan to use separate installations for different regions or divisions, you might include that information in the name, for example AcmeBrazil for a regional installation or AcmeFinance for an installation that audits computers in the Finance department.

4. Select the option to create a new management database and verify the SQL Server computer name, instance name, and database name are correct, then click **Next**.

If the server does not use the default TCP port (1433), you must provide the server and instance names separated by a backslash, then type a comma and the appropriate port number. For example, if the server name is ACME, the instance name is BOSTON, and the port number is 1234, the server name would be ACME\BOSTON,1234.



If you're connecting to a SQL Server availability group listener, click Options (next to the Server Name) and enter the following connection string parameters:

`MultiSubnetFailover=Yes`

5. Type the license key you received, then click **Add** or click **Import** to import the keys directly from a file, then click **Next**.
6. Accept the default location or click **Browse** to select a different Active Directory container to which you want to publish audit-related information, then click **Next**.
7. Select **Enable video capture recording of user activity** if you want to capture a full video record of desktop activity on Windows computers when users are audited, then click **Next**.

Selecting this option enables you to review everything displayed during an audited user session, but will increase the audit store database storage requirements for the installation. You can deselect this option if you are only interested in a summary of user activity in the form of audit trail events. Audit trail events are recorded when users log on, open applications, and select and use role assignments with elevated rights.

8. Review details about the installation and management database, then click **Next**.

If you have SQL Server system administrator (sa) privileges and can connect to the SQL Server instance, the wizard automatically creates the management database.



9. Select the **Launch Add Audit Store Wizard** option if you want to start the Add Audit Store wizard, then click **Finish**.

If you want to create the first audit store database at a later time, you should deselect the **Launch Add Audit Store Wizard** option and click **Finish**.

For more information about adding the first audit store database, see [Create the first audit store](#).

How to create an installation without system administrator privileges

If you do not have the appropriate permission to create SQL Server databases, you cannot use the New Installation wizard to create the management database without the assistance of a database administrator.

If you do not have system administrator privileges, the wizard prompts you to specify another set of credentials or generate SQL scripts to give to a database administrator. For example:



If you don't have a database administrator immediately available who can enter the credentials for you, you cannot continue with the installation.



To create an installation when you don't have system administrator privileges:

1. Select the option to generate the SQL scripts, then click **Next**.
2. Select the folder location for the scripts, then click **Next**.
3. Review details about the installation and management database you want created, then click **Next**.

The wizard generates two scripts: Script1 prepares the SQL Server instance for the management database and Script2 creates the database.

4. Click **Finish** to exit the New Installation wizard.
5. Send the scripts to a database administrator with a service or change control request.

Note: You should notify the database administrator that the scripts must be run in the proper sequence and not modified in any way. Changes to the scripts could render the database unusable.

6. After the database administrator creates the database using the scripts, open the Audit Manager console to run the New Installation wizard again.
7. Type the name of the installation, then click **Next**.
8. Select **Use an existing database** and verify the database server and instance name, then click the Database name list to browse for the database name that the database administrator created for you.

If the server does not use the default TCP port, specify the port number as part of the server name. For example, if the port number is 1234, the server name would be similar to ACME\BOSTON,1234.
9. Select the database name from the list of available databases, click **OK**, then click **Next**.
10. You should only select an existing database if the database was created using scripts provided by Centrify.
11. Type a license key or import licenses from a file, then click **Next**.
12. Review details about the audit management database to be installed, then click **Next**.
13. Select the **Launch Add Audit Store Wizard** option if you want to start the Add Audit Store wizard, then click **Finish**.



Create the first audit store

If you selected the Launch Add Audit Store Wizard at the end of the New Installation Wizard, the Add Audit Store Wizard opens automatically. You can also open the wizard at any time by right-clicking the Audit Stores node in the Audit Manager console and choosing Add Audit Store.

To create the first audit store:

1. Type a display name for the audit store, then click **Next**.
 - Tip:** If your plan specifies multiple audit stores, use the name to reflect the sites or subnets serviced by this audit store. Note that an audit store is actually a record in the management database. It is not a separate process running on any computer. You use a separate wizard to create the databases for an audit store.
2. Click **Add Site** or **Add Subnet** to specify the sites or subnets in this audit store.
 - If you select Add Site, you are prompted to select an Active Directory site.
 - If you select Add Subnet, you are prompted to type the network address and subnet mask.

After you make a selection or type the address, click **OK**. You can then add more sites or subnets to the audit store. When you are finished adding sites or subnets, click **Next** to continue.

The computer you use to host the audit store database should be no more than one gateway or router away from the computers being audited. If your Active Directory sites are too broad, you can use standard network subnets to limit the scope of the audit store.

3. Review information about the audit store display name and sites or subnets, then click **Next**.
4. Select the **Launch Add Audit Store Database Wizard** option if you want to create the first audit store database, then click **Finish**.



Create the audit store database

If you selected the Launch Add Audit Store Database Wizard check box at the end of the Launch Add Audit Store Wizard, the Add Audit Store Database Wizard opens automatically. You can also open the wizard at any time from the Audit Manager console by expanding an audit store, right-clicking the Databases node, and choosing Add Audit Store Database.

To create the first audit store database:

1. Type a display name for the audit store database, then click **Next**.
The default name is based on the name of the audit store and the date the database is created.
2. Select the option to create a new database and verify that the SQL Server computer name, instance name, and database name are correct.
The default database name is the same as the display name. You can change the database name to be different from the display name, if you want to use another name.

If the server does not use the default TCP port, specify the port number as part of the server name. For example, if the port number is 1234, the server name would be similar to ACME\BOSTON,1234.

When entering the SQL Server host computer name, note that you can enter either the server short name (which is automatically resolved to its fully qualified domain name, or FQDN) or the actual server FQDN or the CNAME alias for the server.

If the database is an Amazon RDS SQL Server:

- a. Select the **This is an Amazon RDS SQL Server** option.
- b. In the Server Name field, enter the RDS SQL Server database instance endpoint name used for Kerberos authentication.
For example, if the database host name is northwest1 and the domain name is sales.acme.com, then the endpoint name would be northwest1.sales.acme.com.

Click **Options** to enter additional connection string parameters or to enable data integrity checking.

- You can enable or disable data integrity checking once, when you create the audit store database. To change the state, you must rotate to a new audit store database.



Connecting to SQL Server on a remote computer

To create an audit store database on a remote computer, there must be a one-way or two-way trust between the domain of the computer on which you are running the Add Audit Database wizard and the domain of the computer hosting SQL Server. The Active Directory user account that you used to log on to the computer where the Audit Manager is installed must be in a domain trusted by the computer running SQL Server. If there is no trust relationship, you must log on using an account in the same domain as the computer running SQL Server. If you are accessing the computer running SQL Server remotely, you can use the Run As command to change your credentials on the computer from which you are running the wizard.

Verify network connectivity

The computer hosting the SQL Server database for the active audit store server be online and accessible from the Audit Manager console and from the clients in the Active Directory site or the subnet segments you have defined for the audit store. You should verify that there are no network connectivity issues between the computers that will host collectors and those hosting the SQL Server databases.

How to create the database without system administrator privileges

If you do not have system administrator privileges, the wizard prompts you to specify another set of credentials or generate SQL scripts to give to a database administrator. If you don't have database administrator credentials or a database administrator immediately available who can enter the credentials for you, you should generate the scripts, then follow the prompts displayed to exit the wizard.

To add the database to the audit store after you have generated the scripts:

1. Send the scripts to a database administrator with a service or change control request.

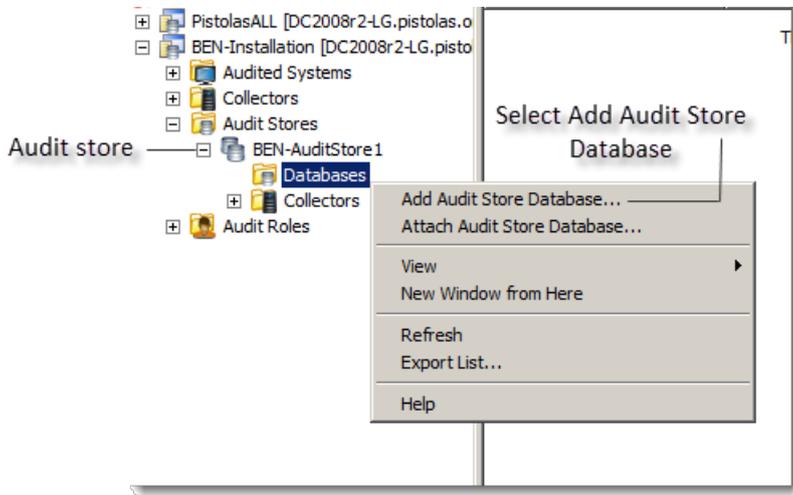
Note: You should notify the database administrator that the scripts must be run in the proper sequence and not modified in any way. Changes to the scripts could render the database unusable.

2. After the database administrator creates the database using the scripts,



open the Audit Manager console.

- Expand the installation node, then expand Audit Stores and the specific audit store you for which you want a new database.
- Select **Databases**, right-click, then click **Add Audit Store Database**. For example:



- Type a display name for the audit store database, then click **Next**.
- Select **Use an existing database** and select the database that the database administrator created for you.

Because this is the first audit store database, you also want to make it the active database. This option is selected by default. If you are creating the database for future use and don't want to use it immediately, you can deselect the **Set as active database** option.

If the server does not use the default TCP port, specify the port number as part of the server name. For example, if the port number is 1234, the server name would be similar to ACME\BOSTON, 1234.

The installation, management database, and first audit store database are now ready to start receiving user session activity. Next, you should install the collectors and, finally, the agents to complete the deployment of the audit and monitoring service infrastructure.

Installing and configuring Centrify audit collectors

After you have created a new installation, with an audit management database and at least one audit store and audit store database, you must add the collectors that will receive audit records from the agents and forward those



records to the audit store. For redundancy and scalability, you should have at least two collectors. For more information about planning how many collectors to use and the recommended hardware and network configuration for the collector computers, see [Decide where to install collectors and audit stores](#).

Set the required permission

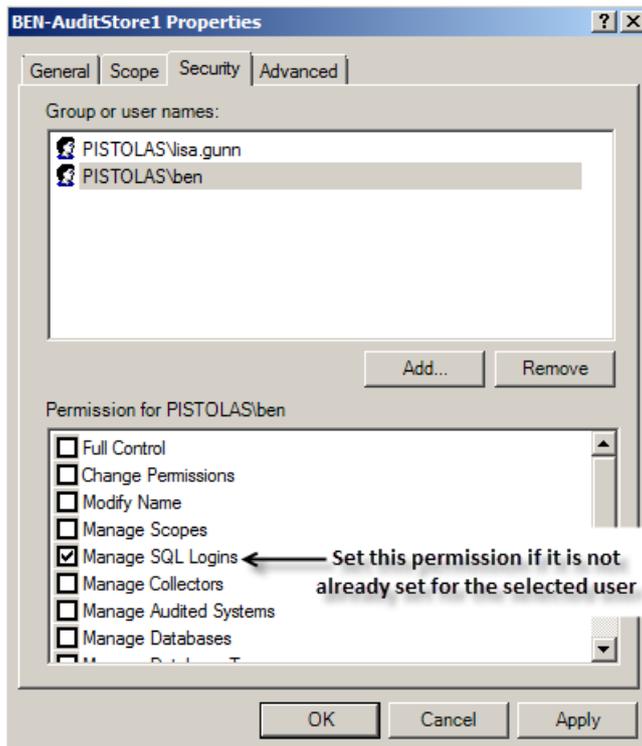
Before you configure a collector, you should check whether your user account has sufficient permissions to add new collector accounts to the audit store database. If you are a database administrator or logged on with an account that has system administrator privileges, you should be able to configure the collector without modifying your account permissions. If you have administrative rights on the computer hosting Audit Manager but are not a database administrator, you can set the appropriate permission before continuing.

To set the permission required to add accounts to the audit store database:

1. Open Audit Manager.
2. Expand the installation, then expand Audit Stores.
3. Select the audit store that the collector will connect to, right-click, then click **Properties**.
4. Click the **Security** tab.
5. Click **Add** to search for and select the user who will configure the collector.



6. Select the **Manage SQL Logins** right, then click **OK**.



Install the collector service using the setup program

If your user account has sufficient permissions to add new collector accounts to the audit store database, you can install a collector by running the Centrifry setup program on a selected computer. When prompted to select components, select Audit Collector and deselect all of the other components, then click **Next**. Follow the instructions in the wizard to select the location for installing files and to confirm your selections, then click **Finish** to complete the installation.

Configure the audit collector service

By default, when you click **Finish**, the setup program opens the Collector Configuration Wizard. Alternatively, you can start the configuration wizard at any time by clicking Configure in the Collector Control Panel.



To configure the collector service:

1. Type the port number to use, then click **Next**.

The default port is 5063 for communication from agents to the collector. If you want to use a different port, the wizard checks whether the port is open in the Windows firewall.

If you're running another firewall product, open the port with the tools provided by that product. If there's an upstream firewall—such as a dedicated firewall appliance—between the Collector and the computers to be audited, contact the appropriate personnel to open the port on that firewall.

2. Select the installation of which this collector will be a part, then click **Next**.

The configuration wizard verifies that the installation has an audit store that services the site that the collector is in and that the collector and its audit store database are compatible.

3. Select whether you want to use Windows authentication or SQL Server authentication when the collector authenticates to the audit store database, then click **Next**.

In most cases, you should choose Windows authentication to add the computer account to the audit store database as a trusted, incoming user.

If Microsoft SQL server is in a different forest or in an untrusted forest, you should use SQL Server Management Studio to set up one or more SQL Server login accounts for the collector. After you create the SQL Server login account for the collector to use, you can select SQL Server authentication, then type the SQL Server login name and password in the wizard.

4. Choose the maximum number of connections you want for the SQL Server Connection Pool, then click **Next**.
5. Review your settings for the collector, then click **Next**.
6. Click **Finish** to start the collector service and close the wizard.

Installing the Centrifry Agent for Windows

You must install an agent on every Windows computer that you want to manage or audit. You can install the agent in the following ways:



- Interactively, by running the Centrify setup program on each computer.

When the installation finishes, the agent configuration panel launches automatically. You can configure the agent to enable Centrify services right away, or exit the configuration panel and configure the agent later. See [Installing the Centrify Agent for Windows interactively using the setup program](#) for details about this installation method.

- Silently, by executing appropriate commands in a terminal window on each computer. This method also requires you to configure the agent registry settings on each computer. See [Installing the Centrify Agent for Windows silently on remote Windows computers](#) for details about this installation method.

A variation of this method is to use a third-party software distribution product, such as Microsoft System Center Configuration Manager (SCCM), to execute the appropriate command line remotely, so that the software is deployed on remote computers. Using a third-party software distribution product is not covered in this guide.

- Silently and centrally, by using a Windows group policy to execute installation and registry configuration commands remotely on each computer that is joined to the domain. See [Installing the Centrify Agent for Windows silently on all domain computers by using group policy](#) for details about this installation method.

Regardless of the deployment method you choose, you should first make sure that the computers where you plan to deploy meet all of the installation prerequisites.

Verifying prerequisites

Before installing the Centrify Agent for Windows, verify the computer on which you plan to install meets the following requirements:

- The computer is running a supported Windows operating system version.
- The computer is joined to Active Directory.
- The computer has sufficient processing power, memory, and disk space for the agent to use.
- The computer has Windows security update KB3033929 installed if it is running Windows 7 with Service Pack 1 or Windows Server 2008 R2 with Service Pack 1.



- The computer has .NET 4.6.2 or later installed.
- The computer has Windows Installer version 4.5 or newer.

If you are installing interactively using the setup program, the setup program can check that the local computer meets these requirements and install any missing software required. If you are installing silently or from a Group Policy Object, you should verify the computers where you plan to install meet these requirements.

Installing the Centrify Agent for Windows interactively using the setup program

The procedure in this section describes how to use the agent installation wizard to install the agent on a Windows computer. After the agent is installed, you will enable the agent to use one or more services that you installed earlier on the main administrative computer as described in [Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory](#).

To install the agent on Windows using the setup program:

1. Insert the Centrify distribution CD into the computer on which you wish to install the agent or browse to the location where you have saved downloaded Centrify 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 installation of Centrify software.
3. If a previous version of the agent is installed, click **Yes** when prompted to upgrade the Centrify 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 Centrify Agent for Windows page, click **Install**.
8. Click **Finish** to complete the installation and start the agent configuration



panel.

Go to [Configuring the agent](#) for details about using the agent configuration panel to enable Centrify services and configure how the agent interacts with those services.

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 Centrify services that are installed on the main administrative computer as described in [Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory](#). 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 [Running the setup program on a Windows computer](#)) 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 Centrify services that are available to be enabled are displayed.
3. In the list of Centrify services, highlight a service and click **OK**.
4. Provide additional information about the service that you are enabling:
 - **Centrify 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.



- **Centrify Identity Services 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.

- **Centrify Privilege Elevation Service:**

- 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 **Centrify Identity Services 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 Centrify 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 Centrify Identity Services Platform](#)
- [Configuring agent settings for privilege elevation](#)

Configuring agent settings for the 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 Centrify services that are currently enabled. You can configure any service listed in the **Enabled services** section.
2. Click **Centrify 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.
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 [Monitoring collector status locally](#).



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 Centrify Identity Services Platform

If you want to reconfigure agent settings for the Centrify Identity Services Platform 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 Centrify Identity Services Platform:

1. In the Windows Start menu, click **Agent Configuration** in the list of applications.
The agent configuration panel opens, and displays the Centrify services that are currently enabled. You can configure any service listed in the **Enabled services** section.
2. Click **Centrify Identity Services Platform**, and then click **Settings**.
3. In the General tab, review the authentication options in the Features area:

- **Multi-factor authentication:**

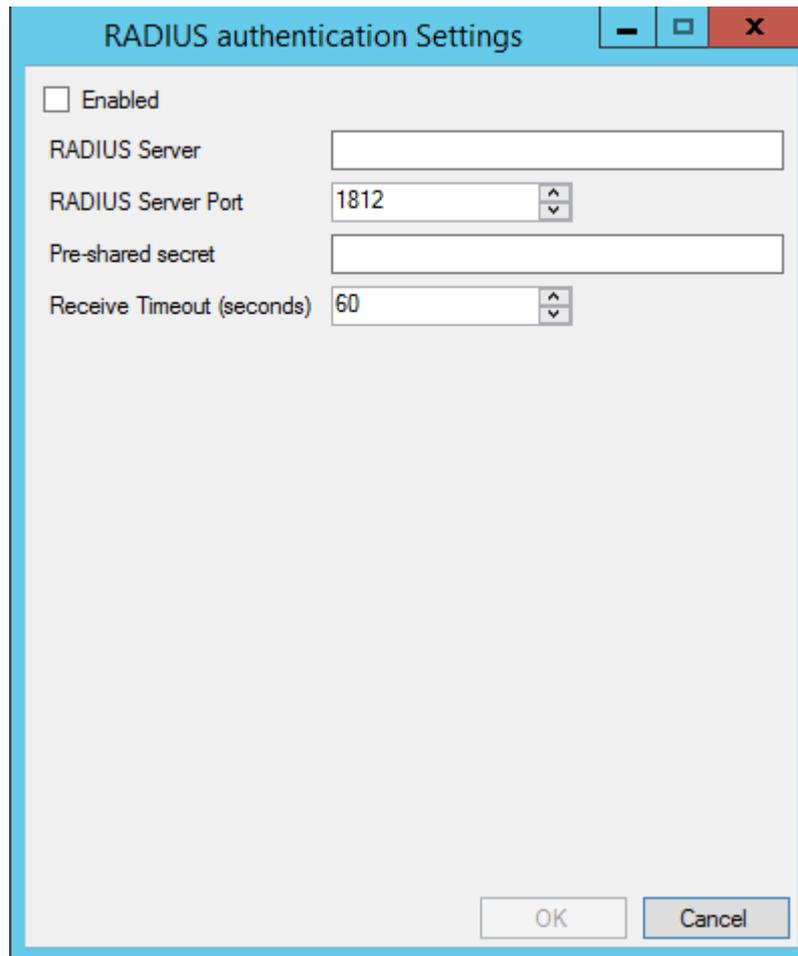
- If the status is **Enabled**, the computer is not joined to a zone, and you can configure all Identity Platform settings that are shown in the General tab.
- If the status is **Enabled per zone settings**, the computer is joined to a zone, and most Identity Platform settings are based on the zone configuration.

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.

Multi-factor authentication displays in the Authentication Source drop-down once the status is Enabled per zone settings.

- **RADIUS authentication:**

- If the status is **Enabled**, you can select this option to use as the authentication option for privilege elevation. You can enable this option either by group policy or a local configuration setting.
- If the status is **Disabled**, click **Details** to configure and enable the RADIUS server connection.



RADIUS authentication displays in the Authentication Source drop-down once the status is Enabled.

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 service), you can open the agent configuration panel manually and configure the agent as described in this section.

If you haven't yet configured the agent settings for privilege elevation, see [Configuring the agent](#) for details.

To configure existing agent settings for privilege elevation:

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

The agent configuration control panel opens, and displays the Centrify services that are currently enabled. You can configure any service listed in the **Enabled services** section.
2. Click **Centrify Privilege Elevation Service**, and then click **Settings**.
3. In the General tab, click **Change**.
4. In **Change the Centrify 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 [Running diagnostics and viewing logs for the agent](#).

Installing the agent without MFA login

If desired, you can install the Centrify Agent for Windows without the MFA login feature. This can be useful in situations where either you don't want to enforce multi-factor authentication or you don't use Privileged Access Service.

To install the Centrify Agent for Windows without the MFA login feature:

- Run the following command:

```
msiexec /i "Centrify Agent for windows64.msi" /qn PRIVILEGEONLY=1
```

Installing the Centrify Agent for Windows silently on remote Windows computers

If you want to perform a “silent” (also called *unattended*) installation of the Centrify Agent for Windows, you can do so by specifying the appropriate command line options and Microsoft Windows Installer (MSI) file to deploy. You must execute the commands on every Windows computer that you want to manage or audit.

Note: You can also use a silent installation to automate the installation or upgrade of the agent on remote computers if you use a software distribution product, such as Microsoft System Center Configuration Manager (SCCM), to deploy software packages. However, installing remotely in this way is not covered in this topic.

Deciding to install with or without joining the computer to a zone

Before you begin a silent installation, you should decide whether you will wait until later to join the computer to a zone, or join the computer to a zone as part of the installation procedure.

If you install without joining a zone during installation:

- See [Configuring registry settings](#) for details about the registry settings that you can configure manually after the installation finishes.



- See [Installing silently without joining a zone](#) for details about performing the installation.

If you install and join a zone during installation:

- You use a transform (MST) file that is provided with Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service to configure a default set of agent-specific registry keys during the silent installation.
- You can optionally edit the MST file before performing the installation to customize agent-specific registry settings for your environment.
- You can optionally use the registry editor to configure registry settings after the installation finishes.
- See [Configuring registry settings](#) for details about the registry settings that you can configure by editing the MST file.
- See [Editing the default transform \(MST\) file](#) for details about how to edit the MST file before you perform the installation.
- See [Installing and joining a zone silently](#) for details about performing the installation.

Configuring registry settings

When you perform a silent installation, several registry settings specific to the agent are configured by the default MSI file. In addition, a default transform (MST) file is provided for you to use if you join the computer to a zone as part of the installation procedure. When executed together, the default MSI and MST files ensure that the computer is joined to a zone, and that a default set of agent-specific registry keys is configured.

If your environment requires different or additional registry settings, you can edit the MST file before performing an installation. Then, when you execute the MSI and MST files to perform an installation, your customized registry settings are implemented. For details about how to edit the MST file, see [Editing the default transform \(MST\) file](#).

Note: If you do not join the computer to a zone during installation, you do not use the MST file. In this situation, you can create or edit registry keys manually after the installation finishes by using the, or the registry editor.

The following table describes the agent-specific registry settings that are available for you to configure during installation (by using the MST file) or after



installation (by using the or the registry editor). Use the information in this table if you need to configure registry settings differently than how they are configured by the default MSI and MST files. Keep the following in mind as you review the information in the table:

- The default MSI file is named `Centrify Agent for windows64.msi`, and is located in the **Agent** folder in the Centrify download location.
- The default MST file is named `Group Policy Deployment.mst`, and is located in the **Agent** folder in the Centrify download location.
- If you want to install the agent without the MFA login feature, use the `Group Policy Deployment-PrivilegeOnly.mst`, and is located in the **Agent** folder in the Centrify download location.
- All of the settings in the following table are optional, although some are included in the default MSI and MST files so that they are configured when the MSI and MST files execute during an installation.
- Settings that are included in the default MSI and MST files are noted in the table.
- Some settings are environment-specific, and therefore do not have a default value. Others are not environment-specific, and do have a default value.
- The settings described in the table are located in the MSI file's Property table.
- The **Setting** column shows both the property name in the MSI file, and the name (in parentheses) of the registry key in the Windows registry.



| Service | Setting | Description |
|-------------------------|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auditing and Monitoring | REG_MAX_FORMAT (MaxFormat) | <p>Specifies the color depth of sessions recorded by the agent.</p> <p>The color depth affects the resolution of the activity recorded and the size of the records stored in the audit store database when you have video capture auditing enabled. You can set the color depth to one of the following values:</p> <ul style="list-style-type: none">0 to use the native color depth on an audited computer.1 for a low resolution with an 8-bit color depth2 for medium resolution with a 16-bit color depth (default)4 for highest resolution with a 32-bit color <p>This setting is included in the default MSI file. In the registry, this setting is specified by a numeral (for example, 1). In the MSI file Property table, it is specified by the # character and a numeral (such as #1). The default value is 1.</p> |
| Auditing and Monitoring | REG_DISK_CHECK_THRESHOLD (DiskCheckThreshold) | <p>Specifies the minimum amount of disk space that must be available on the disk volume that contains the offline data storage file. You can change the percentage required to be available by modifying this registry key value.</p> <p>This setting is included in the default MSI file. In the registry, this setting is specified by a numeral (for example, 1). In the MSI file Property table, it is specified by the # character and a numeral (such as #10).</p> <p>The default value is 10, meaning that at least 10% of the disk space on the volume that contains the offline data storage file must be available. If this threshold is reached and there are no collectors available, the agent stops spooling data and audit data is lost.</p> |



| Service | Setting | Description |
|----------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auditing and Monitoring | REG_SPOOL_DIR (SpoolDir) | <p>Specifies the offline data storage location.</p> <p>The folder location you specify will be where the agent saves (“spools”) data when it cannot connect to a collector.</p> <p>This setting is not included in the default MSI file. To use it, you must edit the default transform (MST) file so that it is processed together with the MSI file during installation, or create it manually in the registry after the installation finishes.</p> |
| Auditing and Monitoring | REG_INSTALLATION_ID (InstallationId) | <p>Specifies the unique global identifier (GUID) associated with the installation service connection point.</p> <p>This setting is not included in the default MSI file. To use it, you must edit the default transform (MST) file so that it is processed together with the MSI file during installation, or create it manually in the registry after the installation finishes.</p> |
| Auditing and Monitoring | REG_LOG_LEVEL_DA (LogLevel) | <p>Specifies what level of information, if any, is logged. Possible values are:</p> <ul style="list-style-type: none">■ off■ information■ warning■ error■ verbose <p>This setting is included in the default MSI file. The default value is <code>information</code>.</p> |
| Authentication & Privilege | REG_RESCUEUSERSIDS (RescueUserSids) | <p>Specifies which users have rescue rights. Type user SID strings in a comma separated list. For example:</p> <p><i>user1SID,user2SID,usernSID</i></p> <p>This setting is not included in the default MSI file. To use it, you must edit the default transform (MST) file so that the setting is processed together with the MSI file during installation, or create it manually in the registry after the installation finishes.</p> |



| Service | Setting | Description |
|----------------------------|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication & Privilege | REG_LOG_LEVEL_DZ (LoggingLevel) | <p>Specifies what level of information, if any, is logged. Possible values are:</p> <ul style="list-style-type: none">offinformationwarningerrorverbose <p>This setting is included in the default MSI file. The default value is <code>information</code>.</p> |
| Authentication & Privilege | GPDeployment | <p>Specifies whether the computer is joined to the zone where the computer was pre-created. This setting is used only during installation and does not have a corresponding registry key. Possible values are:</p> <ul style="list-style-type: none">0 - The computer is not joined to the zone.1 - The computer is joined to the zone. <p>This setting is included in the default transform (MST) file. To use it, you must execute the MST file when you execute the default MSI file. The default value is 1, meaning that the pre-created computer is joined to the zone.</p> |
| Authentication & Privilege | ZONEDATA | <p>Specifies 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.</p> <p>Possible values are:</p> <ul style="list-style-type: none">YESNO <p>The default value is NO in the default MSI file.</p> |

Editing the default transform (MST) file

This section describes how to edit the default transform (MST) file `Group Policy Deployment.mst`. You execute the MST file together with the installation (MSI) file during a silent installation if you want to join the computer to a zone as part of the installation.

The MST file specifies registry key settings that are different from those specified in the MSI file. You use the MST file to customize a silent installation



for a specific environment. Using an MST file makes it unnecessary to edit registry keys manually after a silent installation.

Note: By default, auditing features are installed when you install the Centrifify Agent for Windows. The service is not enabled by default, but the service item in the configuration panel appears if the feature is enabled through group policy.

See [Installing and joining a zone silently](#) for instructions about how and when to execute the MST file.

To edit the default MST file:

1. You will use the Orca MSI editor to edit the MST file. Orca is one of the tools available in the Windows SDK. If the Windows SDK (or Orca) is not installed on your computer, download and install it now from this location: [https://msdn.microsoft.com/en-us/library/aa370557\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa370557(v=vs.85).aspx)
2. Execute `Orca.exe` to launch Orca.
3. In the **Agent** folder in the Centrifify download location, copy `Group Policy Deployment.mst` so that you have a backup.
4. In Orca, select **File > Open** and open the `Centrifify Agent for windows64.msi` file located in the **Agent** folder in the Centrifify download location.
5. In Orca, select **Transform > Apply Transform**.
6. In Orca, navigate to the **Agent** folder in the Centrifify download location and open `Group Policy Deployment.mst`.

The file is now in transform edit mode, and you can modify data rows in it.

7. In the Orca left pane, select the Property table.

Notice that a green bar displays to the left of “Property” in the left pane. This indicates that the Property table will be modified by the MST file.

The right pane displays the properties that configure registry keys when the MSI file executes. Notice that the last property in the table, `GPDeployment`, is highlighted in a green box. This indicates that the `GPDeployment` property will be added to the MSI file by the MST file.

Note: In order for the computer to join a zone during installation, the `Group Policy Deployment.mst` file must specify the `GPDeployment` property with a value of 1.



8. In the right pane, edit or add properties as necessary to configure registry keys for your environment. See the table in [Configuring registry settings](#) for details about agent-specific properties that are typically set.
 - To edit an existing property, double click its value in the **Value** column and type a new value.
 - To add a new property, right-click anywhere in the property table and select **Add Row**.
9. After you have made all necessary modifications, select **Transform > Generate Transform** to save your modifications to the default MST file. Be sure to save the MST file in the same folder as the MSI file. If the MST and MSI files are in different folders, the MST file will not execute when you execute the MSI file.

The MST file is now ready to be used as described in [Installing and joining a zone silently](#).

Installing silently without joining a zone

This section describes how to install the agent silently without joining the computer to a zone. This procedure includes configuring registry settings manually using the registry editor or a third-party tool.

Note: To install the agent and join the computer to a zone during installation, see [Installing and joining a zone silently](#) for more information.

Check prerequisites:

1. Verify that the computers where you plan to install meet the prerequisites described in [Verifying prerequisites](#). If prerequisites are not met, the silent installation will fail.
2. If you are installing audit and monitoring service, verify that the following tasks have been completed:
 - a. Installed and configured the SQL Server management database and the SQL Server audit store database.
 - b. Installed and configured one or more collectors.
 - c. Configured and applied the Centrify DirectAudit Settings group policy that specifies the installation name.



To install the Centrify Agent for Windows silently without joining the computer to a zone:

1. Open a Command Prompt window or prepare a software distribution package for deployment on remote computers.

For information about preparing to deploy software on remote computers, see the documentation for the specific software distribution product you are using. For example, if you are using Microsoft System Center Configuration Manager (SCCM), see the Configuration Manager documentation.

2. Run the installer for the Centrify Agent for Windows package. For example:

```
msiexec /qn /i "Centrify Agent for windows64.msi"
```

By default, none of the services are enabled.

3. Use the registry editor or a configuration management product to configure the registry settings for each agent. See the table in [Configuring registry settings](#) for details about agent-specific registry keys that you can set.

For example, under HKEY_LOCAL_MACHINE\Software\Centrify\DirectAudit\Agent, you could set the DiskCheckThreshold key to a value other than the default value of 10%.

Installing and joining a zone silently

This section describes how to install the agent and join the computer to a zone at the same time. The procedure described here includes the following steps in addition to executing the MSI file:

- You first prepare (pre-create) the Windows computer account in the appropriate zone.
- You execute an MST file together with the MSI file to join the computer to a zone and configure registry settings during the installation.

Note: Joining the computer to a domain is applicable only when you are enabling Authentication & Privilege features.

To install the agent without joining the computer to a zone during installation, see [Installing silently without joining a zone](#) for more information.



Check prerequisites:

1. Verify that the computers where you plan to install meet the prerequisites described in [Verifying prerequisites](#). If prerequisites are not met, the silent installation will fail.
2. If you are enabling audit and monitoring service in addition to Authentication & Privilege, verify that the following tasks have been completed:
 - a. Installed and configured the SQL Server management database and the SQL Server audit store database.
 - b. Installed and configured one or more collectors.
 - c. Configured and applied the Centrify DirectAudit Settings group policy that specifies the installation name.

To install the Centrify Agent for Windows and add a computer to a zone during installation:

1. Prepare a computer account in the appropriate zone using Access Manager or the PowerShell command `New-CdmManagedComputer`. See [Preparing Windows computer accounts](#) for more information.
2. You will use the default transform file `Group Policy Deployment.mst` in Step 3 to update the MSI installation file so that the computer is joined to the zone in which it was pre-created in Step 1. You can optionally modify `Group Policy Deployment.mst` to change or add additional registry settings during installation.

If you want to edit `Group Policy Deployment.mst` to change or add additional registry settings and have not yet done so, edit it now as described in [Editing the default transform \(MST\) file](#).

In order for the computer to join the zone from Step 1, the `Group Policy Deployment.mst` file must specify the `GPDeployment` property with a value of 1.

3. Run the following command:

```
msiexec /i "Centrify Agent for windows64.msi" /qn TRANSFORMS="Group Policy Deployment.mst"
```

By default, Centrify Privilege Elevation Service is enabled by joining a zone. If the zone is also configured with a platform instance (tenant), Identity Services Platform will also be enabled. If you want to enable auditing, configure the corresponding registry value in the Property page of the MST file: `REG_CURRENT_INSTALLATION` or via Group Policy.



You can also choose to install the specify 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. To specify that the agent retrieves zone data before the computer restarts, run the following command:

```
msiexec /i "Centrify Agent for windows64.msi" /qn TRANSFORMS="Group Policy Deployment.mst" ZONEDATA="YES"
```

The computer will be restarted automatically to complete the deployment and start the agent.

Installing the Centrify Agent for Windows silently on all domain computers by using group policy

You can use a group policy object (GPO) to automate the deployment of the Centrify Agent for Windows. Because automated installation fails if all the prerequisites are not met, be sure that all the computers on which you intend to install meet the requirements described in [Verifying prerequisites](#).

Note: If you install the Centrify Common Component before you install the agent, information about the installation of the agent can be captured in a log file for troubleshooting purposes.

To create a new group policy object for the deployment of the Centrify Agent for Windows:

1. Prepare computer accounts in the appropriate zones using Access Manager or the PowerShell command `New-CdmManagedComputer`. See [Preparing Windows computer accounts](#) for more information.
2. Copy the `Centrify Agent for windows64.msi` and `Group Policy Deployment.mst` installer files to a shared folder on the domain controller or another location accessible from the domain controller.
When you select a folder for the agent installer files, right-click and select **Share with > Specific people** to verify that the folder is shared with Everyone or with appropriate users and groups.
3. Right-click on the `Centrify Agent for windows64.msi` file, then select **Edit with Orca**.
4. Select **Transform > Apply Transform**, then select `Group Policy Deployment.mst` from the same location as the `Centrify Agent for windows64.msi` file.



5. Select the Property table on the left hand side and add the following:

| Property | Value | Comments |
|----------------------------------------------|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| REG_ ZONELESS_ MFA_TENANT | Tenant URL | (Ex: https://aaa1111.my.centrixy.net:443/) Note: You must include "https://" and ":443/" |
| REG_ ZONELESS_ MFA_ENABLED | true | Default Value = false |
| REG_ EFFECTIVE_ ZONELESS_ MFA_USERS | Comma-Separated user or group names, or enter * for All AD users | |
| REG_ CONNECTOR_ BRANDING | Centrixy | |

6. Close Orca and save the changes as a new mst file.
Make sure you save it in the same location as the msi file.
7. On the domain controller, click **Start > Administrative Tools > Group Policy Management**.
8. Select the domain or organizational unit that has the Windows computers where you want to deploy the Centrixy agent, right-click, then select **Create a GPO in this domain, and Link it here**.
9. For example, you might have an organizational unit specifically for Centrixy-managed Windows computers. You can create a group policy object and link it to that specific organizational unit.
10. Type a name for the new group policy object, for example, Centrixy Agent Deployment, and click **OK**.
11. Right-click the new group policy object and click **Edit**.
12. Expand **Computer Configuration > Policies > Software Settings**.
13. Select **Software installation**, right-click, and select **New > Package**.
14. Navigate to the folder you selected previously, then select the Centrixy Agent for windows64.msi file, and click **Open**.
15. Select **Advanced** and click **OK**.
16. Click the **Modifications** tab and click **Add**.
17. Select the .mst file created previously, then click **Open**, and click **OK**.



18. Close the Group Policy Management Editor, right-click the **Centrify Agent Deployment** group policy object, and verify that **Link Enabled** is selected.

By default, when computers in the selected domain or organizational unit receive the next group policy update or are restarted, the agent will be deployed and the computer will be automatically rebooted to complete the deployment of the agent.

If you want to test deployment, you can open a Command Prompt window to log on to a Windows client as a domain administrator and force group policies to be updated immediately by running the following command:

```
gpupdate /force
```

After installation, all of the registry settings that were specified in the MSI and MST files are configured. If you need to further configure registry settings, use the registry editor to do so as described in [Installing the Centrify Agent for Windows silently on remote Windows computers](#).

Installing the agent on a computer running Server Core

You cannot use the `autorun.exe` or the `setup.exe` program to install components on a computer that is configured to run as a Server Core environment. Instead, you must install from Microsoft Installer (`.msi`) files using the `msiexec` command-line program.

To install the Centrify Agent for Windows on Server Core:

1. Use the Deployment Image Servicing and Management (DISM) or another command-line tool to enable the .NET Framework.

For example, if the .NET Framework is located on the installation media in the `D:\sources\sxs` folder, use the following command:

```
DISM /Online /Enable-Feature /FeatureName:NetFx3 /All /LimitAccess /Source:D:\sources\sxs
```

2. Copy the Centrify Agent for Windows files to the Server Core computer.

For example:

```
copy D:\Common\Centrify* C:\CentrifyAgent
copy D:\Agent\* C:\CentrifyAgent
```



3. Install the Centrify Common Component service using the `.msi` file.
For example, to install the Centrify Common Component on a computer with 64-bit architecture, you might use the following command:

```
msiexec /i "Centrify Common Component64.msi" /qn
```

4. Install the Centrify Agent for Windows using the `.msi` file.
For example, to install the Centrify Agent for Windows with identity management, privilege elevation, auditing, and monitoring features enabled on a computer with 64-bit architecture, you might run the following command:

```
msiexec /qn /i "Centrify Agent for windows64.msi" ADDLOCAL=ALL
```

You can also choose to install the specify 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. To specify that the agent retrieves zone data before the computer restarts, run the following command:

```
msiexec /i "Centrify Agent for windows64.msi" /qn TRANSFORMS="Group Policy Deployment.mst" ZONEDATA="YES"
```

5. Restart the computer with the appropriate shutdown options to complete the installation and start agent services.

For example, you might run the following command:

```
shutdown /r
```

Installing additional consoles

You can install additional consoles on any domain computers you want to use for managing access using zones or roles, or for managing the audit and monitoring service infrastructure. You also might want to install additional consoles on the computers to be used by auditors. You can install additional consoles from the Centrify Management Services setup program or from individual component-specific setup programs. For example, you can use the Centrify Audit Analyzer Console.exe setup program to install Audit Analyzer on a computer.



Installing group policy extensions separately from Centrify Access Manager

Centrify group policy extensions are packaged separately from Access Manager, enabling the following installation options:

- You can install Centrify group policy extensions on any Windows domain computer without also installing Access Manager on the computer.
- You can install Access Manager on any Windows domain computer without also installing Centrify group policy extensions on the computer.

The group policy extension package has its own .exe and .msi installer files, so that you can install group policy extensions interactively through an installation wizard (by executing the .exe file) or silently from the command line (by executing the .msi file). Additionally, you can select or de-select the group policy extensions for installation when you run the Access Manager installation wizard.

Note: At the start of an installation, the group policy extension installer checks for previously installed versions of group policy extensions. If it detects a newer version than the version you are trying to install, the installation stops.

To install standalone group policy extensions interactively with the group policy installer:

1. On the Windows domain computer where you will install group policy extensions, navigate to the Centrify ISO bundle containing the group policy extension installer file.

The installer file is named `CentrifyDC_GP_Extension-#. #.#-architecture.exe`.

For example:

`CentrifyDC_GP_Extension-5.2.3-win64.exe`

In most distributions, the installer file is located in the following folder in the ISO bundle:

`DirectManage\Group Policy Management Editor Extension`

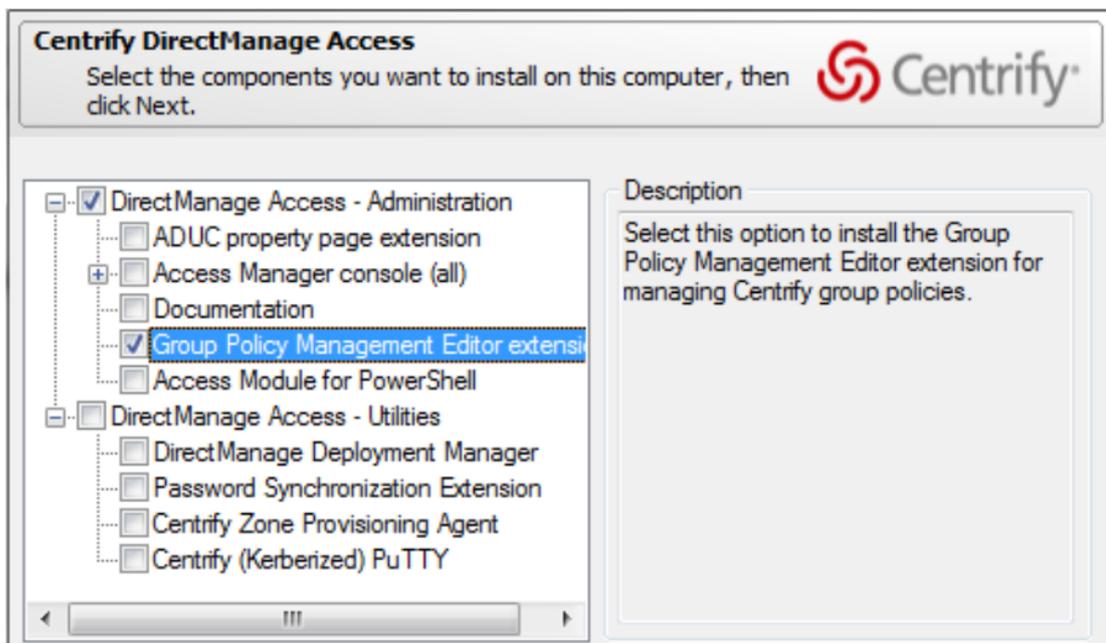
2. Double-click the installer file to launch the Centrify Group Policy Management Editor Extension Setup Wizard.



3. Follow the wizard installation instructions to install the group policy extensions.

To install standalone group policy extensions interactively with the Management Services installer:

1. On the Windows domain computer where you will install group policy extensions, launch the setup program for Centrify Management Services components as described in [Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory](#).
2. Proceed through the setup program until you reach the wizard page in which to select individual components to install.
3. De-select every component except for **Group Policy Management Editor extension for managing Centrify group policies**:



4. Continue to follow the wizard installation instructions as described in [Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory](#) until you are finished with the installation.



To install standalone group policy extensions silently without installing Access Manager:

1. Open a Command Prompt window.
2. Execute the group policy extension .msi installer file from the command line.

The installer file is named `CentrifyDC_GP_Extension-#.##-architecture.msi`.

For example:

```
CentrifyDC_GP_Extension-5.2.3-win64.msi
```

In most distributions, the installer file is located in the following folder in the ISO bundle:

```
DirectManage\Group Policy Management Editor Extension
```

The following is a typical command to run the 64-bit .msi installer file:

```
msiexec /qn /i "CentrifyDC_GP_Extension-5.2.3-win64.msi"
```

For more information about installing with a .msi file, see [Installing the Centrify Agent for Windows silently on remote Windows computers](#).

To install Access Manager interactively without installing group policies:

1. On the Windows domain computer where you will install group policy extensions, launch the Centrify Management Services setup program and select Authentication & Privilege as described in [Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory](#).
2. Proceed through the setup program until you reach the wizard page in which to select individual components to install.
3. De-select the **Group Policy Management Editor extension** component.
4. Continue to follow the wizard installation instructions as described in [Installing authentication, privilege elevation, and audit and monitoring services and updating Active Directory](#) until you are finished with the installation.



Managing zones

Zones are the key component for organizing access rights and role assignments for Windows computers. This chapter describes how to use Access Manager to create zones, manage zone properties, add Windows computers to selected zones, and move and rename zone objects.

The following topics are covered:

| | |
|-----------------------------------------------------------|-----|
| Starting Centrify Access Manager for the first time | 109 |
| Preparing to use zones | 113 |
| Creating a new parent zone | 117 |
| Creating child zones | 120 |
| Opening and closing zones | 122 |
| Changing zone properties | 123 |
| Delegating control of administrative tasks | 124 |
| Adding Windows computers to a zone | 127 |
| Preparing Windows computer accounts | 127 |
| Changing the zone for the computer | 128 |
| Leaving a zone | 128 |
| Renaming a zone | 129 |
| Working directly with managed computers | 131 |

Starting Centrify Access Manager for the first time

The first time you start Access Manager, a Setup Wizard prepares the Active Directory forest with parent containers for licenses and zones. The Setup



Wizard also sets the appropriate permissions for the objects. For example, all authenticated users are granted read access of the Licenses container by default. These steps are typically performed once by a domain administrator. If you choose to, you can create the container objects manually.

What to do before updating Active Directory

Before you use Access Manager the first time, you should contact the Active Directory administrator to determine the appropriate location for the Licenses and Zones parent containers and whether you have the appropriate rights for completing this task. The specific administrative rights required for this task depend on the policies of your organization and who has permission to create classStore and parent and child container objects in Active Directory.

Rights required for this task

If you don't have administrative rights to create container objects in Active Directory, a domain administrator in the forest root domain can manually create the container objects and set the rights on those objects to allow other users to complete the initial configuration without being members of an administrative group.

The following table describes the minimum rights that must be granted on manually created container objects for other users to successfully complete the configuration with the Setup Wizard.

| This target object | Requires these permissions | Applied to |
|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------|-----------------------------------|
| Licenses container | ■ Read all properties | This object only |
| | ■ Create classStore objects | |
| | ■ Modify permissions | |
| | ■ Write Description property | This object and all child objects |
| | ■ Write displayName property | |
| By default, all Authenticated Users have read and list contents permission for the Licenses container and all of its child objects. | | |
| Zones container | ■ Read all properties | This object only |
| | ■ Create classStore objects | |
| | ■ Create Container objects | |
| | ■ Write displayName property | This object and all child objects |



If you are a domain administrator and use the Setup Wizard to create the container objects, you should add a security group for Zone Administrators to Active Directory. Set the following permissions on the parent Zones container to allow other users to manage zones.

| This target object | Requires these permissions | Applied to |
|--------------------|------------------------------|-----------------------------------|
| Zones container | ■ Read all properties | |
| | ■ Create Container objects | This object only |
| | ■ Delete Container objects | |
| | ■ Write displayName property | This object and all child objects |

Who should perform this task

A Windows Active Directory administrator performs this task, depending on your organization's policies, by running the Setup Wizard or by manually creating container objects and notifying another user of the location of the container objects. The user who runs the Setup Wizard must be granted the rights required to create classStore objects.

How often you should perform this task

In most organizations, you only do this once for an Active Directory forest. However, if you want to create more than one administrative boundary, you can create additional parent containers as needed.

Steps for completing this task

The following instructions illustrate how to run the Setup Wizard from Access Manager.

To update Active Directory using Access Manager:

1. Open Access Manager.
2. At the Welcome page, click **Next**.
3. Select **Use currently connected user credentials** to use your current log on account or select **Specify alternate user credentials** and type a user name and password, then click **Next**.



4. Select a location for installing license keys in Active Directory, then click **Next**.

The default container for license keys is *domain_name/Program Data/Centrify/Licenses*. To create or select a container object in a different location, click **Browse**. If an Active Directory administrator has created the Licenses container for you, click Browse and navigate to the appropriate location. The Setup Wizard will create a `classStore` object in the location you specify.

You can create additional containers in other locations later using the Manage Licenses dialog box.

5. Review the permission requirements for the container, then click **Yes** to confirm your selection.

6. Type or copy and paste the license key you received, then click **Add**.

If you received multiple license keys, add each key to the list of installed licenses, then click **Next**. If you received license keys in a text file, click **Import** to import the keys directly from the file instead of adding the keys individually, then click **Next**.

7. Select **Create default zone container** and specify a location for the Zones container, then click **Next**.

The default container location for zones is *domain_name/Program Data/Centrify/Zones*. To create or select a container object in a different location, click **Browse**. If an Active Directory administrator has created the Zones container for you, click Browse and navigate to the appropriate location. The Setup Wizard will create a `classStore` object in the location you specify.

Any zones you create are placed in this container location by default.

The next three pages only apply if you are managing multiple platforms. For a Windows-only deployment, you can click **Next** to leave the following options unselected:

- Grant computer accounts in the Computers container permission to update their own account information.
- Register administrative notification handler for Microsoft Active Directory Users and Computers snap-in.
- Activate Centrify profile property pages.

8. Review and confirm your configuration settings, click **Next**, then click **Finish**.

After you click Finish, the Access Manager console is displayed.



What to do next

Create at least one parent zone.

Where you can find additional information

If you want to learn more about the importance and benefits of using zones, see the following topics for additional information:

- [Access control for Windows computers](#)
- [How zones organize access rights and roles](#)
- [Identity and privilege management](#)

Preparing to use zones

One of the most important aspects of managing computers with Centrify software is the ability to organize computers, users, and groups into **zones**. You use zones to create logical groupings for:

- Managing access rights, role definitions, and role assignments.
- Delegating administrative tasks based on a separation of duties.
- Associating groups of computers and groups of users with specific role assignments.

Controlling access through hierarchical zones

Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service for Windows only supports **hierarchical zones**. Hierarchical zones enable you to establish parent-child zone relationships, allowing rights, role definitions, and role assignments to be inherited down the zone hierarchy. One of the first decisions you need to make is how you can use the zone hierarchy most effectively.

With hierarchical zones, you define rights and roles in a parent zone so that those definitions are available in one or more child zones, as needed. Child zones can also inherit user and group role assignments. At any point in the zone hierarchy, you can choose to use or override information from a parent zone.



There are no predefined limits to the number of zones that can be used in a zone hierarchy or the number of levels deep zones can be nested in the hierarchy you define. For practical purposes, keep the hierarchy similar to the following:

- One or more top-level **parent** zones that includes all users and groups.
- One to three levels of intermediate **child** zones based on natural access control or administrative boundaries.

There are many different approaches you can take to defining the scope of a zone, including organizing by platform, department, manager, application, geographical location, or how a computer is used. The factors that are most likely to affect the zone design, however, will involve managing access rights and roles and delegating administrative tasks to the appropriate users and groups.

Managing access rights and roles using zones

Zones enable you to grant specific rights to users in specific roles on specific computers. By assigning roles, you can control the scope of resources any particular group of users can access and what those users can do. For example, all of the computers in the finance department could be grouped into a single zone called “finance” and the members of that zone could be restricted to finance employees and senior managers, each with specific rights, such as permission to log on locally, access a database, update certain files, or generate reports.

Rights represent specific operations users are allowed to perform. A **role** is a collection of rights that can be defined in a parent or child zone and inherited. For example, a role defined in a parent zone can be used in a child zone, in a computer role, or at the computer level.

System and predefined rights

There are specialized login rights, called system rights. The system rights for Windows computers are:

- **Console login is allowed:** Specifies that users are allowed to log on locally using their Active Directory account credentials.
- **Remote login is allowed:** Specifies that users are allowed to log on remotely using their Active Directory account credentials.



- **PowerShell remote access is allowed:** Specifies that users are allowed to log on remotely to PowerShell.

There are additional predefined rights that allow access to specific applications. For example, there are predefined rights that allow users to run Performance Monitor or Server Manager without having an administrator's password. You grant users permission to access computers by assigning them to a role that includes at least one login right. You can then give them access to specific applications or privileges using additional predefined or custom access rights.

Granting permission to log on

By default, zones always provide the **Windows Login** role to allow users to log on locally or remotely to computers in the zone. Users must have at least one role assignment that grants console or remote login access or they will not be allowed to access any of the computers in the zone.

Note: The Windows Login role grants users the permission to log on whether they are authenticated by specifying a user name and password or by using a smart card and personal identification number (PIN).

Because the Windows Login role only allows users to log on, it is often assigned to users in a parent zone and inherited in child zones. However, the Windows Login role does not override any native Windows security policies. For example, most domain users are not allowed to log on to domain controllers. Assigning users the Windows Login role does not grant them permission to log on to the domain controllers. Similarly, if users are required to be members of a specific Windows security group, such as Server Operators or Remote Desktop Users, to log on to specific computers, the native Windows security policies take precedence.

There are additional predefined roles that grant specific rights, such as the **Rescue - always permit login** role that grants users the "rescue" right to log on if audit and monitoring service is required but not available. In general, at least one user should be assigned this role to ensure an administrator can log on if the audit and monitoring service fails or a computer becomes unstable.



Delegating administrative tasks in hierarchical zones

You can use zones to delegate administrative tasks to specific users or groups. Using hierarchical zones, you can give separate groups of administrators the authority to manage a different sets of computers and users without granting them permission to perform actions on other computers, in other zones, or on other Active Directory objects. You can also use zones to establish a separation of duties so that only specific groups or users can perform certain tasks. For example, you can create a child zone for software-development and give the `dev_mgrs` group authority to manage rights and roles and manage role assignments on the computers in that zone.

By creating child zones and delegating administrative tasks within those zones, you can group computers that form a natural administrative set or that should be managed by different administrative teams. For example, you might want to group computers that are managed by a local support organization in one zone and computers that are managed by a corporate IT group in another zone. You can also control what different groups of users can do within each child zone. For example, you can set up regional zones to provide a separation of duties, authorizing users in San Francisco to manage computers in their local office while a team in Barcelona has authority to join computers to the zone and manage role assignments for offices located in Spain but does not have the authority to add users or groups.

Associating computers and role assignments

You can use zones to associate a set of users with a particular role assignment to a particular set of computers. This association of a group of computers with a particular role assignment is called a **computer role**. For example, you might have several computers that are dedicated to a specific function, such as hosting Oracle databases, or to a functional area, such as payroll. Some groups of users who access these computers might require a specific set of rights. For example, the database administrators who access the computers hosting Oracle databases need different rights than users who are updating payroll records in the databases being hosted.

A computer role enables you to link the privileges associated with the database administrator role assignment, such as permission to backup and restore or create new tables, with the computers that host the Oracle databases. You can configure a separate computer role for the rights required by the users processing payroll on the same set of computers. The computer



role creates the link between users with a specific role assignment, database administrator or payroll department, and the computers where that role assignment applies.

If you add an Oracle database server, you add it to the computer group. If new users are assigned the database administrator role, they automatically receive the appropriate access rights on the computers hosting Oracle databases.

You can also use computer roles to specify whether you want session-level auditing for a group of computers.

Creating a new parent zone

In most cases, you design a basic zone structure as part of the deployment process. After the initial deployment, you can create new hierarchical zones any time you have new administrative boundaries. For example, if you acquire another organization, add offices that are managed by a different group, or restructure the organization along different functional lines, you are likely to need new zones.

What to do before creating a new parent zone

Before you can create parent zones, you must have installed Access Manager and run the Setup Wizard. You should also have a basic zone design that describes how you are organizing information, for example, whether you are using one top-level parent zone or more than one parent zone. There are no other prerequisites for performing this task.

Rights required for this task

Only the user who creates a zone has full control over the zone and can delegate administrative tasks to other users and groups through the Zone Delegation Wizard. To create new zones, your user account must be a domain user with the following permissions:



| Select this target object | To apply these permissions |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parent container for new zones, for example: <i>domain</i> <i>/Centrify/Zones</i> | On the Object tab, select Allow to apply the following permission to this object and all child objects: <ul style="list-style-type: none">■ Create Container Objects■ Create Organizational Unit Objects <p>Note: Both permissions are required if you want to allow zones to be created as either container objects or organizational unit objects.</p> |
| Parent container for Computers in the zone | On the Object tab, select Allow to apply the following permission to this object only: <ul style="list-style-type: none">■ Create group objects■ Write Description property |

Note: If the Active Directory administrator manually sets the permissions required to create zones, you should verify that the account also has permission to add an authorization store, define rights and roles, and manage role assignments.

Who should perform this task

A Windows domain administrator performs this task, depending on your organization's policies. The user who creates the zone is responsible for delegating administrative tasks to other users or groups, if necessary. In most organizations, this task is done using an account with domain administrator privileges.

How often you should perform this task

After you are fully deployed, you create new zones infrequently to address changes to your organization.

Steps for completing this task

The following instructions illustrate how to create a new parent zone using Access Manager. Examples of script that uses the Windows API are included in the Centrify Software Developer's Kit or may be available in community forums



on the Centrify website. For code examples using ADEdit, see the *ADEdit Command Reference and Scripting Guide*.

To create a new parent zone using Access Manager:

1. Open the Access Manager console.
2. In the console tree, select **Zones** and right-click, then click **Create New Zone**.

3. Type the zone name and, optionally, a longer description of the zone. In most cases, you should use the default parent container and container type that you created when you configured the Active Directory forest, then click **Next**.

For zones that include Windows computers, you should always use the default zone type, which creates the new zone as a hierarchical zone. For Windows computers, only hierarchical zones are supported. The only reasons for changing the default other settings would be if you want to:

- Create a zone in a new location to separate administrative activity for different groups of administrators.
- Create a zone as an organizational unit because you want to assign a Group Policy Object to the zone.

4. Review information about the zone you are creating, then click **Finish**.

What to do next

After you create a new parent zone, you might want to create its child zones.

Where you can find additional information

If you want to learn more about the importance and benefits of using zones, see the following topics for additional information:

- [How zones organize access rights and roles](#)
- [Preparing to use zones](#)



Creating child zones

For Windows, the primary reason for creating child zones is to inherit role definitions and role assignments from a parent zone. Less often, you might want to use a child zone to override role definitions and assignments that you have made in a parent zone. For example, if you have created a role definitions that allows a user to run a specific application with administrative privileges in a parent zone, you can use child zones to limit the scope of that right to specific subsets of computers.

What to do before creating child zones

Before you create child zones, you must have installed Access Manager, run the Setup Wizard to create the Zones container, and created at least one parent zone. You should also have a basic zone design that describes the zone hierarchy for the child zone. There are no other prerequisites for performing this task.

Rights required for this task

Only the user who creates a zone has full control over the zone and can delegate administrative tasks to other users and groups through the Zone Delegation Wizard. To create new child zones, your user account must be a domain user with the following permissions:



| Select this target object | To apply these permissions |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Container for the parent zones, for example if the parent zone is berlin: <i>domain/MyOU/Zones/berlin</i> | <p>On the Object tab, select Allow to apply the following permission to this object and all child objects:</p> <ul style="list-style-type: none">■ Create Container Objects■ Create Organizational Unit Objects <p>Note: Both permissions are required if you want to allow zones to be created as either container objects or organizational unit objects.</p> |
| Parent container for Computers in the zone | <p>On the Object tab, select Allow to apply the following permission to this object only:</p> <ul style="list-style-type: none">■ Create group objects■ Write Description property <p>These permissions are only needed if you are supporting “agentless” authentication in the new zone.</p> |

Note: If the Active Directory administrator manually sets the permissions required to create zones, you should verify that the account also has permission to add an authorization store, define rights and roles, and manage role assignments.

Who should perform this task

A Windows administrator performs this task, depending on your organization’s policies. The user who creates the zone is responsible for delegating administrative tasks to other users or groups, if necessary. In most organizations, this task is done using an account with domain administrator privileges.

How often you should perform this task

After you are fully deployed, you create new child zones infrequently to address changes to the scope of ownership and administrative tasks.



Steps for completing this task

The following instructions illustrate how to create a new child zone using Access Manager.

To create a new child zone using Access Manager:

1. Open the Access Manager console.
2. In the console tree, expand **Zones** and individual zones to select the parent zone for the new child zone.
3. Right-click, then click **Create Child Zone**.
4. Type the zone name and, optionally, a longer description of the zone. Because this is a child zone, you should use the default parent container and container type, then click **Next**.
5. Review information about the child zone, then click **Finish**.

Opening and closing zones

Because properties and objects are organized into zones, you must open a zone to work with its contents. If you open a parent zone, its child zones are also available for you to use by default. If you open a child zone, you can choose whether to open its parent zone. Once you open a zone, it stays open until you close it and you can have multiple zones and zone levels open at the same time. If you have a large number of zones, you should close any zones you aren't actively working with for better performance.

As an alternative to opening individual or parent and child zones manually, you can automatically load all zones in a forest or all zones in a specific container at startup time. If you choose to load all zones, you cannot manually close zones.

To open an individual parent or child zone:

1. Open Access Manager.
2. In the console tree, select **Zones** and right-click, then click **Open Zone**.
3. Type all or part of the name of the zone you want to open, then click **Find Now**.



4. Select the zone to open from the list of results, then click **OK**. You can use the CTRL and SHIFT keys to select multiple zones.

After you open the zones you want to work with, you should save your changes when you exit the Access Manager console, so that the open zones are displayed by default the next time you start the console.

To close an open zone:

1. Open Access Manager.
2. Expand the zone hierarchy until you can select the specific zone name you want to close
3. Right-click, then click **Close**.
4. Click **Yes** to confirm that you want to close the zone.

To load all zones automatically:

1. Open Access Manager.
2. In the console tree, select Centrify Access Manager, right-click, then click **Options**.
3. On the **Filter Settings** tab, select **Load all zones**, then select **connected forest** to automatically load all zones in the forest or click **Browse** to navigate to specific container.

Selecting this option prevents you from opening or closing any zones manually. You should not select the Load all zones option if you want to manually open and close individual zones for performance reasons.

Changing zone properties

After you create a zone, you can change its zone properties at any time. For example, if you want to change the parent zone for a child zone, you can do so by modifying the child zone's properties.



To change the properties for a zone:

1. Open Access Manager.
2. Expand **Zones** to display the list of zones, then expand the zone hierarchy until you see the zone you want to modify.
3. Select the zone, right-click, then click **Properties**.
4. On the General tab, you can view the location of the zone in Active Directory and the zone type.

From the General tab, you can make the following changes:

- Change the parent zone for a child zone.
- Modify the zone description.
- Select a specific Licenses container for the zone to use.
- Configure the access control list of permissions for the zone.

For example, click **Browse** to find and select a new zone to use as the parent of a child zone, then click **OK** to save the new zone properties. For Windows computers, only the properties on the General tab are applicable.

Moving a child zone to a new parent zone

You can make an existing zone a child of another zone by dragging and dropping it from one zone to another or by changing the Parent zone field on the zone's Properties General tab.

If a child zone inherits role assignments from its parent zone, the console displays a warning message and prevents you from moving the zone until you have removed the role assignments. If moving the zone creates a circular hierarchy, the console prevents you from moving the zone.

Delegating control of administrative tasks

If you are the creator of a parent or child zone, you can use the Access Manager console to give other users and groups permission to perform specific types of administrative tasks within each zone you create. For example, assume you have created a zone called Finance. Certain users or groups who access computers in that zone must be able to perform administrative tasks on their



own without your help. You want to give them the permissions they require to accomplish specific tasks without turning over full control to anyone except your most trusted administrative staff. Using Access Manager and the Zone Delegation Wizard, you select the appropriate groups and users for the Finance zone and specify exactly what each do. For example:

- Members of the group `Finance-ITStaff` are allowed to perform All administrative tasks within the Finance zone. They can change zone properties, join and remove computers from the zone, define rights and roles, and assign roles to users and groups. Only your most trusted administrative staff are members of this group.
- Members of the group `FinanceManagers` are allowed to join and remove computers from the zone and assign roles to users and groups.
- Members of the group `FinanceUsers` are allowed to add users, add groups, and join computers to the zone, but perform no other tasks.
- The users `jason.elliison` and `noah.stone` have permission to remove computers from the zone.

In most cases, each zone should have at least one Active Directory group that can be delegated to perform all administrative tasks, so that members of that group can manage their own zone. You are not required to create or use a zone administrator group for every zone. However, assigning the management of each zone to a specific user or group creates a natural separation of duties for administrative tasks.

If you delegate control for individual tasks—for example, by assigning only the join computers task to one group and only the add and remove users tasks to another—you should ensure the members of each group know the tasks they are assigned.

You can delegate administrative tasks for parent zones, for child zones, and for individual computers. Because computer-level overrides are essentially single computer zones, you can assign administrative tasks to users and groups at the computer level.

To delegate which users and groups have control over the objects in a zone:

1. Open Access Manager.
2. Expand **Zones** to display the list of zones, then expand the zone hierarchy until you see the specific zone you want to modify.
3. Select the zone, right-click, then click **Delegate Zone Control**.



4. Click **Add** to find the users, groups, or computer accounts to which you want to delegate specific tasks.
5. Select the type of account—**User**, **Group**, or **Computer**—to search for, type all or part of the account name, then click **Find Now**.
6. Select one or more accounts from the list of results, then click **OK**.
7. Repeat Step 4 through Step 6 until you are finished adding users and groups to which you want to assign the same administrative tasks, then click **Next**.
8. Select the tasks you want to delegate to the user or group, then click **Next**.

For example, if you want all of the members of the group you selected in the previous steps to be able perform all administrative tasks for a zone, select **All**.

9. Review your delegation settings, then click **Finish** to close the wizard.

Granting the authority to perform all administrative tasks

Only the administrator who creates a zone has full control over the zone's properties and only that administrator can delegate administrative tasks to other users. For each zone you create, you should identify at least one user or group that can be delegated to perform all administrative tasks. For example, if you have a Finance zone, you may want to create a Finance Admins group in Active Directory and then delegate **All** tasks to that group so that members of that group can manage the zone.

Although you are not required to create or use a zone administrator group for every zone, assigning the management of each zone to a specific user or group simplifies the delegation of administrative tasks.

If members of the designated administrative group must be able to create parent or child zones, they should be assigned the rights described in [Creating a new parent zone](#) and [Creating child zones](#).

Restricting authority to specific administrative tasks

You can use the Zone Delegation Wizard to set up fine-grain control over the specific administrative tasks different sets of users or groups can perform. For example, you can choose to grant the Join Operators group permission to join



computers to the zone and no other tasks. You can then specify another group is only allowed add and remove users. If you choose to use fine-grain control over specific administrative tasks, you should ensure the members of those groups know their restricted authority.

Note: If you delegate administrative tasks to one or more groups that have members logged on, you should inform the group members that they should log out and log back on so that they can perform the administrative tasks assigned to the group.

Adding Windows computers to a zone

To use identity and privilege management features, a Windows computer must have the Centrify agent for Windows installed, be joined to an Active Directory domain, and joined to a Centrify zone. Depending on your organization's policies, you can either allow any authenticated user with a valid domain account to join a zone or require a domain administrator account to join a zone.

If you want to have individual users deploy the Centrify agent for Windows on their own computers and join a zone without administrative rights, you can prepare the zone in advance and let users know which zone to join. If only domain administrators are allowed to join computers to zones, you should log on to computers with the Centrify agent for Windows installed using an account that has appropriate administrative rights and provide a password.

Preparing Windows computer accounts

If joining a zone is restricted to privileged users, you may want to prepare a computer account in the zone before joining. By preparing the computer account before joining, users can add their computers to the zone without any special rights or permissions in Active Directory.

To prepare a Windows computer account using Access Manager:

- Open Access Manager.
- Expand **Zones** to display the list of zones, then expand the parent and child zone hierarchy until you see the specific zone to which you want to add the computer account.
- Right-click, then click **Prepare Windows Computer**.



- Click **Find Now** to search for and select the computer account to add to the selected zone.
- Click **OK** to add the computer account to the Access Manager console in the zone's Computers container.

Changing the zone for the computer

You can move computer accounts from one zone to another at any time, if needed. Users who have administrative privileges can change the current zone on their local computer using the agent configuration panel. You can also change the zone information for a computer from Access Manager by changing its Active Directory properties or by dragging and dropping the computer from its current to a new zone.

To change the zone for a computer using Access Manager and Active Directory properties:

1. Open Access Manager.
2. Expand **Zones** to display the list of zones, then expand the zone hierarchy until you see the specific zone you want to modify.
3. Expand **Computers** to display the list of computers in the zone.
4. Select the computer that you want to modify, then right-click and select **AD Properties**.
5. Click the **Centrify Windows Profile** tab.
6. Click **Browse** and type all or part of the zone name, then click **Find Now**.
7. Select the new zone for the computer from the list of results, then click **OK**.
8. If the computer has role assignments defined, Access Manager prevents you from moving the computer until you remove the role assignments.

Leaving a zone

You can remove a computer from a zone at any time. Users who have administrative privileges can leave the current zone on their local computer using the agent configuration panel. You can also remove the zone information for a computer from Access Manager by deleting the computer from its current



zone. Leaving the zone does not remove the computer object from Active Directory.

To remove a computer from a zone using Access Manager:

- Open Access Manager.
- Expand **Zones** to display the list of zones, then expand the zone hierarchy until you see the specific zone you want to modify.
- Expand **Computers** to display the list of computers in the zone.
- Select the computer that you want to remove from the zone, right-click, then select **Delete**.
- Click **Yes** to confirm the removal of the computer from the zone.

Renaming a zone

You can rename a zone at any time. For example, if your organization changes how business units are aligned, moves to a new location, or merges with another organization, you might want to update zone names and descriptions to reflect these changes. You might also want to rename zones if your initial deployment did not use a naming convention for new zones, and you want to implement one after you have agents deployed.

What to do before renaming a zone

Before you rename zones, you might want to define and document a naming convention to use for future zones or the reasons for changing the zone name. You should also identify the computers in the zone to be renamed. You do not need to restart the agent on Windows computers for the new zone name to be recognized. However, you might need to perform other administrative tasks—such as changing role assignments—after renaming a zone. There are no other prerequisites for performing this task.

Rights required for this task

To rename a zone, your user account must be set with the following permissions:



| Select this target object | To apply these permissions |
|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Parent container for an individual zone For example, a <code>ZoneName</code> container object, such as: <code>domain /Zones/arcade</code> | Click the Properties tab and select Allow to apply the following properties to this object only: <ul style="list-style-type: none">Write DescriptionWrite nameWrite Name These are the minimum permissions required to rename a zone and not allow a user or group to modify any other zone properties. You can set permissions manually, or automatically grant these and other permissions to specific users or groups by selecting the Change zone properties task in the Zone Delegation Wizard. |

Who should perform this task

A Windows administrator performs this task, depending on your organization's policies. The user who creates the zone is responsible for delegating administrative tasks to other users or groups, if necessary. In most organizations, this task is done using an account with domain administrator privileges.

How often you should perform this task

After you are deployed, you rename zones only when you need to address organizational changes or to implement or improve the naming conventions you use.

Steps for completing this task

The following instructions illustrate how to rename a zone using Access Manager.

To rename a zone using Access Manager:

1. Open Access Manager.
2. Expand **Zones** to display the list of zones, then expand any child zones in the zone hierarchy until you see the specific zone you want to modify.



3. Select the zone to change, right-click, then click **Rename**.
4. Type the new name and, if needed, any changes to the zone description.
You do not have to restart any Centrify agents on the computers in the zone you have renamed. Computers will remain joined to the zone even after changing the zone name.
5. Users who have administrative privileges can verify the updated zone name on their local computer using the agent configuration panel.

Working directly with managed computers

When you deploy a Centrify agent on a computer, that computer has tools installed locally to allow you to manage access, troubleshoot agent operations, and view information about roles and role assignments, and auditing status.

Depending on the rights associated with the role you are using, you can use the tools on the managed computer to open new desktops, run individual applications with elevated privileges, connect to services on remote computers, join or change the zone for a computer, set the level of detail to record in log files, generate diagnostic information for the agent, and view detailed information about your own or other users' effective rights and roles.

Using the agent configuration

The Centrify agent for Windows provides an agent configuration panel from which you can configure agent settings for the Privileged Access Service, Centrify Privilege Elevation Service, and Centrify Audit & Monitoring Service. If you have the appropriate privileges, you can use the agent configuration panel to select the zone for a computer to join, change the current zone, or remove a computer from a zone.

To use the agent configuration panel to select the zone for a local computer:

1. Log on to a computer where the Centrify agent is deployed.
2. From the Windows Start menu, select **Agent Configuration**.
3. Click **Centrify Privilege Elevation Service**.
4. Click **Settings**.
5. On the General tab, click **Change**.



6. Click **Browse**, type all or part of the zone name, and click **Find Now** to search for the zone.
7. Select the new zone in the search results, click **OK**, then click **OK** to return General tab.
8. Click **Close** to return to the agent configuration panel.

You can also use the agent configuration panel to set logging level, view logs, and get diagnostic information about agent operations. For more information about using the agent configuration panel to configure logging and get diagnostic information, see [Troubleshooting and common questions](#).

If you allow users to join their own computers to a zone, you should notify them of the zone to use and see that they have access to the User's Guide for Windows.



Managing access rights and roles

This chapter describes how to establish role-based access controls for the computers that have the Centrify Agent for Windows installed and identity and privilege management features enabled.

The following topics are covered:

| | |
|-----------------------------------------------------------------------|-----|
| Basics of authorization and access rights | 134 |
| Adding predefined rights to a zone | 137 |
| Defining desktop access rights | 140 |
| Defining application rights | 142 |
| Defining network access rights | 159 |
| Defining custom roles with specific rights | 161 |
| Assigning users and groups to a role | 168 |
| Making rights and roles available in other zones | 169 |
| Viewing rights and roles | 171 |
| Scenario: Using a network access role to edit group policies | 173 |
| Scenario: Using multiple roles for network resources | 174 |
| Defining rights for Windows applications that encrypt passwords | 175 |
| Enabling access across multi-tiered application layers | 176 |
| Requiring users to justify privilege elevation | 177 |
| Working with computer roles | 178 |
| Assigning roles on multiple computers at once | 183 |



| | |
|--------------------------------------------------------------------------------------------------|-----|
| Using the Authorization Center directly on managed computers | 185 |
| Working with the authorization cache on managed computers | 186 |
| Configuring PowerShell Remote Access | 190 |
| Authentication service enforcement | 191 |
| Configuring MFA with RADIUS for Centrify Privilege Elevation Service for Windows checklist | 191 |
| Adding remote users automatically | 197 |
| Enabling users to run applications with alternate accounts | 197 |

Basics of authorization and access rights

You can use Access Manager to centrally manage what users can do on computers that have the Centrify Agent for Windows installed. For example, you can control who can log on or connect remotely for each computer in a zone through the assignment of roles. As discussed in [Managing access rights and roles using zones](#), a **right** represents a specific operation that a user is allowed to perform.

System rights allow users to log on

For Windows computers, the most basic rights are the system rights that determine whether a user can log on locally, log on remotely, or both. The rights that grant users local and remote access are defined by default in the Windows Login role so that you can grant users access simply by assigning the Windows Login role and without defining any custom roles or any additional access rights. You can enable or disable these system rights in any custom role definition, but you cannot add, modify, or delete them.

In most cases, you can assign the Windows Login role to all local Windows users, all Active Directory users, or both, to allow users to log on locally or remotely. However, the system rights in the Windows Login role do not override any native Windows security policies. For example, most domain users are not allowed to log on locally on domain controllers. Depending on how your organization has configured native Windows security policies, users might need to be members of a specific Windows security group, such as



Server Operators or Remote Desktop Users, to log on to specific computers locally or remotely.

If you would like to require multi-factor authentication for users or groups that use Centrify-managed Windows computers, you must assign them the **require MFA for login** role in addition to the Windows Login role as there is no system right to enable multi-factor authentication within the Windows Login role.

If you enable multi-factor authentication, users will be required to type their password and provide a second form of authentication before being able to log on. For example, you can configure an authentication profile that requires users to answer a phone call, click a link in an email message, respond to a text message, provide a one-time-password (OTP) token, or answer a security question. Before defining this system right, however, you should be aware that multi-factor authentication for Centrify-managed Windows computers relies on the infrastructure provided by the Privileged Access Service.

For more information about preparing to use multi-factor authentication, see the Multi-factor Authentication Quick Start Guide.

In addition to the system rights that specify whether a user can log on locally or remotely, you can use the **Rescue rights** setting to specify that users in a particular role should always be allowed to log on to a computer. This option is intended as a “safety net” for “emergency” situations when users would normally be locked out. For example, if auditing is required for a role, but the agent is not running or has been removed, users are not allowed to log on. You can use the rescue rights option to allow selected administrative users access to computers when they would otherwise be locked out and prevented from logging on. Because this option allows unaudited activity, you should strictly limit its use.

Note: If you do not explicitly set the Rescue rights option for any users, only the local administrator and the domain administrator accounts will have rescue rights. Those accounts are always allowed to log on by default.

Windows-specific rights can grant users privileged access

In general, you use the default Windows Login role for most users during the initial deployment to prevent disruptions in user access. You can then define custom roles to add specialized access rights to grant users additional privileges in a controlled manner.

For Windows computers, these specialized access rights are:



- **Desktop** access rights enable users to create additional working environments and run applications in that desktop with their own credentials but as a member of an Active Directory or built-in group. Users who are assigned to a role with desktop rights can switch from their default desktop to a desktop with administrator privileges without having to enter an Administrator password. With a desktop right, users can also run any application from their default desktop using a selected role and credentials without opening a new desktop.
- **Application** access rights enable users to run specific local applications as another user or as a member of an Active Directory or built-in group. Users who are assigned to a role with application rights can log on with their normal Active Directory credentials and run a specific application using a role with elevated privileges without having to enter the service account or Administrator password.
- **Network** access rights enable users 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. Users who are assigned to a role with network access rights can perform administrative operations on a remote server using a role with elevated privileges that only applies to the operations performed on the network computer without having to enter the service account or Administrator password. You can use zones to control who can connect and perform tasks on remote computers and what their elevated privileges allow them to do.

Combining rights into roles and role assignments

You can combine the system rights and specialized Windows rights into **role definitions** that reflect the needs of a specific job function, such as database administrator or web services administrator, or a particular task, such as troubleshooting application failures. You can then assign those roles to specific users and groups.

You can configure rights, role definitions, and role assignments in any parent or child zone. In most cases, you define rights and roles in a parent zone and make role assignments in a child zone.

Roles can be assigned to individual Active Directory users or to Active Directory groups. Therefore, you can manage how roles are applied to users completely through Active Directory group membership.



The rights from multiple role assignments accumulate, which provides great flexibility and granularity in how you define and assign rights and roles. For example, you can use the Windows Login role to control console and remote access, and define a second role with desktop access rights so that a user assigned to both roles could log in and create another desktop for accessing applications with administrative privileges. By separating login and desktop access rights into separate roles, not every user who is allowed to log on can create a desktop with administrative privileges.

Deciding where to define and assign roles

Because access rights are additive, it is important to consider where you define and assign roles to control who has administrative privileges on which computers. For example, it might seem reasonable to assign the predefined Windows Login role to all Active Directory users. Doing so, however, could grant broad permission to log on locally or remotely on computers to which you want to restrict access. If you assign that role in a parent zone, it is inherited along with any additional rights granted in child zones.

In most cases, it is appropriate to define roles in parent zones, but assign roles carefully in child zones to avoid granting access rights on computers that host administrative applications or sensitive information.

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 users 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 the predefined rights in the context of a role definition.



To create predefined rights in a zone:

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone where you want to define a predefined right.
3. Expand **Authorization > Role Definitions**.
4. Select a role definition, right-click, then select **Add Right**.
5. Select a type of right if you want to filter the list of rights displayed.
For example, select Any Windows Rights or Any Windows Applications to list only Windows-specific rights.
6. Click **Create Predefined Rights**.
7. Select the specific predefined rights you want created in the zone you selected in Step 2 from the list of available rights, then click **OK**.
By default, all of the selected predefined rights are added to the role definition in the zone. You can deselect any of the rights you don't want added to the role definition.
8. If you have selected at least one of the predefined rights as applicable for the role definition, click **OK**.
If none of the predefined rights is applicable for the role definition, you can click **Cancel** to add the rights to the zone without adding them to the role definition.

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

Enabling multi-factor authentication for Windows rights

In addition to the **require MFA for login** role, which requires users to provide both their password and a second form of authentication to log on to a Centrify-managed Windows computer, you can enable multi-factor authentication for a predefined right. When you define a desktop, application, or network access right, you can choose to enable multi-factor authentication for that right. For example, if you want to require multi-factor authentication before a user can open a privileged desktop, you would issue that user a role with a predefined desktop right that has multi-factor authentication enabled.



To enable multi-factor authentication for a right definition:

1. Right-click the predefined right after adding it to a role definition.
2. Select **Properties**.
3. Click the **Run As** tab and select **Re-authenticate current user** and **Require multi-factor authentication**.

Note: Before defining this right, you should be aware that multi-factor authentication for Centrify-managed Windows computers relies on the infrastructure provided by the Privileged Access Service.

4. Click **OK**.

Using multi-factor authentication when there are selective cross-forest trusts

If you have domains in different forests that have a two-way selective trust relationship, any computer or user accounts that are used to log on to the remote forest must be granted the “Allowed to authenticate” right on the domain controllers in both forests to get role information.

In addition to granting the “Allowed to authenticate” right to users and to computers with the Centrify agent for Windows installed, the right must also be granted to computers that host your Centrify connectors.

After you grant these computers and users the “Allowed to authenticate” right for the domains in both forests, users that are assigned a role with a multi-factor authentication right for privilege elevation will be able to authenticate using any of the authentication mechanisms that you have assigned to them.

If a connector is not allowed to authenticate on the remote domain controller, some multi-factor authentication mechanisms may fail to authenticate users.

For more information about preparing to use multi-factor authentication, see the Multi-factor Authentication Quick Start Guide.



Defining desktop access rights

When users log on with their normal Active Directory credentials, Windows brings up the **default desktop** for the user logging on. You can define desktop rights to enable users to create additional working environments—new desktops—that run using their own credentials but with the privileges of an Active Directory or built-in group.

Users who are assigned to a role with desktop rights can switch from their default desktop to a desktop with elevated privileges to perform administrative tasks. For example, if assigned to a role that has a desktop right, a user can create a new desktop and switch to it when he needs perform administrative tasks such as install new software or stop running services on the local computer account. The user can perform these tasks without having to enter the service account or Administrator password.

Users who are assigned a role with desktop rights can also select any application on the computer, right-click, and run the application using a selected role. The difference between the desktop right and an application right is that the desktop right allows the user to run any applications using the privileged account defined in the desktop right. An application right restricts access to a specific application using the privileged account explicitly defined for that application.

Desktop rights are useful for users who frequently perform tasks that require the privileges associated with the Administrator account.

To define a desktop right:

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone where you want to define a desktop right.
3. Expand **Authorization > Windows Right Definitions**.
4. Select **Desktops**, right-click, then click **New Windows Desktop**.



5. On the General tab, type a name and a description for the desktop right.

| For this | Do this |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name you want to use for this desktop right. For example, if the desktop allows a user to create a desktop using the privileges associated with a service account, you might include the security group in the name. |
| Description | Type a description for this desktop right. The description is optional. You can use it to provide a more detailed explanation of the privileges associated with the desktop. |
| Priority | Set the priority for this desktop right. |

6. Click the **Run As** tab.

You can browse for and select a specific group that will allow you to log on with your own credentials but with the elevated privileges of the specified group.

Click **Add AD Groups** or **Add Built-in Groups** to search for and select a previously-defined or built-in group with the privileges you want to add to the logged in user's account.

Select **No re-authentication required** to allow users to use the desktop right without any additional authentication.

Select **Re-authenticate current user** if you want to prevent the desktop right and its privileges from being used by anyone not authorized to do so. Selecting this option also allows you to enable multi-factor authentication for the right. For more information, see [Enabling multi-factor authentication for Windows rights](#).

If you select the Re-authenticate current user option, users are prompted to re-enter their password to verify their identity before they are allowed to create a new desktop or switch between desktops. Forcing users to re-authenticate ensures the privileges associated with the desktop are only granted to users who have been assigned those privileges.

If you select this Re-authenticate current user option for users who are authenticated using a smart card, users must enter a personal identification number (PIN) or a password to resume working with the desktop.

7. Click **OK** to save the desktop right.



Where desktop rights apply

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 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.

Defining application rights

Application rights allow users to run specific applications using either another user account or using their own credentials but with the privileges of an Active Directory or built-in group.

When you create an application right, you specify one or more application executable files to which you want to control access. 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 example, the executable file for SQL Server Management Studio resides in different locations in Windows 2005, Windows 2008, and Windows 2012. By specifying all instances of the executable file in one application right, you can use that application right to control access to SQL Server Management Studio on computers running any of those operating systems.

You can also use Centrify application utilities to allow access to common administrative tasks such as software installation, network, and Windows feature management. For more information on using these utilities, see [Using Centrify application utility rights](#)

Note: Although it is possible to define different applications (for example, SQL Server Management Studio and Internet Explorer) in one application right, this is not a recommended practice.



Instead, it is recommended that you create separate application rights for different applications.

How to specify which applications are in an application right

You can specify which application executable files are in an application right in these ways:

- You can specify the path and file name of an application executable file. You can perform this operation in two ways:
 - Manually, by typing or pasting the path and file name into an application right definition form. Specifying files manually is recommended only if you need to include a small number of files in the definition—typically just one or two. See [Defining an application right manually](#) for more information.
 - By navigating to the executable file or a running process that was launched by the executable file. After locating the executable file, you can import the path and file name into the application right definition form. See [Using an installed application or running process to create application rights](#) for more information.
- You can specify search criteria for application executable files, and then include all application executable files that match those criteria in the application right. You can perform this operation in two ways:
 - Manually, by typing or pasting values into search criteria fields. See [Defining an application right manually](#) for more information.
 - By importing values into search criteria fields from an executable file or from a running process that was launched by the executable file. See [Using an installed application or running process to create application rights](#) for more information.

See [Examples of application right definitions](#) for examples of defining application rights in all of these ways.

Defining an application right manually

This section describes how to create an application right by manually typing or pasting information into several application right definition forms.



Note: Alternatively, you can import information into application right definition forms from an executable file or from a running process that was launched by the executable file. See [Using an installed application or running process to create application rights](#) for more information.

To define an application right manually:

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone where you want to define an application right.
3. Expand **Authorization > Windows Right Definitions**.
4. Select **Applications**, right-click, then click **New Windows Application**.
5. On the General tab, type a name and a description for the application right, and specify a priority for the application right.

| For this | Do this |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name you want to use for this application right. For example, if the right allows a user to run SQL Server Configuration Manager using the privileges associated with a security group, you might include the service account in the name. For example, you might use a name like SQL Config Manager. |
| Description | Type a description for this application right. The description is optional. You can use it to provide a more detailed explanation of the privileges associated with running the application. |
| | Set the priority for this application right. If more than one application right is added to the same role definition, the priority value determines the application right to use when users assigned to that role open that application. The lower the value, the higher the priority. For example, a right with the priority of 1 takes precedence over a priority value of 2. If the application rights have the same priority value, the application right listed first under the role definition is used. |

6. Click the **Match Criteria** tab and use it to create or edit application definitions. Each application definition specifies one application or a group of applications. The set of application definitions displayed in the **Match Criteria** tab defines the set of applications that can be run by this application right.

In the **Match Criteria** tab, click **Add** to create a new application definition.



The Definition Settings dialog appears.

7. In the upper portion of the Definition Settings dialog, provide this information about the application definition.

| For this | Do this |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | <p>Type a description for this application definition.</p> <p>For example, if the definition specifies one executable file (such as SQL Server Management Studio for Windows 2005), you might type Windows 2005 SQL Server Management Studio here. Or, if the definition specifies more general criteria so that multiple executable files (such as SQL Server Management Studio for all versions of Window) can run, you might type a more general description such as SQL Server Management Studio.</p> |
| File Type | <p>Select the type of executable file for this definition. If you are constructing the definition so that it specifies multiple executable files, all files must all be of the type that you specify here. Supported file types are:</p> <ul style="list-style-type: none">■ .bat■ .cmd■ .com■ .cpl■ .exe■ .msc■ .msi■ .msp■ .ps1■ .vbs■ .wsf |

8. To specify executable files in this definition by typing or pasting the file name and location, select the **Path** option. Go to Step 9 and continue from there.

Specifying files in this way is recommended only if you need to include a small number of files in the definition—typically just one or two.

To specify a larger number of executable files in this definition, it is recommended that you select file parameters that are common to the set of files. Files that match the parameters are then included in the definition. To do this, go to Step 10 and continue from there.

9. Perform this step to specify a small number of executable files in this definition. In this step, you type or paste information about the executable



file name, location(s), and arguments. When you are done with this step, go to Step 11 and continue from there.

| For this | Do this |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name of the application executable file. If this field is defined, you must also select a path option (standard system path or a specified path). For example, to specify the SQL Server Management Studio executable, type SSMS . exe . |
| Standard system path | Select Standard system path to use the directories where the user would normally find the application specified. For example, to use the application executable in its default directory, select Standard system path . |



| For this | Do this |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Specify path | <p>Select Specify path if you want to define the location of the application specified. If you select this option, you can specify one or more paths, separated by a semicolon (;).</p> <p>Supported path variables are %systemroot%, %system32%, %syswow64%, %program files%, %winagentinstall%, and %program files(x86)% (note that a space between “program” and “files” is required).</p> <p>For example, to specify the location of the SQL Server Management Studio executable file in Windows 2008, type C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\SShell\Common7\IDE.</p> |
| Arguments | <p>If you selected a file type of .MSC in Step 7, the Arguments option is required. The Arguments option is optional for all other file types.</p> <p>Select the Arguments option and leave the argument field blank to specify that the application cannot accept any arguments.</p> <p>To specify that the application can run using any argument, leave the Arguments option deselected. For example, if you specified the SQL Server Management Studio executable and left the Arguments option deselected, users can run SQL Server Management Studio with any option on a local computer with elevated privileges.</p> <p>If you want to restrict the arguments allowed, in the argument field type the list of arguments to allow. Valid arguments must be enclosed by quotation marks and separated by a space. For example, to allow users to run the specified application using argument1, argument2, or argument3, you would specify the list of arguments like this:</p> <p>“argument1” “argument2” “argument3”</p> <p>By default, arguments that you specify do not need to be a case-sensitive match, but do need to be an exact match (that is, a match is returned if the actual argument is a partial match of the argument string that you specify). If arguments must be a case-sensitive match for a particular application, select the Keep arguments case sensitive option. If arguments can be a partial match for a particular application, deselect the Match whole string only option.</p> |

10. Perform this step to specify a larger number of executable files in this definition. In this step, you use the **File details** area to specify characteristics that are used to search for applications to include in this definition. All of the characteristics that you specify must be met in order for an application to be a match. For example, if you specify a product name of Microsoft SQL Server and a company name of Microsoft Corporation, all executable files that meet both of those criteria are included in this definition.



Note: This step describes how to manually fill in each field in the **File details** area. You can select any combination of these fields to specify the file characteristics for which to search. Alternatively, you can populate fields in the Definition Settings dialog by importing values from an installed executable file or from a running process. Filling in fields by importing is faster and more accurate than filling in fields manually one at a time. For details about filling in fields by importing, see [Using an installed application or running process to create application rights](#).

| For this | Do this |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product Name | Select an operator (i s or contains) from the drop-down list and in the provided field type the product name for which to search. If you select i s , matches are returned for product names that exactly match the string that you type here. If you select contains , matches are returned for product names that contain the string that you type here anywhere in the product name. |
| Company | Select an operator (i s or contains) from the drop-down list and in the provided field type a company name for which to search. |
| File Description | Select an operator (i s or contains) from the drop-down list and in the provided field type a file description for which to search. |
| Volume Serial # | Select an operator (i s , contains , starts with , or ends with) from the drop-down list and in the provided field type a serial number for which to search. The supported format is 8-character hex string (FFFFFFFF). This criterion is matched only if the executable file was from CD/DVD media. |
| Publisher | Select an operator (i s , contains , starts with , or ends with) from the drop-down list and in the provided field type publisher information for which to search. For example, publisher information could look similar to: CN=Centrify Corporation, OU=Digital ID Class 3 - Microsoft Software Validation v2, O=Centrify Corporation, L=Sunnyvale |
| Product Version | Select an operator (equal , earlier or equal , or later or equal) from the drop-down list and in the provided field type product version information for which to search. For example, the product version could look similar to: 3.1 |



| For this | Do this |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File Version | <p>Select an operator (equal, earlier or equal, or later or equal) from the drop-down list and in the provided field type file version information for which to search.</p> <p>For example, the file version could look similar to:</p> <p>3.1.2</p> |
| File Hash | <p>Select this option to match applications using the encrypted file hash for the application. The file hash for the application is generated using the SHA-1 encryption algorithm, which is FIPS-compliant.</p> <p>You can click Import Process or Import File and select an application to populate the File Hash field for which to search. Only applications with a hash string that is exactly the same as the string generated by the MD5 algorithm are matched.</p> <p>You can only use file hash matching to identify an application for files that are less than 500MB to limit the CPU and memory used to calculate the file hash. If the file with matching hash information is larger than 500MB, an empty value is returned for the file hash field.</p> |
| Owner | <p>In the provided field, type owner information for which to search. Matches are returned for owner information that exactly matches the string that you type here.</p> <p>Owner information can be:</p> <ul style="list-style-type: none">■ AD user/group/builtin (SID)■ local user (user name)■ local group (group name) <p>For example, the owner could look similar to:</p> <ul style="list-style-type: none">■ NT AUTHORITY\SYSTEM■ DEMO\Ed.Admin (this is an AD user account)■ Amy Adams (this is a local user account) |

11. Optionally select the **Application requires administrative user** option to specify that applications in this definition run only if `RequestedExecutionLevel` is set to `requireAdministrator` in the application manifest. If you select this option, the applications in this definition run only for administrators and require that the applications be launched with the full access token of an administrator. This option applies only to .exe files.
12. Click **OK** to save the definition. You are returned to the **Match Criteria** tab, and the new or modified definition appears in the **Match Criteria** list of definitions.



13. Click the **Run As** tab and select the account that has the privileges you want to enable for this application right.

You can browse for and select a specific user account or have the application run using the logged in user's account credentials but with the elevated privileges of a specified group. Click **Add AD Groups** or **Add Built-in Groups** to search for and select a previously-defined or Built-in group with the privileges you want to add to the logged in user's account.

In most cases, you select a specific user account only if the application should run as a service account. However, some applications require a specific privileged user account to be used. For example, Microsoft System Center Operations Manager (SCOM) and Exchange require a user account. If you are defining an application right for an application that requires a privileged user account rather than membership in a privileged group, you should create a service account and use that account for the run-as account.

Select **Re-authenticate current user** if you want to prevent the application right and its privileges from being used by anyone not authorized to do so. Selecting this option also allows you to enable multi-factor authentication for the right. For more information see [Enabling multi-factor authentication for Windows rights](#).

If you select this option, users are prompted to re-enter their password to verify their identity before they are allowed to select a role for running a local application. Forcing users to re-authenticate ensures the privileges associated with the application right are only granted to users who have been assigned those privileges.

If you select this option for users who are authenticated using a smart card, users must enter a personal identification number (PIN) or a password to resume working with the application.

14. Click **OK** to save the application right.

Using Centrify application utility rights

This section describes how you can manage user access to Windows programs and features using Centrify application utility rights.

There are many common administrative tasks such as managing software installations, changing network settings, and adding or removing Windows features that require access to the `explorer.exe` application on Windows



systems. Because granting users privileged access to `explorer.exe` can allow the user to perform many other tasks that you may want to remain restricted, you can use the Centrify application utilities, **Application Manager**, **Network Manager** and **Windows Feature Manager**, to grant access to these tasks using the corresponding predefined rights.

When you create a new zone, the Centrify utility rights are automatically added to the list of Windows Right Definitions. However, in zones that existed before the addition of these utility rights, you may need to add them by following the procedure below.

To add the Centrify Utilities to the list of Windows Right Definitions

1. Right click **Windows Right Definitions** and select **Add predefined rights**.

Windows Right Definitions can be found in the following location:

The application rights can be found in the following location:

Access Manager > Zones > Zone Name > Authorization > Windows Right Definitions

2. Select the rights you would like to add and click **OK**.

The rights will now appear under **Applications**.

It is important to note that if you do not install the Centrify agent for Windows in the default location during the installation or upgrade process, users who are assigned these rights may not be able to access the corresponding applications. If you have installed the agent in a location other than the default location, you can specify a variable in the application right settings to allow them to be used by assigned users by doing the following:

To specify the application right path

1. Right click on the application right and select **Properties**.

The application rights can be found in the following location:

Access Manager > Zones > Zone Name > Authorization > Windows Right Definitions > Applications.

2. Click the **Match Criteria tab**, and then click **Edit**.
3. Check the **Path** box in the **Commands components** section, and select **Specific path**.
4. In the **Specific path** field, enter the following variable:

`%winagentinstall%`



Do this for each of the Centrify Utility application rights.

Application Manager

Application Manager is a Centrify utility that allows a user to manage installed software. Application Manager is similar to the Windows utility Programs and Features. It can allow users who are assigned a role with the **Centrify Utility - Application Manager** right to Refresh, Uninstall, Change, or Repair installed software.

Windows Feature Manager

When you assign workstation users a role with the predefined right **Centrify Utility - Windows Feature Manager**, they will be able to access the normal Windows Feature Manager, where they can choose what Windows features to add or remove.

When you assign server users a role with this right, the Centrify Windows Feature Manager will launch. This utility is similar to the normal Windows utility, with a few notable differences.

Opening the Centrify utility will launch a wizard. When you select whether to add or remove roles and features on the first screen of the wizard, you can only perform one action at a time. For example, if you choose **Add roles and features**, you will not be able to remove any installed features until you go back to the initial screen and choose **Remove roles and features**.

Additionally, when you attempt to install features that require the installation of dependent components, you will be prompted to add those features. All features with one or more components installed will appear with a check mark next to the name.

Network Manager

When you assign users a role with the predefined right Centrify Utility - Network Manager, they will be able to access the Centrify version of Network Manager that is similar to the Windows version.

Users assigned a role with this right can view a list of network adapters for Ethernet and wireless connections and configure their IP and DNS settings.



Using an installed application or running process to create application rights

This section describes how to create an application right by importing values from an installed executable file or from a running process. After values are imported into the application right definition form, you can select which fields to use as search criteria for matching applications. Applications that match the search criteria are included in the application definition.

For more information about filling in fields by importing, see [Examples of application right definitions](#).

To define an application right based on an installed application:

1. Follow the procedure for creating a new application right manually to the point where the Definition Settings dialog opens (see [Defining an application right manually](#)).
2. In the Definition Settings dialog, click **Import File**.
3. Navigate to an application executable file, highlight the file, and click **Open**.

Fields in the Definition Settings dialog fill in with all of the information that is available for the file that you selected. For example, if you navigated to `C:\Program Files\Centrify\Access Manage` and selected the `Mmc_config.exe` file, the Definition Settings dialog would look similar to this:



Definition Settings

Description:

File Type:

Command components

Path
Name:
 Standard system path
 Specific path:

Arguments
 Keep arguments case sensitive
 Require to match whole string

File details

Product Name: Product Version:

Company: File Version:

File Description: File Hash:

Volume Serial #:

Publisher: Owner:

Application requires administrative user

Notice that:

- The **File Type** field is set to `.exe`.
- The **Path** option is selected, and the file name and path name are filled in.
- Most fields in the **File details** section are filled in, but none are selected.

The settings shown in this example specify that only the `Mmc_config.exe` file located in `C:\Program Files\Centrify\Access Manage` is included in the application right. The information in the **File details** section is not used because no options in that section have been selected.

4. Choose whether to expand the definition to include other executable files, or to save the definition as it is currently defined (so that it specifies only the `Mmc_config.exe` file shown here).

To expand the definition to include other executable files, go to Step 5 and continue from there.

To save the definition as it is currently defined:



- In the **Description** field, type a description for this application definition. This is the string that displays in the list of application definitions on the **Match Criteria** tab.
 - Click **OK**.
 - Continue to define the application right as described in [Defining an application right manually](#).
5. To expand the definition to include other executable files, use the **File details** area to specify characteristics that are used to search for executable files. All of the characteristics that you specify must be met in order for an executable file to be a match. See [Defining an application right manually](#) for details about operators and syntax for each option in the **File details** area.
- Deselect the **Path** option.

This step is necessary because all of the search options that you select use the AND operator when the search executes. If you leave the **Path** option selected, the search is constrained to this location and the definition will include only the file that is specified in the **Name** field.
 - In the **File details** area, select options to define search criteria for executable files.

Selecting criteria that are more general will usually result in a greater number of executable files being included in the definition. In the example shown in Step 3, you would select only the **Company** option if you wanted to allow this definition to run all .exe files having a company name tag of `Centrify Corporation`. Select additional options to limit the scope of the search so that fewer executable files are included in the definition.
 - In the **Description** field, type a description for this application definition. This is the string that displays in the list of application definitions on the **Match Criteria** tab.
 - Click **OK**.
 - Continue to define the application right as described in [Defining an application right manually](#). When you are done, the application right is available to use.



To define an application right based on a running process:

1. Follow the procedure for creating a new application right manually to the point where the Definition Settings dialog opens (see [Defining an application right manually](#)).

2. In the Definition Settings dialog, click **Import Process**.

A list of running processes displays. By default, the list does not include these processes:

Processes having an owner of SYSTEM, Local Service, or Network Service

- conhost.exe
- dllhost.exe
- dwm.exe
- explorer.exe
- svchost.exe
- taskhost.exe

To display these processes, select the **Show all processes** option.

Note: System Idle Process and processes having unsupported file extensions (for example, .scr) are never shown.

3. Highlight a process and click **OK**.

Fields in the Definition Settings dialog fill in with information from the executable file that launched the process that you selected.

4. Select executable files to include in this definition as described in Step 4 on page 149 through Step 5 on page 150. When you are done, the application right is available to use.

Examples of application right definitions

This section contains these examples of how to use the Definition Settings dialog to specify an application right definition:

- **Example 1: Manually specify one application path and file name**—
Describes how to define an application right to run the Access Manager console by manually entering the path name and application name.
- **Example 2: Manually specify one application residing in two locations**—
Describes how to define an application right to run SQL Server



Management Studio on Windows 2008 and Windows 2012 systems by manually entering the application name and the path names to the application on both systems.

- **Example 3: Specify one application by importing its location**—Describes how to define an application right to run the Access Manager console by navigating to the `Centrifdc.msc` file and importing its information.
- **Example 4: Specify several applications by importing and specifying search criteria**—Describes how to define an application right to run SQL Server Management Studio on several versions of the Windows operating system by navigating to the `ssms.exe` file on Windows 2008, importing its information, and constructing application search criteria based on that information.

Example 1: Manually specify one application path and file name

In this example, it is assumed that you want to create an application right to run the Access Manager console application, and you know the path and file name of the application executable file.

1. Open the Definition Settings dialog and fill it in as follows:

Description—Type a name of your choice (for example, **Default Access Manager Console Application**).

Path—Select this check box.

Name—Type the application name; in this case `Centrifdc.msc`.

Arguments—Select this check box and specify which arguments can be executed through this application right.

Specific path—Select this option and type the full path name to the `Centrifdc.msc` executable file:

`C:\Program Files\Centrif\Access Manager`

2. Click **OK** to save the application right definition setting.

Example 2: Manually specify one application residing in two locations

In this example, it is assumed that you want to create an application right to run SQL Server Management Studio on Windows 2008 and Windows 2012 systems. The SQL Server Management Studio executable file resides in different locations in those operating systems, and you know the paths those locations.



1. Open the Definition Settings dialog and fill it in as follows:

Description—Type a name of your choice (for example, **SQL Server Management Studio 2008/2012**).

Path—Select this check box.

Name—Type the application name; in this case `ssms.exe`.

Arguments—Optionally select this check box and specify which arguments can be executed through this application right.

Specific path—Select this option and type the full path names to the **Ssms.exe** executable file in Windows 2008 and Windows 2012.

Separate the path names with a semicolon:

```
C:\Program Files (x86)\Microsoft SQL  
Server\100\Tools\Binn\VSShell\Common7\IDE;C:\Program  
Files\Microsoft SQL Server\110\Tools\Binn\ManagementStudio
```

2. Click **OK** to save the application right definition setting.

Example 3: Specify one application by importing its location

This example is similar to Example 1; it is assumed that you want to create an application right to run the Access Manager console application. Unlike in Example 1, you are not sure of the path name to the application executable file and you will navigate to it rather than type it in the form.

1. Open the Definition Settings dialog.
2. Click **Import File**.
3. Navigate to the `Centri fydc.msc` executable file, highlight it, and click **Open**.
4. Verify that the Definition Settings dialog fills in with application information.
5. In the Description field, type a name of your choice (for example, Default Access Manager Console Application).
6. Click **OK** to save the application right definition setting.

Example 4: Specify several applications by importing and specifying search criteria

This example is similar to Example 2; it is assumed that you want to create an application right to run SQL Server Management Studio on more than one version of the Windows operating system, starting with Windows 2008. Unlike



in Example 2, you do not want to constrain the latest version of Windows to Windows 2012. Instead, you want to account for future versions of Windows and provide the capability to run SQL Server Management Studio on future Windows releases.

1. Open the Definition Settings dialog on a Windows 2008 system.
2. Click **Import File**.
3. Navigate to the `ssms.exe` executable file, highlight it, and click **Open**.
The Definition Settings dialog fills in with information from the Windows 2008 version of `ssms.exe`.
4. Deselect the **Path** option so that the definition is not constrained just to that location.
5. Select the **File Description** option and keep the default operator and string.
6. Select the **Product Version** option and change the operator from **equal** to **later or equal**.

The definition is now configured to include all `.exe` files having a file description tag of **SSMS - SQL Server Management Studio** and a product version later than or equal to the version that is installed on this Windows 2008 system.

7. In the Description field, either keep the string that was imported with the `ssms.exe` file or type a description of your choice.
8. Click **OK** to save the application right definition setting.

Defining network access rights

Network access rights allow users to access services on remote computers using another user account on the remote computer. Users who are assigned to a role with network access rights are only granted the elevated privileges when accessing the remote computer.

To define a network access right:

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone where you want to define an application right.



3. Expand **Authorization > Windows Right Definitions**.
4. Select **Network Access**, right-click, then click **New Network Access**.
5. On the General tab, type a name and a description for the network access right.

| For this | Do this |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name | Type the name you want to use for this network access right. For example, if the right allows a user to connect remotely to a Microsoft SQL Server instance using the privileges associated with a database system administrator account, you might include the SQL login name. For example, you might use a name like sysadmin. |
| Description | Type a description for this network access right. The description is optional. You can use it to provide a more detailed explanation of the privileges associated with this right. |
| Priority | Set the priority for this application right. If more than one network access right is included in the roles selected, the priority value determines which network access right to use. The lower the value, the higher the priority. For example, a right with the priority of 1 takes precedence over a priority value of 2. If users have multiple roles selected, the priority value of the network access right determines which network access right takes precedence over the access rights in other roles. For more information about selecting multiple roles for connecting to remote servers, see Scenario: Using multiple roles for network resources . |

6. Click the **Access** tab to select the account that has the privileges you want to enable for accessing the remote computer.

You can browse for and select a specific user account, create a new account, or access the remote computer using the logged-in user's account credentials but with the elevated privileges of a specified group account. Click **Add AD Groups** or **Add Built-in Groups** to search for and select a previously-defined or Built-in group with the privileges you want to add to the logged in user's account.

In most cases, you select a specific user account only if accessing the remote computer using a service account.

Select **Re-authenticate current user** if you want to prevent the network access right and its privileges from being used by anyone not authorized to do so. Selecting this option also allows you to enable multi-factor



authentication for the right. For more information see [Enabling multi-factor authentication for Windows rights](#).

If you select this option, users are prompted to re-enter their password to verify their identity before they are allowed to select a role for accessing applications on a remote computer. Forcing users to re-authenticate ensures the privileges associated with the network access right are only granted to users who have been assigned those privileges.

If you select this option for users who are authenticated using a smart card, users must enter a personal identification number (PIN) or a password to resume working with the remote server.

7. Click **OK** to save the network access right.

Using network access rights when there are two-way selective cross-forest trusts

If you have domains in different forests that have a selective two-way trust relationship, any computer or user accounts that are used to log on to the remote forest must be granted the “Allowed to authenticate” right on the domain controllers in both forests to get role information. After you grant the computer used to access the remote server the “Allowed to authenticate” right for the domains in both forests, you can select roles that grant network access rights from either forest.

If an account is not allowed to authenticate on the remote domain controller, you cannot view or select roles that would otherwise allow you to perform tasks on the remote server.

Defining custom roles with specific rights

Rights can be combined or used independently of each other to create role definitions. Role definitions describe job functions that require a specific set of rights, including the specific days and times the role should be available for performing the operations allowed. If you have created desktop, application, or network access rights, you must create at least one role definition to use these rights.

To create a new role definition for a job function, you need to do the following:



- Create a new role and specify when the role is available.
- Specify how users in the role are allowed to log on.
- Add specialized Windows access rights to the role, as applicable.
- Specify whether the role requires multi-factor authentication before it can be selected.

In most cases, creating a separate role definition for each access right gives you the most granular control over what users assigned to a role can do. For example, if you create separate role definitions for desktop, application, and network access rights, you can choose which apply to specific users and groups through role assignments.

Creating a role definition with desktop rights

Before you can make the desktop rights you have defined available to users or groups, you must create one or more role definitions that include those rights. Desktop rights are especially useful to include in roles for users who frequently perform tasks that require the privileges associated with the Administrator group.

To create a new role definition with desktop rights:

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone where you want to define a new role that includes a desktop right.
3. Expand the **Authorization** node.
4. Select **Role Definitions**, right-click, then click **Add Role**.
5. Type a role name and optional description for the role.
The description can include details about time restrictions for the role and whether the role is audited or not.
6. Select **Allow local accounts to be assigned to this role** if you want to be able to assign local users or groups to the role you are creating.
If you do not select this option, only Active Directory domain users can be assigned to the role.
7. Click **Available Times** and use the grid to specify when to allow or deny access for this role definition if you want to restrict when this role is



available.

8. Click the **System Rights** tab and select **Console login is allowed** to allow users in the role to log on locally.

To use the desktop right, the user must be able to log on locally on the computer. If you want to allow users to log on using a remote desktop connection, you can also select **Remote login is allowed**.

Note: Remote computers must be configured to allow remote desktop connections for the “Remote login is allowed” right to be valid. You can configure a computer to allow remote desktop connections by right-clicking Computer and selecting Properties or from the System Control Panel, then clicking **Remote settings**.

Users must be assigned to at least one role with either console login or remote login rights to access any computers where the Centrify Agent for Windows is installed. You can grant access using the Windows Login role definition or the system rights in any custom role definition.

The Windows right **PowerShell remote access is allowed** allows you to log on remotely to PowerShell.

If you want to allow users to log on even when the Windows agent isn't running or when audit and monitoring service is required but not available, you can select the rescue right. Because this right allows users to log on without having their activity audited, you should only assign roles with this right to trusted administrators or under controlled conditions. For example, assume you have a computer with sensitive information that normally requires all user activity to be audited. If that computer has application or operating system issues that require you to disable auditing temporarily, you can use a role with the rescue right to log on to that computer to diagnosis and fix the issue.

9. In the **Authentication** tab, you can add multi-factor authentication. If you want to require multi-factor authentication for users to access the role, select **Require multi-factor authentication for login**. You can also require multi-factor authentication for access to individual rights when you define the rights to add to roles. For more information see [Enabling multi-factor authentication for Windows rights](#).



10. Click the **Audit** tab and select an option.

If you select **Audit not requested/required**, users can log on to audited computers without having their session activity recorded. An audit trail event is recorded in the Windows event log when users open a desktop with this role, but the detailed record of what took place during the session is not captured.

If you select **Audit if possible**, session activity is recorded when users open a desktop with elevated privileges on audited computers and not recorded when they log on to computers where audit and monitoring service is not enabled or audited computers when auditing is not currently running.

If you select **Audit required**, users can only open a desktop with elevated privileges when auditing is running. If audit and monitoring service is not available or not currently running, the role is not available and users cannot use the elevated privileges.

11. Click **OK** to save the role definition.
12. Select the role definition, right-click, then click **Add Right** to add a desktop right to the role definition.
13. Select the desktop right from the list of rights from the current zone and from any parent zones, then click **OK** to add the right to the role definition.

Creating a role definition with application rights

Before you can make the application rights you have defined available to users or groups, you must create one or more role definitions that include those rights. Application rights are especially useful to include in roles for users who infrequently require access to specific applications with the privileges associated with the Administrator account or a service account on a local computer.

To create a new role definition with application rights:

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone where you want to define a new role that includes an application right.
3. Expand the **Authorization** node.
4. Select **Role Definitions**, right-click, then click **Add Role**.



5. Type a role name and optional description for the role.
The description can include details about time restrictions for the role and whether the role is audited or not.
6. Click **Available Times** and use the grid to specify when to allow or deny access for this role definition if you want to restrict when this role is available.

7. Click the **System Rights** tab and select **Console login is allowed** to allow users in the role to log on locally.

To use the Run as selected role utility and an application right, the user must be able to log on locally on the computer where the application runs. If you want to allow users to log on using a remote desktop connection, you can also select **Remote login is allowed**.

Users must be assigned to at least one role with either console login or remote login rights to access any computers where the Centrify Agent for Windows is installed. You can grant access using the Windows Login role definition or the system rights in any custom role definition.

If you want to require multi-factor authentication for users to access the role, select **Require multi-factor authentication**. You can also require multi-factor authentication for access to individual rights when you define the rights to add to roles. For more information see [Enabling multi-factor authentication for Windows rights](#).

8. Click the **Audit** tab and select an audit and monitoring service option.
 - If you select **Audit not requested/required**, users can log on to audited computers without having their session activity recorded. An audit trail event is recorded in the Windows event log when users select this role to run the application, but the detailed record of what took place during the session is not captured.
 - If you select **Audit if possible**, session activity is recorded when users select this role to run the application and not recorded when they use the application on computers where audit and monitoring service is not enabled or audited computers when audit and monitoring service is not currently running.
 - If you select **Audit required**, users can only select this role to run the application when audit and monitoring service is running. If audit and monitoring service is not available or not currently running, the role is not available and users cannot use their elevated privileges.
9. Click **OK** to save the role definition.



10. Select the role definition, right-click, then click **Add Right** to add the application right to the role definition.
11. Select the application right from the list of rights from the current zone and from any parent zones, then click **OK** to add the right to the role definition.

Creating a role definition for network access rights

Before you can make the network access rights you have defined available to users or groups, you must create one or more role definitions that include those rights. Network access rights are especially useful to include in roles for users who require remote access to network services with the privileges associated with the domain Administrator account or a service account on the remote computer.

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone where you want to define a new role that includes a network access right.
3. Expand the **Authorization** node.
4. Select **Role Definitions**, right-click, then click **Add Role**.
5. Type a role name and optional description for the role.
The description can include details about time restrictions for the role and whether the role is audited or not.
6. Click **Available Times** and use the grid to specify when to allow or deny access for this role definition if you want to restrict when this role is available.
7. Click the **System Rights** tab and select **Remote login is allowed** to allow users in the role to connect to services on the remote computer.

The user must be able to connect to the computer remotely to perform administrative tasks on that computer. If you want to allow users to log on locally, you can also select **Console login is allowed**.

Users must be assigned to at least one role with either console login or remote login rights to access any computers where the Centrify Agent for Windows is installed. You can grant access using the Windows Login role definition or the system rights in any custom role definition.



If you want to require multi-factor authentication for users to access the role, select **Require multi-factor authentication**. You can also require multi-factor authentication for access to individual rights when you define the rights to add to roles. For more information see [Enabling multi-factor authentication for Windows rights](#).

8. Click the **Audit** tab and select an auditing option.

If you select **Audit not requested/required**, users can connect to remote audited computers without having their session activity recorded. An audit trail event is recorded in the Windows event log when users select this role to connect to remote servers, but the detailed record of what took place during the session is not captured.

If you select **Audit if possible**, session activity recorded when users log on to audited computers and not recorded when they log on to computers where audit and monitoring service is not enabled or audited computers when audit and monitoring service is not currently running.

If you select **Audit required**, users can only log on to audited computers when audit and monitoring service is running. If audit and monitoring service is not available or not currently running, the role is not available and users cannot use their elevated privileges.

9. Click **OK** to save the role definition.
10. Select the role definition, right-click, then click **Add Right** to add a network access right to the role definition.
11. Select the network access right from the list of rights from the current zone and from any parent zones, then click **OK** to add the right to the role definition.

Combining rights in the same role definition

The previous sections illustrate how to create custom role definitions specifically for desktop, application, or network access rights. You can also combine multiple rights in the same role definition. For example, you can create a role definition that allows a user to open a specific application on the local computer using a service account with elevated privileges. The same role definition can also include a network access right that enables the user to modify information on a remote server.



Assigning users and groups to a role

You can assign a role to an Active Directory user or to an Active Directory group. You can assign a role that is defined in the current zone or in a parent zone. You can also specify optional start and end times for the role assignment.

To assign users and groups to a role in a zone:

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone where you want to make role assignments.
3. Expand **Authorization**.
4. Select **Role Assignments**, right-click, then click **Assign Role**.
5. Select the role definition from the list of roles, then click **OK**.

By default, the role is set to start immediately and never expire. You can set a **Start time**, **End time**, or both start and end times for the role assignment. For example, if the role applies to a contractor who will be hired for a specific amount of time and you want to automatically disable the role after they finish the job and leave the organization, you can specify the start and end times when you assign the role.

6. Select whether the role assignment applies to all Active Directory accounts, all local accounts, or specific Active Directory and local accounts.

To assign the role to specific accounts, click **Add AD Account** to search for and select the Active Directory groups or users to assign to the role, then click **OK**.

Rights and role assignments for local users

The rights you assign to users and group in a particular role apply to Active Directory users and groups. They can also apply to locally-defined users and groups if you configure the role definition to allow local accounts to be assigned to the role. All Windows users, including local users, must be assigned at least one role that allows them log on locally, remotely, or both.



Restricting roles that include network access rights

Because role definitions can include a combination of rights and you can assign roles to local users, Active Directory users, or both, it is possible for you to assign roles that include network access rights to local accounts. Access Manager does not prevent you from configuring role definitions or role assignments in this way. However, users who log on with a local account will not be allowed to select the Advanced View or those network access rights for the remote computer. Therefore, you should avoid configuring role definitions that include network access rights and allow local accounts. Instead, you should keep role definitions that include network access rights separate from role definitions that allow local accounts to be assigned.

Making rights and roles available in other zones

The access rights and role definitions that you create are specific to the zone where you configure them, and to any child zones of that zone. Once configured, though, you can copy and paste or drag and drop the definitions from one zone to another. After you import the information into a new zone, you can modify any of the details you have previously defined. For example, you can choose to export all the rights you have defined in one zone but create a completely new set of role definitions for those rights in the import zone.

Rights, roles, and role assignments are all inherited from parent to child zones, so generally there is no need to import or export roles within a zone hierarchy, but you may want to do so across zones. For example, if you have set up separate parent zones for different lines of business or different functional groups in your organization, you might want to import rights and roles from one business unit or functional group to another.

Exporting a zone's rights and role definitions

You can export right and role definitions to an xml file that you can then use to import these definitions into another zone.



To export rights and role definitions:

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone that has the rights and roles you want to export.
3. Expand Select the **Authorization** node, right-click, then click **Export Roles and Rights**.
4. Select the information you want to export, then click **Next**.
5. Click **Browse** to specify a location and file name for the export file, then click **Next**.
6. Review the information to be exported, then click **Finish**.

Importing rights and role definitions into a new zone

You can import rights and role definitions that you have previously saved from a different zone. You can also copy a paste or drag and drop rights and roles to a different zone.

To import rights, role definitions, and role assignments:

Before you begin, be certain you have saved rights and role definitions from a different zone and know the location of the xml file in which they are saved.

1. Open Access Manager.
2. Expand **Zones** and the parent zone or child zones until you see the zone into which you want to import rights and roles.
3. Select the **Authorization** node, right-click, then click **Import Roles and Rights**.
4. Click **Browse** to navigate to the file that contains the authorization information you want to import, then click **Next**.
5. Select the information you want to import, then click **Next**.
6. Review the information to be imported, then click **Finish**.



Copying rights and role definitions into a new zone

Exporting and importing information from one zone to another is the best solution if you want to include most or all information about rights and roles in a new zone. If you want to limit the information copied from one zone to another, you can copy and paste or drag and drop the information instead. With copy and paste, you can select specific right definitions, role definitions, or role assignments that you want to include in a new zone.

To copy role assignments from one zone to another, however, you should verify that the role definition associated with the role assignment exists in the new zone or is included in the information you are copying to the new zone.

To copy rights, role definitions, or role assignments:

1. Open the Access Manager.
2. Expand **Zones** and the parent zone or child zones until you see the zone that has the rights, role definitions, or role assignments you want to copy.
3. Expand the **Authorization** node.
4. Expand **Window Right Definitions**, **Role Definitions**, or **Role Assignments** until you see the specific right, role, or role assignment you want to copy.
5. Select the specific right, role definition, or role assignment to copy, right-click, then click **Copy**.
6. Open a different zone and expand **Authorization > Windows Right Definitions**, **Role Definitions**, or **Role Assignments**, right-click, then click **Paste**.

Alternatively, you can select a specific right, role definition, or role assignment and drag it to the appropriate node in a new zone.

Viewing rights and roles

You can view the status and effective rights for any user in a zone, whether they have been assigned a role or not. You can view detailed information about the rights and role assignments for users by selecting **Show Effective Windows User Rights** in the Access Manager console.



Displaying rights for an individual user in the console

To view role assignments and Windows access rights for a user in the Access Manager console:

1. Open Access Manager.
2. Expand **Zones** and the parent zone or child zones until you see the zone that has the user of interest.
3. Right-click, then click **Show Effective Windows User Rights**.
4. Select a user to see information for the user in the selected zone or click **Browse** to select a specific computer in the zone if you only want to view user rights for a particular computer in the selected zone.
5. Click a tab to see the user's role assignments, desktop rights, application rights, or network access rights.
 - **Role Assignments** lists the user's role assignments, including where the assignment was made. For example, the Object Assigned column indicates whether the assignment for a user is explicit (*user@domain*), from a group (*group@domain*), or inherited from another setting (All AD Accounts). The Start Time and End Time are only displayed for roles that have time constraints.
 - **Windows Desktops** lists the user's desktop rights granted by the roles to which the user is assigned. The tab identifies the account that can be used to open a new desktop or run an application, the zone where the desktop right is defined, and the role definition that includes the right.
 - **Windows Applications** lists the user's application rights granted by the roles to which the user is assigned. The tab identifies the specific application and the account that can be used to run the application, the zone where the application right is defined, and the role definition that includes the right.
 - **Network Access** lists the user's network access rights granted by the roles to which the user is assigned. The tab identifies the account that can be used to connect to services on a remote computer, the zone where the network access right is defined, and the role definition that includes the right.
6. Click **Close** when you are finished reviewing user rights in a zone or on particular computers.



Scenario: Using a network access role to edit group policies

The steps in this section illustrate a specific scenario of how to configure and use a desktop right and a network access right that allows the user Josh.Adams to log on with his normal Active Directory credentials, open an application that enables him to edit group policies, then connect to a domain controller with administrative privileges so that he can edit a Group Policy Object.

1. Install the Centrify Agent for Windows on the domain controller.
2. Install the Centrify Agent for Windows on a Windows computer that hosts the Group Policy Management console that the Josh.Adams uses to access the domain controller remotely.
3. Assign Josh.Adams the predefined Windows Login role and the custom role definition `gpedi t` that includes a desktop right and a network access right.
4. Josh Adams logs on to his Windows computer using his Active Directory user name and password.
To use a role with network access rights, you cannot log on using a local user account. You must use a domain user account authenticated using Active Directory.
5. On his local computer, Josh right-clicks the Centrify icon in the system tray section of the task bar, then selects New Desktop.
6. In his list of available roles, Josh selects his `gpedi t` role, then clicks OK.
7. Josh opens the Group Policy Management console on his local computer, connects to the domain controller in the console, then selects the default domain policy Group Policy Object.
8. Josh right-clicks the default domain policy, then selects Edit to modify the group policy.
9. When he is done working with the group policies, he switches back to his default desktop.



Scenario: Using multiple roles for network resources

For the local computer, users can select only one role at a time for their desktop or running an application. However, users can select more than one role to access network resources. By selecting multiple roles on the client, users can run applications that connect to multiple remote servers to perform administrative tasks.

In this scenario, Maya.Santiago uses a privileged account to open SQL Server Management Studio on her local computer. From this application, she wants to add accounts that require domain administrator privileges on a remote domain controller and modify database settings on a remote SQL Server instance. To do her work, she needs elevated privileges to run SQL Server Management Studio on her local computer and network access rights to contact the domain controller and the database server.

As the administrator, you have prepared the environment:

- You have put computers in appropriate zones and configured appropriate rights.
- You have configured a role definition, `sideBet-DC-Admin`, that grants network access to the domain controller using elevated privileges.
- You have also configured a role definition, `SQL-DB-Default`, that grants network access to SQL Server instances using elevated privileges.
- You have assigned Maya.Santiago to the roles.

To use an application that connects to multiple remote servers:

1. Install the Centrify Agent for Windows on the domain controller, the computer that hosts the SQL Server instance, and the computer Maya.Santiago uses to manage the SQL Server instance.
2. Assign Maya.Santiago the custom roles definition `sideBet-DC-Admin` that includes a desktop right and a network access right.
3. Maya.Santiago logs on to her Windows computer using her Active Directory user name and password.
4. On her local computer, Maya right-clicks SQL Server Management Studio, selects **Run with Privilege**.



5. Maya clicks **Advanced View** to see the list of available roles and selects `SideBet-DC-Admin` as the local role that enables her to run local applications with administrator privileges.
6. Maya then clicks the **Select one or more network roles** option and selects the `SideBet-DC-Admin` role for remote access to the domain controller and the `SQL-DB-Default` role for remote access to the database server, then clicks **OK**.

After she clicks OK, SQL Server Management Studio starts and she connects to the remote SQL Server instance using Windows authentication. The change to a role with privileges is recorded in the local Windows Application event log.

7. Maya uses SQL Server Management Studio to add and modify information on the domain controller and the SQL Server database.
8. When she is done working, she closes the application and returns to her default desktop and her login account privileges.

Defining rights for Windows applications that encrypt passwords

Microsoft provides a data protection application-programming interface (DPAPI) to enable applications to secure sensitive information, such as passwords, using encryption. The Data Protection API is the most common way to secure personal information on Windows computers because the information that is encrypted for one user cannot be decrypted by another user. Many applications and system services, including Microsoft Encrypting File System (EFS), Microsoft Internet Explorer, and Google Chrome for example, use the Data Protection API to encrypt passwords.

To use a desktop or application right with an application that uses the Data Protection API, you should select the **Self with added group privileges** option for the Run-as account. If you select this option when defining a right, you can install the Centrify Agent for Windows on the computer where the application using the Data Protection API is installed to allow users to run the application with administrative privileges.

If you want to use a specific user account for an application that uses the Data Protection API, you must install the Centrify Agent for Windows on both the domain controller and the computer where the application using DPAPI is installed. You must also make sure the domain controller is in a zone where

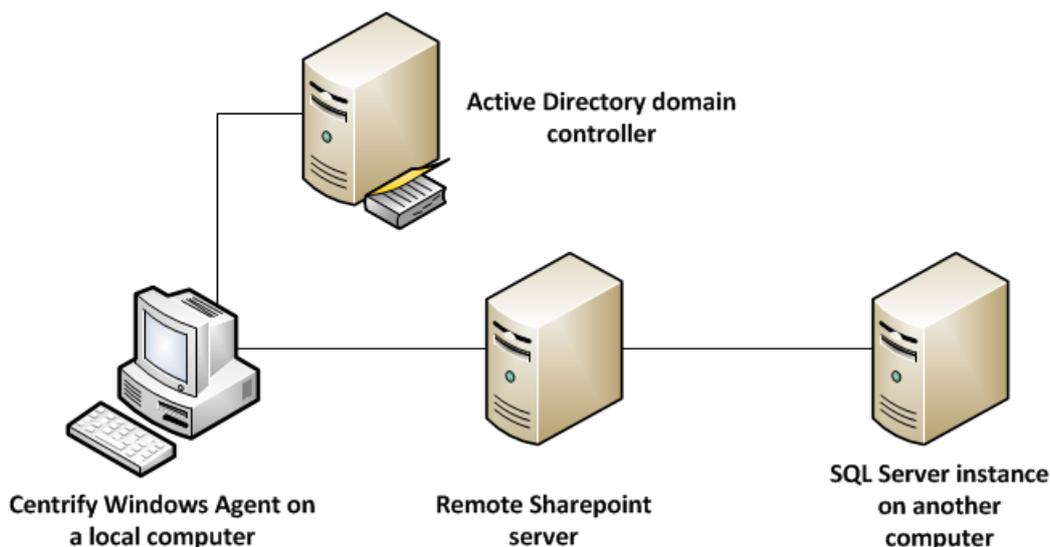


users who are going to use the application are granted network access rights. In this scenario, the domain controller must be able to confirm the identity of the specific user account to allow protected information to be decrypted.

For example, assume you define an application right for running Access Manager using the Windows AM-Owner account and assign the user Steve to a role that has this application right. When Steve logs on to the computer where Access Manager is installed and opens the application using the role he is assigned, the Centrify Agent for Windows on the domain controller identifies him as the user AM-Owner and provides Jess with the master key for encryption and decryption, enabling him to use Access Manager to add computers, deploy agents, and perform other tasks.

Enabling access across multi-tiered application layers

The traditional client/server scenario involves using a Windows client computer to connect to a Windows server to perform some operation. However, it is increasingly common that privileged access must cross multiple application layers. For example, you might have users who log on with their normal credentials who perform administrative tasks on a remote Sharepoint server and those tasks further require access to a SQL Server instance on yet another computer.



One way to ensure access across multiple applications tiers is to have all of the remote computers involved be in the same zone. At a minimum, the client computer and the computer in the first tier must have the Centrify Agent for



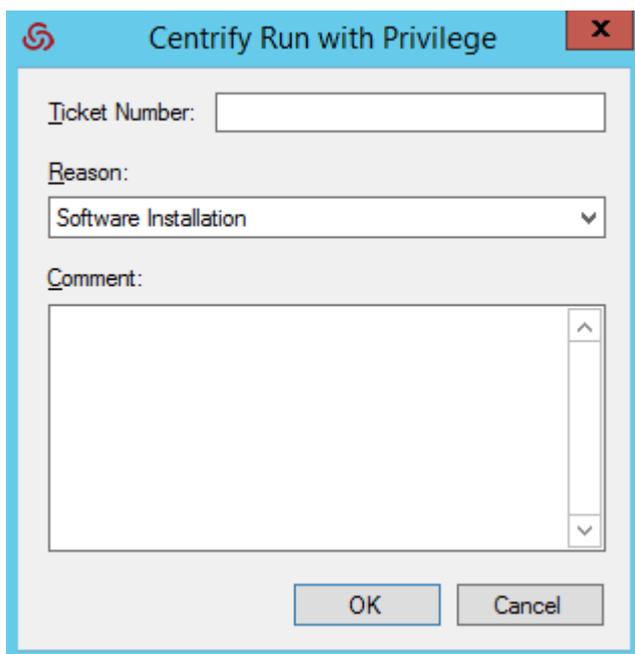
Windows installed. If the client computer and the computer in the first tier are in different zones, which is the most common scenario, you should place computers in any additional tiers in the same zone as the computer in the first tier.

Requiring users to justify privilege elevation

You can assign some group policies that force your users to provide a reason when they choose to run an application with privilege. There are two group policies that you can use:

- **Require justification on privilege elevation:** Use this group policy to require any user to provide a reason when they operate with elevated privileges, such as run with privilege, run as role, and new desktop.
- **Specify a privilege elevation validator:** You can use this computer configuration group policy to validate ticket information that a user enters when she provides a ticket number along with a privilege elevation reason. You can validate ticket information using a customized PowerShell script against a ticketing system, such as ServiceNow.

You can use just one of these policies or both. With either of these policies, when a user goes to run an application with privilege, they're prompted with an additional dialog box where they can enter a ticket number, a reason category, and any comments.



The above dialog box prompts users to enter the following information:



- **Ticket number:** If you have enabled the privilege elevation validator policy and subsequent script, you can validate the ticket number that a user enters against a ticketing system such as ServiceNow. If you haven't enabled the privilege elevation validator policy, users can enter any text string here.
- **Reason:** The user selects the reason category that best fits their situation. Their choices are:
 - Software Installation
 - Remote System Administration
 - Local System Administration
 - Windows Feature Management
 - System Networking Change
 - Maintenance (Shutdown, Reboot, Power Off)
 - PowerShell or Other CLI
 - Centrify Operation (Services, Zone Operations, etc.)
 - Other
- **Comment:** The user enters any comments about their need to run with privilege. You can view these comments in the audit trail event.

For more details about these policies, see the Group Policy Guide and the group policies' explain text.

Working with computer roles

A computer role associates a group of computers in a zone with a set of role assignments to users or groups. For example, you might have a set of computers dedicated to a specific function, such as hosting Oracle databases or payroll processing application. Users who are database administrators for those computers require different privileges than users who update payroll records on those computers.

Using a computer role, you can associate the group of computers that host an Oracle database with a specific role assignment, for example, users who are assigned the `oracle-dba` role. The `oracle-dba` role definition might include desktop and network access rights because the users assigned to the `oracle-dba` role require administrative privileges.



You could also create a second computer role that associates the group of computers that host the payroll processing application with a group of users who are allowed to log on and update payroll records without granting any other administrative privileges. For example, if some of the computers that host an Oracle database are used for payroll processing, you can define another computer role—`payroll-west`—that associates just those computers with the role assignment `payroll_mgmt`. The `payroll_mgmt` role definition might have the console login right and an application right specifically for the payroll application. When users are assigned the `payroll_mgmt` role, they can log on locally and run the payroll application with elevated privileges only on the group of computers defined in the computer role `payroll-west`.

To use computer roles, you must do the following:

- Decide on the attribute the computers in a particular group share. For example, you can use a computer role to identify computers in the web farm, that host specific applications, or serve a specific department.
- Identify the sets of users that share common access rights and create Active Directory groups for them. For example, if you are creating a computer role for Oracle database servers, you might have different access rights for application users, database administrators, and backup operators.
- Identify the role definitions each set of users should be assigned. For example, application users role might use the default `windows Login` role, while administrators might require a custom role definition with desktop and network access rights, and backup operators might require a custom role definition with an application right.

Using computer roles to simplify the management of access rights

Deciding how best to use computer roles requires some planning and configuration that may not be part of your initial deployment plan. To make effective use of computer roles, you also prepare appropriate role definitions for different sets of users. However, computer roles provide a powerful and flexible option for managing access to computers using your existing processes and procedures for managing Active Directory group membership.

After you create a computer role, it is easy to manage even as your organization changes and grows. For example, if another Oracle database server comes online, you add it to the computer group you created for Oracle



database servers in Active Directory. If other DBAs join your organization, you add them to the Active Directory group you created for Oracle administrators. The computer role links the computer group to the role assignment and no additional updates are needed to accommodate these kinds of organizational changes. If you need to modify the access rights, you can change the role definition and have the changes apply to all members of the group.

Create an Active Directory group for a set of computers

Computer roles create links between objects in Active Directory and access rights defined in Access Manager. After you have identified a group of computers that share a common attribute, you should create an Active Directory group for those computers if one does not already exist.

You can also create the computer group and add its members directly from Access Manager when you create the computer role. If you are not preparing the Active Directory group before creating the computer role, you can skip this section and go directly to [Create a new computer role](#).

To create an Active Directory group for computers in a computer role:

1. Open Active Directory Users and Computers to create a new Active Directory group.
2. For example, create a new Active Directory group for Oracle Database Servers.
3. Select the new computer group, right-click, then click **Properties**.
4. Click the **Members** tab, then click **Add**.
5. Click **Object Types**, select **Computers**, then click **OK**.
6. Search for and select the computers that you have identified as Oracle database servers as members of the new group, then click **OK**.
7. Click **OK** to save the group.

Create an Active Directory group for each set of access rights

In addition to the Active Directory group for the computers in a computer role, you should have an Active Directory group for each set of users that should have different access rights. By mapping Active Directory groups to role



definitions, you can manage group membership and access rights at the same time using your current procedures.

To create an Active Directory group for each set of users linked to a computer role:

1. Open Active Directory Users and Computers to create a new Active Directory group for each set of users to link to the computer role.
For example, create separate Active Directory groups for application users, database administrators, and backup operators using a naming convention similar to *ComputerAttribute_Role_UserSet*. For example, create the following Active Directory groups:
 - OracleServers_Role_AppUsers
 - OracleServers_Role_DBAs
 - OracleServers_Role_Backup
2. Select each new group, right-click, then click **Properties**.
3. Click the **Members** tab, then click **Add**.
4. Search for and select the users that you have identified as members of the each group, then click **OK**.
5. Click **OK** to save the group membership.

Create a role definition for each set of users with different access rights

Before you create a new role definition, identify the specific rights associated with each role and define those rights if they do not already exist. For this sample scenario, you might create role definitions similar to the following:

- Oracle_AppUsers with windows Login access and an application right for a specific database application.
- Oracle_DBAs with windows Login access and desktop and network access rights on computers in a specific zone.
- Oracle_Backup with console login allowed right and an application right that allow members of the group to run backup utilities with the privileges of the built-in Backup Operators group.



Create a new computer role

After you have prepared the appropriate Active Directory groups and role definitions for different sets of users, you can create one or more computer roles.

To create a new computer role:

1. Open Access Manager.
2. Expand **Zones** and the parent zone or child zones until you see the zone that has the computer for which you want to define a computer role.
3. Expand the **Authorization** node.
4. Select **Computer Roles**, right-click and click **Create Computer Role**.
5. Type a name and description for the computer role.
For example, type `OracleServers`, and an optional description, such as `Oracle database servers in the San Francisco data center`.
6. In **Computers group** list, select `<...>` to search for the Active Directory group of computers you created in [Create an Active Directory group for a set of computers](#).
Select `<Create group >` if you want to create a new Active Directory group of computers and add members now. If you are creating a new group, click **Browse** to select a container to use, type a group name, and select the scope of the group, then click **OK**.
7. Click **OK** to save the computer role.
8. If you selected an existing computer group, expand **Computer Roles > Members** to see the computers that are members of this computer role.
If you created a new computer group at Step 6, select the new computer role, right-click **Members**, then select **Add Computer** to search for and select one or more computers to add to the group.

Add role assignments to the computer role

If you have created the appropriate Active Directory groups and role definitions that you want to assign, you can now assign the roles to set of users as required.



To add role assignments to users in Active Directory groups:

1. Expand the computer role you just created, for example, expand **OracleServers**.
2. Select **Role Assignments**, right-click, then click **Assign Role**.
3. Select the role definition from the list of roles, then click **OK**.
For example, select the `Oracle_DBAs` role definition. By default, the role is set to start immediately and never expire. You can set a **Start time**, **End time**, or both start and end times for the role assignment. For example, if the role applies to a contractor who will be hired for a specific amount of time and you want to automatically disable the role after they finish the job and leave the organization, you can specify the start and end times when you assign the role.
4. Select whether the role assignment applies to all Active Directory accounts, all local accounts, or specific Active Directory and local accounts, then click **OK** to complete the role assignment.
For example, to assign the `Oracle_DBAs` role to the Active Directory `OracleServers_Role_DBAs` security group, click **Add AD Account**. You can then select **Group** to search for the group, select it from the results, then click **OK**.
5. Repeat Step 1 through Step 4 for each group that you want to add to this computer role. For example, repeat the steps to assign the `Oracle_AppUsers` role to the `OracleServers_Role_AppUsers` security group and the `Oracle_Backup` role to the `OracleServers_Role_Backup` security group.
6. Select the **Role Assignments** node to see all of the role assignments you have defined for groups associated with the computer role.
7. Select the **Members** node to see the computers or groups of computers to which the role assignments apply.

Assigning roles on multiple computers at once

To simplify the process of assigning Active Directory users or groups to a role, you can perform a bulk role assignment. With a bulk role assignment, you can assign a role to multiple Active Directory users and groups on multiple computers at the same time. For example, if you have two groups of SQL Server administrators and three computers where the members of those groups need access to their `SQLServerAdmin` role, you can select those two groups and



those three computers to be assigned the SQLServerAdmin role in the same process. You can also specify optional start and end times for the role assignment and have those settings apply for all of the users, groups, and computers you have selected for bulk assignment.

To assign users and groups to a role in a zone:

1. Open the Access Manager console.
2. Expand **Zones** and the parent zone or child zones until you see the zone where you want to make role assignments.
3. Right-click, then select **Assign Roles to Computers**.
4. Type the user and group names you want to be included in the role assignment, then click **OK**.

You can specify multiple names separated by a semi-colon (;). You can also search for user and group names by typing part of the name and clicking Check Names or by clicking Advanced and entering search criteria.

5. Type the computer names you want to be included in the role assignment, then click **OK**.

You can specify multiple names separated by a semi-colon (;). You can also search for the computer names by typing part of the name and clicking Check Names or by clicking Advanced and entering search criteria.

6. Select a role for the list of roles available, then click **OK**.
7. Review the role assignment start and end time and the user and group accounts that are being assigned the role, then click **OK**.

You can make changes to the start and end times if you want those changes applied for all of the users, groups, and computers that are part of this bulk role assignment.

After you click **OK**, the selected users and groups are then automatically assigned the selected role on the selected computers.



Using the Authorization Center directly on managed computers

The Authorization Center is available on managed computers where you have deployed the Centrify Agent for Windows and enabled the privilege elevation service. From the Authorization Center, you can view details about the rights, role definitions, role assignments, and auditing status for any users. Individual users can see details about their own login rights, effective roles, role assignments, role definitions, and auditing status. Administrators can select any user of interest to view the details for that user.

To use the Authorization Center on a local computer:

1. Log on to a computer where the Centrify Agent for Windows and privilege elevation features are deployed.
2. Click the arrow next to the notifications area in the taskbar.
3. Right-click the Centrify icon, , then select **Open Authorization Center**.
4. Click a tab to see details about the current user's roles.
 - **Effective Login Rights** displays the current user's local, remote, and PowerShell login rights and whether auditing is requested, required, or not applicable.
 - **Effective Roles** lists the roles that have been assigned to the current user and the status of each role names to which the user is assigned. You can right-click a role, then select Role Properties to view additional details, such as any time constraints defined for the role and the specific rights granted by the role.
 - **Role Assignments** lists details about the user's role assignments, including where the assignment was made. For example, the Object Assigned column indicates whether the assignment for a user is explicit, from a group, or inherited from another setting, for example, from the selection of All Active Directory Accounts. You can right-click a role, then select Assignment Properties or Role Properties to view additional details, such as any time constraints defined for the role and the specific rights granted by the role.
 - **Role Definitions** lists detailed information about the selected user's login rights and the audit requirements that have been defined for



the roles the user has been assigned. You can right-click a role definition, then select Properties to view additional details.

- **Auditing** lists the desktops used and auditing status for each desktop started in a session.

5. Click **Browse** to view information for another user.

6. Type all or part of the user name, then click **OK**.

If more than one user name is found, select the appropriate user from the results, then click **OK**.

7. Click **Close** when you are finished viewing detailed authorization information for the selected user.

Working with the authorization cache on managed computers

Authorization information—such as your rights, role definitions, and assignments—is cached locally on each computer where you have deployed the Centrify Agent for Windows. The cache saves access privilege information to improve performance and also to persist elevated privilege capabilities for users and groups when the computer is not connected to Active Directory.

The following sections describe:

- Which Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service capabilities are and are not persisted by the cache when a computer is disconnected from a domain controller.
- Where the cache resides.
- How and when to perform cache operations such as refreshing, flushing, and dumping.

Persisted and non-persisted capabilities

The authentication, privilege elevation, and audit and monitoring services cache persists several role-based capabilities when a computer is not connected to Active Directory. A computer is considered to be not connected when the Windows agent is unable to reach one or more of the following entities:



- The domain to which the computer is joined.
- The domain of any zone in the zone *hierarchy*. The zone hierarchy is the domain of the zone that the machine is joined to, or any parent zones of that joined zone.
- An Active Directory global catalog (GC) associated with any of these domains.

If the Windows agent can reach all of these entities, it is considered to be *connected*.

Persisted capabilities

These capabilities are supported when a computer is not connected:

- Users can log in based on role.
- Users can run applications based on role.
- Users can create desktops based on role.
- Computers can be removed from zones.
- Centrify software can be installed (but the computer cannot be joined to a zone).
- Centrify software can be upgraded, but this practice is not recommended because there will be no authorization data in the cache after the upgrade.

Non-persisted capabilities

These limitations exist when a computer is not connected:

- You cannot join a zone or change a computer's zone.
- The use of Network rights is not supported.

Cache location

The cache resides in

`SYSTEMDRIVE\ProgramData\Centrify\DirectAuthorize\Cache.`



Performing cache operations

You must have administrator privileges to perform the cache operations described here. Available cache operations include:

- Refreshing the cache (perform this operation from the user interface or the command line)
- Flushing the cache (performed from the command line)
- Dumping the cache (performed from the command line)

Refreshing the cache

As administrator, you can refresh the cache from the user interface or from the command line. Refreshing the cache updates the cache with fresh information from Active Directory, ensuring that the agent has the most up-to-date information about users' current rights and roles.

Refreshing the cache is useful if you change authorization information with the management console, and you want to see the updated information on the Windows agent right away.

Note:

In domains containing multiple domain controllers, you might not see the updated information even after you refresh the cache. In cases such as this, wait for Active Directory replication (typically a few minutes), and then refresh the cache again. Alternatively, wait another 10 minutes and the agent will refresh the data on its own.

You can refresh and flush the cache only on computers that are connected to a domain controller.

To refresh the cache from the user interface:

1. Open the agent configuration panel by clicking **Agent Configuration** in the list of applications on the Windows Start menu.
2. Click **Centrify Privilege Elevation Service**.
3. Click **Settings**.
4. Click the **Troubleshooting** tab.
5. Click **Refresh**, then click **OK** to acknowledge the successful operation.



Note: Alternatively, you can execute the `dzrefresh` command line utility to refresh the cache as described in the next section.

To refresh the cache from the command line:

Execute the `dzrefresh` command line utility to refresh the cache. Executing `dzrefresh` performs the same operation as clicking the **Refresh** button in the agent configuration panel **Troubleshooting** tab.

The syntax for running the `dzrefresh` utility is:

```
dzrefresh
```

Flushing the cache

Execute the `dzflush` command line utility to flush (clear) the cache. Flushing the cache removes all cache data and reloads it from Active Directory. You should flush the cache only when directed to do so by Centrify Support. Under most circumstances, you should refresh the cache rather than flush the cache.

The syntax for running the `dzflush` utility is:

```
dzflush
```

Dumping the cache

Execute the `dzdump` command line utility to dump the cache to standard output or to a redirect file that you specify on the command line. You can also use the options shown here to display only specific types of cache data, such as zone hierarchy, role definitions, right definitions, and other data.

You should execute the `dzdump` utility only when directed to do so by Centrify Support.

The syntax for running the `dzdump` utility is:

```
dzdump [/d [directory-path]] [/w=screen-width] [/s] [/n] [/g] [/l] [/a]
[/r] [/i] [/t] [/z] [/u] [/h]
```

If you execute `dzdump` with no options, all `dzagent` in-memory cache is dumped.

Setting valid options

You can use the following options with `dzdump`:



| Use this option | To do this |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <code>/d</code> | Dump cache files from the default location. |
| <code>/d=</code> <i>directory-path</i> | Dump cache files from the specified location. |
| <code>/w=</code> <i>screen-width</i> | Use the specified width rather than the default of 80 for word-wrap. Set <code>/w=0</code> to disable word-wrap. |
| <code>/s</code> | Display SID mappings. |
| <code>/n</code> | Display name mappings. |
| <code>/g</code> | Display assignee mappings. |
| <code>/l</code> | Display assignments in the joined zone hierarchy. |
| <code>/a</code> | Display assignments for SIDs. |
| <code>/r</code> | Display role definitions. |
| <code>/i</code> | Display right definitions. |
| <code>/t</code> | Display access token information. |
| <code>/z</code> | Display zone hierarchy. |
| <code>/u</code> | Display recent user log-ins. |
| <code>/h</code> | Display help information. |

Configuring PowerShell Remote Access

If you want to allow some of your users to be able to run PowerShell commands on remote computers by way of PowerShell remoting, be aware of the following requirements:

- The target computer needs to have the Centrify Agent for Windows installed with the Centrify Privilege Elevation Service enabled.
- Assign the user to a role with the "PowerShell remote access is allowed" system right granted.

If you're using the Centrify Audit & Monitoring Service, when a user attempts to run PowerShell remotely on a computer, the system triggers an audit trail event. Centrify Audit & Monitoring Service is an optional service.

To assign PowerShell remote access to a user:

1. In the **Centrify Access Manager** console, open the zone that the Windows system to be managed belongs to (Centrify Access Manager is not necessary installed on the machine with the Windows agent).



2. Under **Role Definitions**, right-click a role that you'd like to assign PowerShell remote access permission to and select **Properties**.
3. Under **System Rights > Windows rights**, select **PowerShell remote access is allowed**.
4. Right-click **Role >Assignment** and select **Assign Role**.
5. Select the role as defined above and assign the Windows account to it.

Authentication service enforcement

Any time you open the Access Manager console, a background process determines the availability of licenses.

As you increase the number of licenses in use, license enforcement is progressive. If the number of computers is less than 90% of the number of licenses you have purchased, there's no affect on any auditing features. If the number of computers is more than 90% of the licenses purchased, enforcement depends on the number of licenses in use:

- 90-100% of the licensing limit displays a warning message that you are close to over-deployment, but you can continue to use all authentication and privilege elevation features.
- 100-120% of the licensing limit displays a warning message that you must acknowledge by clicking **OK** when you open the console, after which you can resume using the console.
- Over 120% of the licensing limit displays a warning message for 60 seconds when you open the console. If you see the 60 second warning message, use the License dialog box to add license keys to continue using features.

You can contact Centrify to purchase additional licenses or remove some computers to bring the number of licenses used into compliance.

Configuring MFA with RADIUS for Centrify Privilege Elevation Service for Windows checklist

This document provides a configuration checklist for 3rd party multi-factor authentication providers such as Duo, Okta, SecurID (or any other vendor that



provides a RADIUS service) to provide identity validation with the Centrify Privilege Elevation Service in the Microsoft Windows platform.

If you have an identity service provider (such as Duo, Okta, SecureID, and so forth) that you use for MFA logins, you can integrate authentication and privilege elevation with your identity provider and the RADIUS protocol to require MFA for privilege elevation tasks, such as Run with Privilege and New Desktop.

Make sure that you work with your RADIUS expert along with your network and directory services lead administrators during the design and configuration tasks.

The checklist below includes links to documented procedures.

Note: If you use Privileged Access Service, although you can enable MFA with RADIUS, the recommended practice is that you use the native integration.

| Step# | RADIUS Configuration Step | Notes |
|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| RADIUS requirements | | |
| 1 | Gather the following settings for your RADIUS service: <ul style="list-style-type: none">■ IP address or fully qualified domain name■ Port■ Timeout settings■ Pre-shared secret | |
| 2 | Verify that you can generate a RADIUS one-time password successfully. | |
| 3 | Verify that identity authentication is working correctly with your RADIUS system. | |
| 4 | Have access to someone who is knowledgeable about your RADIUS system and can answer questions or help troubleshoot issues, if needed. | |
| Windows and Active Directory requirements for RADIUS configuration | | |



| Step# | RADIUS Configuration Step | Notes |
|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| 5 | A Windows computer to use as a RADIUS client for initial testing, including: <ul style="list-style-type: none">Client nameClient IP address | |
| 6 | Make sure that client systems can reach the RADIUS server over the network (check your firewall settings). You may need help also from your network team if your RADIUS cluster has a load-balancer in the front end. | |
| 7 | You have administrative access to the designated Windows computer so that you can install software and do configurations. | |
| 8 | You have Active Directory account access so that you can modify group policies that apply to the target computer. | |
| 9 | You have access to the Group Policy Management Console. | |
| 10 | Your Active Directory expert must decide how the group policy layout and scope will be designed so that the group policies are applied to the clients based on their RADIUS service availability. | |
| Centrify Authentication and Privilege Elevation Services Requirements for RADIUS configuration | | |
| 11 | Access Manager console is installed on the client computer. | For details, see Running the setup program on a Windows computer . |
| 12 | The Centrify Agent for Windows is installed on the client system, you've configured the system to work with Centrify Privilege Elevation Service, including joining the computer to a zone. | For details, see Installing the Centrify Agent for Windows . |
| 13 | You have administrative access to Access Manager so that you can manage roles and rights. | |



| Step# | RADIUS Configuration Step | Notes |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 14 | <p>The Centrify group policy templates from release 19.6 or later are installed.</p> <p>For RADIUS configuration, you need at least the Centrify Windows settings group policies.</p> | <p>For details, see Installing group policy extensions separately from Centrify Access Manager.</p> |
| 15 | <p>If you want to capture the RADIUS events in your SIEM system, make sure the Audit trail is configured to go to the local log file.</p> | <p>In GPME, go to computer Configuration > Policies > Centrify Audit Trail Settings > Centrify Global Settings > Send audit trail to log file (this is not configured by default).</p> <p>For details, see "Send audit trail to log file" in the <i>Group Policy Guide</i>.</p> <p>For details, see "Send audit trail to log file" in the <i>Group Policy Guide</i>.</p> |
| 16 | <p>You have a role and user to test with. Make sure the role has rights for privilege elevation, such as New Desktop rights or Run as Role.</p> | <p>Make sure that you can elevate privileges successfully for that user and role before you try to configure RADIUS authentication.</p> |
| Configure a system to use RADIUS for privilege elevation (using group policies) | | |



| Step# | RADIUS Configuration Step | Notes |
|-------|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17 | Enable and configure the RADIUS group policies. | <p>Configure the following group policies:</p> <p>Windows > MFA Settings > Specify the authentication source for privilege elevation : set this policy to RADIUS Authentication.</p> <p>Windows > MFA Settings > Remote Authentication Dial-In User Service (RADIUS) Settings ></p> <ul style="list-style-type: none">■ Enable Remote Authentication Dial-In User Service (RADIUS): enable this policy.■ Specify the RADIUS connection timeout: Configure to match your RADIUS timeout setting.■ Specify the RADIUS server IP address: enter your RADIUS IP address.■ Specify the RADIUS server port number: enter your RADIUS port number (the default is 1812). <p>For details, see "Remote Authentication Dial-In User Service (RADIUS) Service Settings" in the <i>Group Policy Guide</i>.</p> <p>For details, see "Remote Authentication Dial-In User Service (RADIUS) Service Settings" in the <i>Group Policy Guide</i>.</p> <p>After you update the policies, do a group policy update on the Windows client computer.</p> |
| 18 | Configure the role to require re-authentication using multi-factor authentication. | <p>For example:</p> <ol style="list-style-type: none">1. Right-click your test role and choose Properties. The Role Properties dialog box opens.2. Click the Run As tab.3. Select Re-authenticate current user and then select Require multi-factor authentication.4. Click OK to apply the changes. |



| Step# | RADIUS Configuration Step | Notes |
|-------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 19 | Run dzflush to make sure that the agent has the changes from Access Manager. | For details, see Using dzflush . |
| 20 | Set the RADIUS shared secret. | <p>The RADIUS secret is unique to each system and will match the secret that the RADIUS server has. You can set the pre-shared secret by either of the following methods on the client computer:</p> <ul style="list-style-type: none">■ Run the Set-CdmRadiusSecret cmdlet to set the RADIUS shared client secret. For details, see the DirectAuthorize PowerShell cmdlet help.■ Use the Agent Configuration settings dialog box to configure the RADIUS server, including the pre-shared secret. <p>For details, see Configuring agent settings for the Centrify Identity Services Platform.</p> |

TEST AND VERIFY

| | | |
|----|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21 | Verify that a user can elevate privileges by entering the RADIUS one-time password. | <p>For example, if your role has New Desktop rights:</p> <ol style="list-style-type: none">1. Right-click the System Tray and select New Desktop.2. In the dialog box that appears, select your test role and click OK.3. If the RADIUS authentication has been configured successfully, you are prompted to enter a password for RADIUS authentication. Enter the password and click Next to continue.4. You can also view the audit trails for the successful authentication in the system's event log. |
| 22 | Verify that a user cannot elevate privileges after entering an incorrect RADIUS one-time password. | |



Adding remote users automatically

If desired, you can configure your deployment so that members of the Windows Login group or the Windows Remote Login group are also automatically added to the Remote Desktop Users group and the CentrifysConsoleLogonUser group.

To make this change, add the following registry entry on each computer where you have installed the Centrifys Agent for Windows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Centrifys\DirectAuthorize\Agent\EnableAddUsersToRdpAndConsoleLogOn = 1
```

If you later uninstall the agent, the uninstall process removes the affected user accounts from the Remote Desktop Users group and the CentrifysConsoleLogonUser group. Only the user accounts that the agent added to those groups are affected.

Enabling users to run applications with alternate accounts

Alternate accounts are typically a privileged or administrator account in Active Directory that's associated with an owner account. You can log in to the alternate account using your main account.

For example, system administrators typically have several accounts, a user account for general log-ins and an administrative account to access specific systems and services.

Here are the things you need to do in order to enable the ability to run with alternate accounts:

1. Set up alternate accounts for users in Privileged Access Service
2. Install a cloud connector in your domain and the Web Server (IWA) service is enabled.
3. Enable the policy entitled "Enable run with alternate account."
4. (Optional but recommended) Configure the following policies to set up a grace period after which time users running applications with alternate accounts must re-authenticate:



- "Require re-authentication to run application with alternate account"
 - "Configure Windows authentication grace period for run with alternate account"
5. Install the Centrify Agent for Windows and enable the Centrify Identity Services Platform service on each computer where you want users to be able to run with alternate accounts.

If you don't enable the run with alternate account feature, your users can still run applications with these alternate accounts by logging in to Privileged Access Service and checking out the password.



Managing local Windows users and groups

You can manage your local Windows users and groups, if desired. This way, you can centrally manage the accounts.

Overall, to manage local users and groups on Windows systems, you'll need to

- Install the Centrify Agent for Windows on each Windows system where you want to manage local accounts.
- Enable local account management on those Windows systems in the Privilege Elevation settings for the agent. For details, see [Enabling Windows local account management](#).
- In Access Manager, you can then add, edit, or remove local users and groups. For details, [Adding local Windows accounts](#) and [Removing local Windows accounts](#)
- Manage the passwords for local Windows accounts. For details, see [Creating and managing local Windows user passwords](#).
- Use group policies to manage local Windows accounts. For details, see the Group Policy Guide.

Adding local Windows accounts

Before you enable local account management on your Windows computers, add the local users and groups in Access Manager.



Note: If you first enable local account management with the enforce option and if you have any existing local accounts on that system but not defined in a zone, then the service will remove those local users during the next synchronization. Built-in local Windows accounts are not removed.

To add a local Windows user:

1. In Access Manager, navigate to either a zone or a Windows computer and go to **Windows Data**
2. Right -click **Local Users** and select **Add User to Zone** or **Add User**, depending on where you're adding the user.
3. Enter the user name and click **OK**.
4. Specify the attributes for the local Windows user:
 - **Full name:** The first and last name of the new local Windows user.
 - **Description:** A description of the user.
 - **State:** Specify one of the following:
 - **Enable:** Set the state to Enable for a local Windows account that is in use.
 - **Disable:** Set the state to Disable for a local Windows account that is not in use.
 - **Remove:** If you've chosen not to enforce local account management, mark the user as Remove and the service will remove the user at the next synchronization interval.

Note: The service will not remove any built-in local Windows accounts, even if you mark it as Remove in Access Manager.
 - **Password options:** If desired, select any of the following:
 - **User must change password at next logon:** The service will force the local Windows user to change the account password the next time that the user logs in to the computer. Note that this option applies only to new accounts.
 - **User cannot change password:** The user won't be able to change the password.



- **Password never expires:** The user's password will never expire.
5. Click **OK** to save your changes.

The new user will be available on the affected systems after the next local account synchronization.

To add a local Windows group:

1. In Access Manager, navigate to either a zone or a Windows computer and go to **Windows Data**
2.
 - a. Right -click **Local Groups** and select **Add Group to Zone** or **Add Group**, depending on where you're adding the group.
 - b. Enter the group name and click **OK**.
3. Specify the attributes for the local Windows group:
 - **Description:** Enter a description of your choice.
 - **Members:** Click **Add** to launch the Add Members dialog. In a comma-separated list, type the names of the users who will be in the group.

Note that Access Manager does not check the validity of the user names that you provide. You should ensure that all of the names that you provide are local Windows user names that currently exist.
 - **State:** Specify either **Enable** or **Remove**.
 - **Enable:** Set the state to **Enable** for a local Windows account that is in use.
 - **Remove:** If you've chosen not to enforce local account management, mark the group as **Remove** and the service will remove the group at the next synchronization interval.
4. Click **OK** to save your changes.

The new group will be available on the affected systems after the next local account synchronization.



Enabling Windows local account management

You can have Centrify manage your local Windows user and group accounts; to do so, you need to enable and configure a few settings. Install the agent and enable local account management on each Windows system where you want to manage local accounts.

Be aware that if you enable local account management, the service does not delete any built-in Windows users or groups, even if you mark one of those accounts for remove.

Note: Windows local account management is not supported on domain controllers.

To configure local account management for Windows:

1. From the Centrify Privilege Elevation Service Settings dialog box Local Account Management tab, click **Configure**.

The Local Account Management Configuration dialog box opens.

2. Select the **Enable local account management** option.
3. Select **Yes** to enforce local account management or **No** to not enforce local account management.

Enforcing local account management means that after you remove a local Windows user or group from Access Manager, the service will remove the local user or group from the computer after the next synchronization.

If you choose not to enforce local account management, in order to remove a user you mark it as removed rather than explicitly removing the account from Access Manager.

4. Specify a script that will run when the service synchronizes local account information with Access Manager and the affected computers. The script can set the passwords for the local accounts and also display a list of enabled, disabled, or removed users.

For details, see [Creating and managing local Windows user passwords](#).

There is a sample script provided that you can use as a starting point:

```
C:\Program Files\Centrify\Centrify Agent for windows\SampleNotification.ps1
```



The script will run after each synchronization of local accounts when the any of the following have occurred:

- New local users are added
 - Local users are enabled
 - Local users are disabled
 - Local users are removed
5. Specify a synchronization interval.

This interval controls how often the service synchronizes local account information between Access Manager and the affected computers. The default is 60 minutes.

6. Click **OK** to save your changes and close the dialog box.

Creating and managing local Windows user passwords

After you create local Windows users, you still need to assign a password to each user. Instead of manually setting the passwords in Local Users and Groups, you'll set up the initial passwords for your local user accounts by way of a PowerShell script.

There is a sample script provided that you can use as a starting point:

```
C:\Program Files\Centrify\Centrify Agent for windows\SampleNotification.ps1
```

In general, the script should both set passwords and notify you of changes in local accounts. The script will run after each synchronization of local accounts when the any of the following have occurred:

- New local users are added
- Local users are enabled
- Local users are disabled
- Local users are removed

Typically, the script should perform the following user account tasks:



- Assign a random password to newly provisioned local users.
- Provide the user account information, including the generated passwords, to your password management solution.

After you have the script set up, you can use group policy to automatically run it. For details, see the *Group Policy Guide*.

How you set up the passwords and the script depends on if you're using a password management system or not. Below are the ways you can set up local user passwords.

Use Privileged Access Service to manage local Windows account passwords:

1. Register for Privileged Access Service.
2. Download the Centrify Client for Windows software package.
3. On each Windows computer where you will assign passwords to local users, run the `cenro11` command to register the computer as a managed resource.
4. Create a PowerShell notification script that runs on each of these Windows computers, gives each user a random password, and sends the password to Privileged Access Service.

In the script, you can set it to run the `csetaccount` command to send the password to Privileged Access Service. For details, see [Windows client commands \(doc portal\)](#).

5. Using one of the following two methods, configure the notification script to run after the agent synchronizes local account information:
 - In the local account management settings for the agent
Agent settings > Local Account Management tab > Configure > Local Account Management Configuration dialog box
 - In the group policy
(Centrify Settings > Windows Settings > Local Account Management > Notification Command Line)

Use a third-party system to manage local Windows account passwords:

1. Create a PowerShell script that runs on each of these Windows computers and gives each user a random password.



2. Include a section in the script that submits the passwords to the password management product for storage and maintenance.
3. Using one of the following two methods, configure the notification script to run after the agent synchronizes local account information:
 - In the local account management settings for the agent
Agent settings > Local Account Management tab > Configure > Local Account Management Configuration dialog box
 - In the group policy
(Centrify Settings > Windows Settings > Local Account Management > Notification Command Line)

Removing local Windows accounts

If you have enabled local account management on a Windows system, there are two different ways to remove users. Your approach depends on if you've configured to enforce local account management or not.

Be aware that if you enable local account management, the service does not delete any built-in Windows users or groups, even if you mark one of those accounts for remove.

To remove a local Windows user or group if local account management is enforced:

- In Access Manager, right-click the user or group and select **Delete**.
The account is removed from Access Manager immediately. When the service next synchronizes local account information, the service removes the user or group from the affected Windows systems too.

To remove a local Windows user or group if local account management is not enforced:

- In Access Manager, right-click the desired user or group and select **Change Profile State**, then select **Remove**.
The account is marked as "Remove" and remains visible in Access Manager. When the service next synchronizes local account information,



the service removes the user or group from the affected Windows systems too.



Managing auditing and audit permissions

This chapter describes how to use the Master Auditor role and group policies to control who is audited and who can search and play back captured user sessions for an installation.

The following topics are covered:

| | |
|-----------------------------------------------|-----|
| Configuring selective auditing | 207 |
| Enabling audit notification | 209 |
| Managing audit roles and auditors | 210 |
| How access roles and audit roles differ | 213 |

Configuring selective auditing

If you are using identity and privilege management features, you can control audit and monitoring service by using Access Manager to configure role definitions with different audit requirements, and then assigning those role definitions to different sets of Active Directory users. For more information about using role definitions to control auditing, see [Defining custom roles with specific rights](#).

If you are using audit and monitoring service without also using identity and privilege management features, you can use group policies to control which Windows users to audit, or to capture activity for all Windows users.

To control audit and monitoring service using group policies:

1. Open the Group Policy Management console.
2. Expand the forest and domains to select the Default Domain Policy object.



3. Right-click, then click **Edit** to open Group Policy Management Editor.
4. Expand Computer Configuration > Policies, then select **Centrify DirectAudit Settings**.
5. Select the Audited user list to identify specific users to audit.
When you enable this group policy, only the users you specify in the policy are audited. If this policy is not configured, all users are audited.
6. Select the Non-audited user list to identify specific users that should not be audited.
When you enable this group policy, only the users you specify are not audited. If this policy is not configured, all users are audited. If you enable both the Audited user list and the Non-audited user list policies, the users you include in the Non-audited user list take precedence over the Audited user list.

The following table details the effect of configuring and enabling the Audited user list and Non-audited user list group policies, and including or not including Windows users in those lists.

| Non-audited user list | Audited user list | How the setting affects auditing |
|------------------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Not configured | Not configured | No users are defined for either policy, so all users accessing audited computers are audited. |
| Not configured | Enabled | Only the users you specify in the Audited user list policy are audited. If no users are specified when the policy is enabled, no users are audited. |
| Not configured | Enabled | Only AUL is enabled, but user is not listed in it. |
| Enabled | Not configured | If no users are specified in the Non-audited user list and the policy is enabled, no users are exempt from auditing. All users are audited. |
| Enabled | Enabled | If both policies are enabled, the non-audited user takes precedence over the audited list of users. If a user is specified in the audited list, that user is explicitly audited. If a user is specified in the non-audited list, that user is explicitly not audited. If the same user is specified in both lists, the user is not audited because the non-audited user takes precedence. If no users are specified for either policy, all users are audited because the non-audited user takes precedence. |



Enabling audit notification

If you enable audit notification, users see a message informing them that their actions are being auditing when they log on. After you enable notification, the message is always displayed on audited computers if the session activity is being recorded.

To enable audit notification for an installation:

1. In the Audit Manager console, right-click the installation name, then select **Properties**.
2. Click the **Notification** tab.
3. Select **Enable notification**.

Deselect this option to turn off notification.

4. Click the browse button to locate and select a text file that contains the message you want to display.

A notification message is required if you select the Enable notification option. The contents of the file you select are displayed below the file location. The maximum text file size is 30 KB.

5. Click the browse button to locate and select an image to appear as a banner across the top of the audit notification.

Displaying a banner image is optional when you enable notification. The maximum image file size is 15 KB. For the best image display, use an image that is 468 pixels wide by 60 pixels high.

Note: Animated GIF files are not supported for use as audit notifications. If you do specify an animated GIF, the image displays as a static image.

6. Click **OK** or **Apply**.

Users will see the notification message the next time they log in.

7. If you enable notification after you have deployed agents, update the local policy on the audited computers by running the following command:

```
gpupdate /FORCE
```



Managing audit roles and auditors

Audit roles grant access to auditors to search, replay, and delete specific audited sessions using the Audit Analyzer console. Each audit role identifies a set of audited sessions, the list of auditors who have access to those sessions, and what the auditors in a specific role are allowed to do.

You identify a set of sessions by specifying criteria you want to use, for example, all sessions from a particular audited computer, associated with a specific application, or recorded during a specific period of time.

You identify the auditors for a set of sessions by specifying individual Active Directory users or Active Directory groups of auditors. If you use Active Directory groups, you can manage the privileges for all of the members of the group using your existing procedures for managing Active Directory groups. You can also configure the type of access granted to each member of the audit role.

You create and assign users and groups to audit roles using the Audit Manager console. You create the audit roles by right-clicking on the Audit Roles node. You add users and groups to an audit role by right-clicking on the specific role name.

Every installation automatically has a Master Auditor role. The Master Auditor has access to all audit data and permission to read, replay, update the review status, and delete sessions for the entire installation. The Master Auditor can also create roles, assign users, set permissions, and delegate administrative tasks for all of the audit stores in the installation. You cannot rename, delete, or modify permissions for the Master Auditor, but you can assign other users and groups to the Master Auditor role.

Granting permission to manage audit roles

The Master Auditor can grant the Manage Audit Role permission for an installation to one or more audit team leaders. The Manage Audit Role permission grants full control over all of the audit roles in the installation. An audit team leader can then create new roles, change the permissions specific audit roles grant, add or remove members, and remove roles.

When creating an audit role, an audit team leader defines the following:



- Target session type and optional other criteria.
- A collection of rights on the target sessions: Read, Update Status, Replay, and Delete.

For example, an audit team leader might define the following audit roles to control what different team members can do:

- A role named Windows Session Viewer for first level reviewers with a target of Windows sessions and only the right to Read session information. The members of the First Review group who are assigned to the Windows Session Viewer audit role can read, but not delete, replay or update the status of Windows sessions in the installation.
- A role named Incident Escalation for security managers with a target of Windows sessions from the last 72 hours, and permission to Read, Replay, and Update Status for the targeted session. The members of the Security group who are assigned to the Incident Escalation audit role can read, replay, and update the review status of Windows sessions from the previous 72 hours, but not delete any of the sessions they have reviewed.

Creating a new audit role

If you are the Master Auditor or have been granted the Manage Audit Role right, you can create new audit roles for your organization.

To create a new audit role:

1. Open Audit Manager.
2. Select Audit Roles, right-click, then click **Add Audit Role**.
3. Type a name and description for the new audit role, then click **Next**.
4. Select the type of session.
For example, select Windows session to limit this audit role to sessions captured by the Centrify agent for Windows.
5. Click **Add** to select additional criteria, such as time constraints, review status, or application used.

After you click Add, select an attribute and the appropriate criteria, then click **OK**. For example, if you select Time, you can then select specific date range or a period of time, such as the past 24 hours or this year.



6. Click **Execute Query** to test the criteria you have selected by examining the results the query returns.
7. Click **Close** to close the query results, then click **Next**.
8. Select the rights to allow for this role, then click **Next**.
9. Review your settings for this role, then click **Next**.

By default, the Assign Users and Groups to the Audit Role option is selected so that you can immediately begin populating the new audit role.

10. Click **Finish** to begin adding users and groups to the role.

Assigning users and groups to an audit role

If you selected the Assign Users and Groups to the Audit Role option at the end of the Add Audit Role wizard, the Assign Users and Groups to the Audit Role wizard opens automatically. You can also open the wizard at any time by right-clicking a specific audit role name in the Audit Manager console and choosing Assign Users and Groups.

To assign users and groups to an audit role:

1. Open Audit Manager.
2. Expand Audit Roles, and select a specific audit role name.
3. Right-click, then click **Assign Users and Groups**.
4. Type all or part of a name and click **OK**.

If there is more than one name that matches the criteria you specify, select the appropriate name from the names found, then click **OK**. A user or group can be a member of more than one audit role.

Delegating audit-related permissions

As the Master Auditor, you can delegate administrative tasks to other Active Directory users or groups. When you grant administrative rights to designated users and groups, you make them “trustees” with permission to perform specific operations. Because delegating administrative tasks to other users is a key part of managing an installation, it is covered in the next chapter.



However, one of the permissions you can delegate to other users and groups is the Manage Audit Role permission. With this permission, selected trustees can create, modify, and delete audit roles. For more information about delegating administrative tasks, see [Setting administrative permissions](#).

Modifying an audit role's properties

The Master Auditor and the audit roles you define are listed under Audit Roles in the Audit Manager console. Selecting a specific audit role name displays a list of members in the right pane. If you are the Master Auditor or been granted the Manage Audit Role permission, you can modify the properties for an audit role after you have created it by selecting the role in Audit Manager, right-clicking, then selecting Properties. For example, you can change the name or description of an audit role, specify the type of sessions members of the role can access, the privileges the audit role grants, and the users and groups who are assigned to the audit role.

How access roles and audit roles differ

Depending on whether you have enabled audit and monitoring service together with identity and privilege manager on an agent-managed computer, you might have two sets of roles or just one set of roles and the information captured and the activity allowed depends on the type of role being used.

Identity and privilege management only

If you have only enabled identity and privilege management on a computer and defined access roles:

- Users will not be able to log on if they are assigned to a role where is audit and monitoring service required.
- Users will be able to log on if they are assigned to a role where the audit if possible option is set. In this case, only identity and privilege management audit trail events are captured. For example, the agent records successful and failed logons and when users change from one role to another. Because audit and monitoring service is not enabled, the agent does not



capture a video record of all user activity. You also are not able to define audit roles to control who can read or delete audit trail records.

- Users will be able to log on if they are assigned to a role that does not require audit and monitoring service. In this case, only identity and privilege management audit trail events are captured.
- Auditors will not be able to review user activity on these computers. You also are not able to define audit roles to control who can read or delete audit trail records.

If no audit and monitoring service components are installed, you must use the Windows Event Viewer to search for and review audit trail events.

Auditing only

If you have enabled only audit and monitoring service on a computer and defined access roles:

- Users will be able to log on if they are assigned to a role where audit and monitoring service is required as long as the agent is running.
- Users will be able to log on if they are assigned to a role where the audit if possible option is set. In this case, logging on starts a video record of all user activity on the computer. Because identity and privilege management are not enabled, the user cannot select any access roles that provide desktop, application, or network access rights. The user cannot change roles so only the audit trail records successful and failed logons events.
- Users will be able to log on if they are assigned to a role that does not require audit and monitoring service. In this case, audit trail events are recorded, but no session activity is captured.
- Auditors will be able to review all or selected user activity on these computers, and you can define audit roles to control who has access to the captured user sessions based on the criteria you specify.

Identity and privilege management and auditing on the same computer

If you have enabled audit and monitoring service together with identity and privilege management on the same computer and defined access and audit



roles:

- Users will be able to log on if they are assigned to a role where audit and monitoring service is required as long as the agent is running. If the agent is stopped for any reason, the user will be allowed to log on only if also assigned a role with a rescue system right.
- Users will be able to log on if they are assigned to a role where the audit if possible option is set. If the audit and monitoring service service is active and you have enabled video capture auditing, both audit trail events and user activity are captured. For example, the agent records successful and failed logons and user activity when users change from one role to another. If the audit and monitoring service service is not enabled or not currently active, the agent does not capture a video record of all user activity.
- Users will be able to log on if they are assigned to a role that does not require audit and monitoring service. In this case, only audit trail events are captured.
- Auditors will be able to review user activity associated with specific roles on these computers, and you can define audit roles to control who has access to the captured user sessions based on the criteria you specify.



Managing auditing for an installation

This chapter describes how to secure and manage the audit and monitoring service infrastructure after the initial deployment of Centrify software on Windows computers. It includes tasks that are done by users assigned the Master Auditor role for an installation and users who are Microsoft SQL Server database administrators.

The following topics are covered:

| | |
|---------------------------------------------|-----|
| Securing an installation | 216 |
| Setting administrative permissions | 222 |
| Managing audit stores | 225 |
| Managing audit store databases | 227 |
| Managing the management database | 235 |
| Managing collectors | 237 |
| Managing audited computers and agents | 240 |
| Adding an installation | 242 |
| Removing or deleting an installation | 244 |

Securing an installation

For production deployments, you can take the following steps to secure an audit and monitoring service installation:

- Use the Installation group policy to specify which installation agents and collectors are part of. By enabling the Installation group policy you can



prevent local administrators from configuring a computer to be part of an unauthorized installation.

- Configure a trusted group of collectors to prevent a hacker from creating a rogue collector to collect data from agents.
- Configure a trusted group of agents to prevent a hacker from performing a Denial of Service attack on the collector and database by flooding a collector with false audit data.
- Encrypt all data sent from the collector to the database.

Before you can follow these steps to secure an installation, you must have access to an Active Directory user account with permission to create Active Directory security groups, enable group policies, and edit Group Policy Objects.

To secure an installation using Windows group policy:

1. Open the Group Policy Management console.
2. Expand the forest and domain to select the Default Domain Policy object.
3. Right-click, then click **Edit** to open Group Policy Management Editor.
4. Expand Computer Configuration > Policies > Centrify DirectAudit Settings, then select **Common Settings**.
5. Double-click the **Installation** policy in the right pane.
6. On the Policy tab, select **Enabled**.
7. Click **Browse** to select the installation you want to secure, then click **OK**.
8. Click **OK** to close the Installation properties.

Securing an audit store with trusted collectors and agents

By default, audit stores are configured to trust all audited computers and collectors in the installation. Trusting all computers by default makes it easier to deploy and test audit and monitoring service in an evaluation or demonstration environment. For a production environment, however, you should secure the audit store by explicitly defining the computers the audit store can trust.

You can define two lists of trusted computers:



- Audited computers that can be trusted.
- Collector computers that can be trusted.

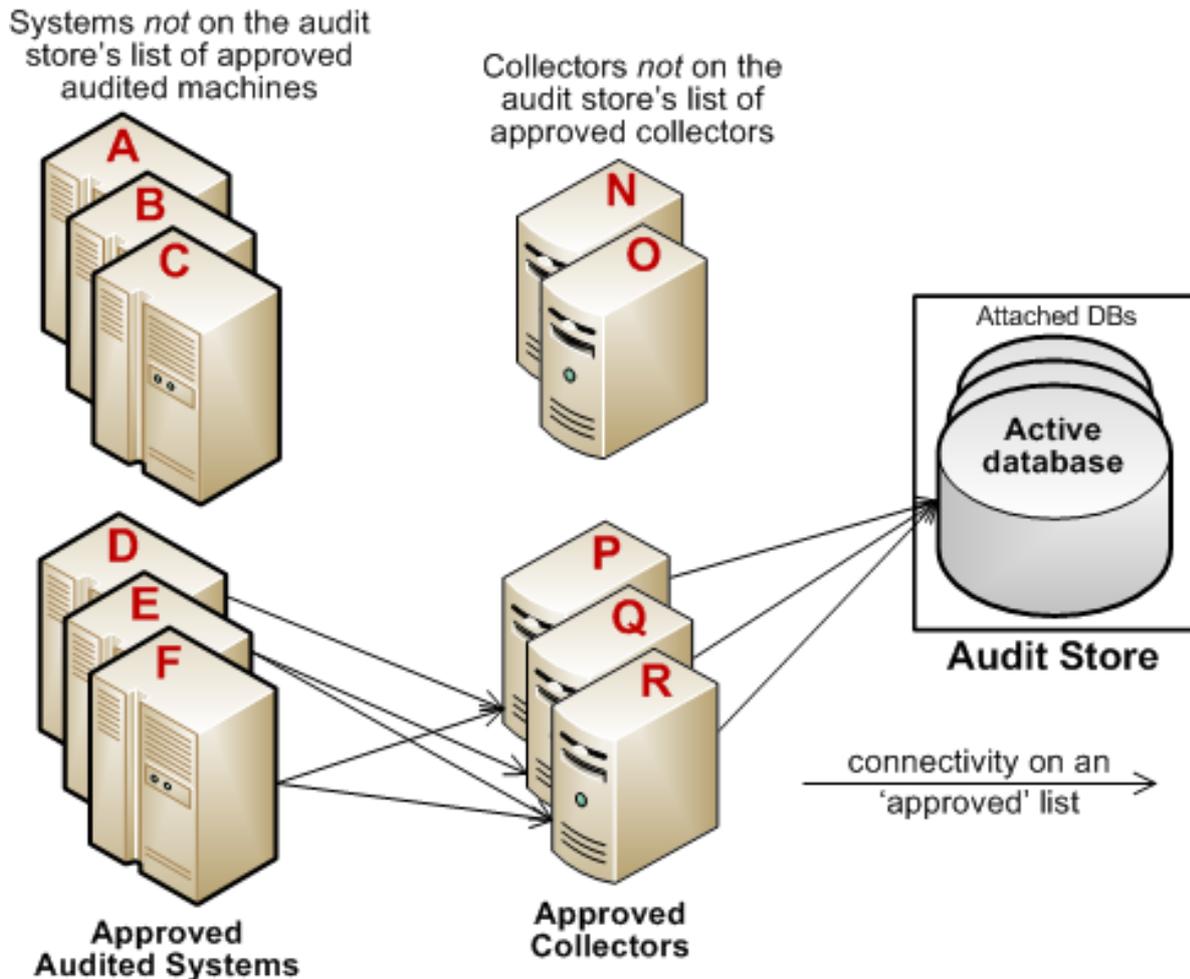
To secure an audit store:

1. Open the Audit Manager console.
2. Expand the installation and Audit Stores nodes.
3. Select the audit store you want to secure, right-click, then select **Properties**.
4. Click the **Advanced** tab.
5. Select **Define trusted Collector list**, then click **Add**.
6. Select a domain, click **OK**, then search for and select the collectors to trust and click **OK** to add the selected computers to the list.

Only the collectors you add to the trusted list are allowed to connect to the audit store database. All other collectors are considered untrusted and cannot write to the audit store database.
7. Select **Define trusted Audited System list**, then click **Add**.
8. Select a domain, click **OK**, then search for and select the audited computers to trust and click **OK** to add the selected computers to the list.

Only the audited computers you add to the trusted list are allowed to connect to the trusted collectors. All other computers are considered untrusted and cannot send audit data to trusted collectors.
9. Click **OK** to close the audit store properties dialog box.

The following example illustrates the configuration of trusted collectors and trusted audited computers.



In this example, the audit store trusts the computers represented by P, Q, and R. Those are the only computers that have been identified as trusted collectors in the audit store Properties list. The audit store has been configured to trust the audited computers represented by D, E, and F. As a result of this configuration:

- Audited computers D, E, and F only send audit data to the trusted collectors P, Q, and R.
- Trusted collectors P, Q, and R only accept audit data from the trusted audited computers D, E, and F.
- The audit store database only accepts data for its trusted collectors P, Q, and R, and therefore only stores audit data that originated on the trusted audited computers D, E, and F.

Disabling a trusted list

After you have added trusted collectors and audited computers to these lists, you can disable either one or both lists at any time to remove the security



restrictions. For example, if you decide to allow audit and monitoring service data from all audited computers, you can open the audit store properties, click the Advanced tab, and deselect the **Define trusted Audited System list** option. You don't have to remove any computers from the list. The audit store continues to only accept data from trusted collectors.

Using security groups to define trusted computers

You can use Active Directory security groups to manage trusted computer accounts. For example, if you create a group for trusted audited computers and a group for trusted collectors, you can use those groups to define the list of trusted collectors and audited computers for the audit store. Any time you add a new computer to one of those groups, thereafter, it is automatically trusted, without requiring any update to the audit store properties.

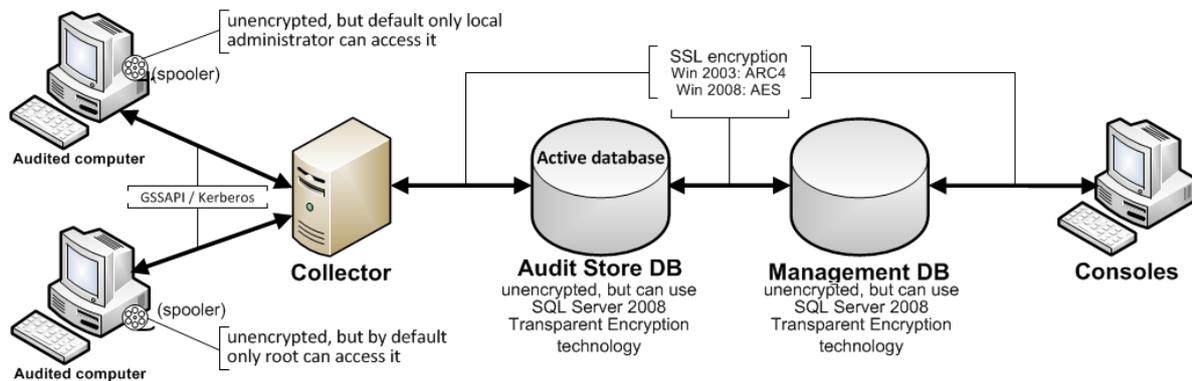
Securing network traffic with encryption

The last step in securing an installation is to secure the data collected and stored through encryption. The following summarizes how data is secured as it moves from component to component:

- Between an audited computer and the spooler that stores the data locally when no collectors are available, audit data is not encrypted. Only the local Administrator account can access the data by default.
- Between the audited computer's data collection service (wdad) and the collector, data is secured using Generic Security Services Application Program Interface (GSSAPI) with Kerberos encryption.
- Between the collector and the audit store database, data can be secured using Secure Socket Layer (SSL) connections and ARC4 (Windows 2003) or AES (Windows 2008) encryption if the database is configured to use SSL connections.
- Between the audit store and management databases, data can be secured using Secure Socket Layer (SSL) connections and ARC4 (Windows 2003) or AES (Windows 2008) encryption if the database is configured to use SSL connections.
- Between the management database and the Audit Manager console, data can be secured using Secure Socket Layer (SSL) connections and ARC4 (Windows 2003) or AES (Windows 2008) encryption if the database is configured to use SSL connections.



The following illustration summarizes the flow of data and how network traffic is secured from one component to the next.



Enabling Secure Socket Layer (SSL) communication

Although the database connections can be secured using SSL, you must configure SSL support for Microsoft SQL Server as part of SQL Server administration. You must also have valid certificates installed on clients and the database server. If you are not the database administrator, you should contact the database administrator to determine whether encryption has been enabled and appropriate certificates have been installed. For more information about enabling SSL encryption for SQL Server and installing the required certificates, see the following Microsoft support article:

<http://support.microsoft.com/kb/316898>

Enabling encryption for Microsoft SQL Server Express

If you use Microsoft SQL Server Express, encryption is turned off by default. To secure the data transferred to the database server, you should turn encryption on.

To enable encryption for each audit store and management database:

1. Log on to the computer hosting an audit store or management database with an account that has database administrator authority.
2. Open **SQL Server Configuration Manager**.
3. Select the SQL Server Network Configuration node, right-click **Protocols for DBINSTANCE**, then select **Properties**.
4. On the **Flags** tab, select **Yes** for the **Force Encryption** option, then click **OK** to save the setting.



Using a service account for Microsoft SQL Server

When you install Microsoft SQL Server, you specify whether to use Windows authentication or a mix of Windows and SQL Server authentication. You also specify the accounts that the database services should use. By default, system accounts are used. If SQL Server uses a domain user account instead of a system account, you should ensure that the account has permission to update the SQL Server computer object in Active Directory. If the account has permission to update the computer where SQL Server is running, SQL Server can publish its service principal name (SPN) automatically. Getting the correct service principal name is important because Windows authentication relies on the SPN to find services and DirectManage Audit uses Windows authentication for console-to-audit management database connections. If the SPN is not found, the connection between the console and audit management database fails.

The audit management database-to-audit store connection and the collector-to-audit store connection can use either Windows authentication or SQL Server authentication. If SQL Server authentication is used, it does not matter whether the SQL Server instance uses a system account or a service account. If you have configured SQL Server to use Windows authentication only, be sure that the Windows account is allowed to connect to the audit management database and to the audit store database.

Setting administrative permissions

When you create a new installation, you become the primary administrator for that installation. As the primary administrator and Master Auditor, you have full control over the entire installation and the ability to delegate administrative tasks to any other Active Directory user or group. When you grant administrative rights to designated users and groups, you make them “trustees” with permission to perform specific operations. You can set granular permissions to tightly control what specific users can do or grant broad authority over operations in an installation.

If you have a large or widely-distributed installation, you can also install additional Audit Manager and Audit Analyzer consoles for the users who have been delegated administrative tasks to use.



To delegate administrative tasks to other users:

1. Open Audit Manager.
2. Select the installation name, right-click, then click **Properties**.
3. Click the **Security** tab to delegate administrative tasks for the entire installation.
4. Click **Add** to add Active Directory users or groups to the list of trustees who granted any type of rights on this installation.
5. Select a user or group listed, then select the appropriate rights for that trustee, then click **OK**.

The following table lists the rights available.

| Select this permission | To grant these rights to a trustee |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full Control | <ul style="list-style-type: none">■ All operations on the selected installation. |
| Change Permissions | <ul style="list-style-type: none">■ Add or remove users and groups as trustees for the installation.■ Modify permissions for trustees on the selected installation. |
| Modify Name | <ul style="list-style-type: none">■ Modify display name for the selected installation. |
| Manage Management Database List | <ul style="list-style-type: none">■ Add or remove management databases for the selected installation. |
| Manage Audit Store List | <ul style="list-style-type: none">■ Add or remove audit stores for the selected installation. |
| Manage Collectors | <ul style="list-style-type: none">■ Enable a trusted group of collectors for this audit store.■ Add a collector to the trusted group of collector in this audit store.■ Remove collector from the trusted collectors in this audit store.■ Remove disconnected collector records from this audit store. |



| Select this permission | To grant these rights to a trustee |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manage Audited Systems | <ul style="list-style-type: none">■ Enable trusted group of audited computers for this audit store.■ Add a computer to the trusted group of audited computers in this audit store.■ Remove a computer from the trusted group of audited computers in this audit store.■ Remove disconnected audited computer records from this audit store. |
| Manage Audit Role | <ul style="list-style-type: none">■ Add, modify, or remove audit roles in the selected installation.■ Assign users and groups to audit roles.■ Remove users and groups from roles. |
| Manage Queries | <ul style="list-style-type: none">■ Add, modify, or remove queries in the selected installation. |
| Manage Publications | <ul style="list-style-type: none">■ Add or remove publication locations for the selected installation. |
| Manage Licenses | <ul style="list-style-type: none">■ Add or remove license keys for the selected installation. |
| Modify Notification | <ul style="list-style-type: none">■ Enable or disable audit notification in the selected installation.■ Select the notification message.■ Select a banner image. |
| Modify Audit Options | <ul style="list-style-type: none">■ Enable or disable the option to capture video of all user activity on audited computers.■ Control whether users are allowed to update the review status of their own sessions.■ Control whether users are allowed to delete their own sessions. |
| View | <ul style="list-style-type: none">■ Enable to view audited computers and sessions. |

6. Click **OK** to complete the delegation of administrative rights for the selected installation.

You can also delegate administrative tasks for individual audit stores and management databases, and set permissions on audit roles. For information about delegating administrative tasks for audit stores, see [Configuring permissions for an audit store](#). For information about delegating administrative tasks for management databases, see [Configuring permissions for the management database](#).



For information about setting permissions on audit roles, see [Managing audit roles and auditors](#).

Managing audit stores

An audit store defines a set of Active Directory sites or subnets and a collection of databases that contain audit data. Typically, an installation has one audit store with multiple databases. However, you can add audit stores if you are auditing computers in a large and widely distributed network or have multiple Active Directory sites with computers you want to audit.

Configuring the scope of an audit store

In most organizations, a single audit store is used to map to an Active Directory site. However, there are situations where you might want to define the scope of an audit store based on subnets. For example:

- If you have a subnet that Active Directory considers part of a site that is connected over a slow link you might want to configure a separate audit store and collectors that service audited computers in the remote subnet.
- If you have very large Active Directory site, you might require multiple audit stores for load distribution. You can accomplish this by partitioning an Active Directory site into multiple audit stores based on subnets. Each subnet has its own audit store, set of collectors, and audited computers.

You can configure the scope of an audit store by adding or removing Active Directory sites or subnets.

To configure the scope for an audit store:

1. Open Audit Manager.
2. Expand the installation node, then expand Audit Stores and select a specific audit store name.
3. Right-click, then select **Properties**.
4. Click the **Scope** tab.
5. Click **Add Site** to select an Active Directory site from the list of sites found or click **Add Subnet** to type a specific subnet address and mask.



Configuring permissions for an audit store

If you are the Master Auditor or have Change Permission rights, you can modify the rights granted to Active Directory users or groups. When you enable rights for designated users and groups, you make them “trustees” with permission to perform specific operations.

To configure permissions for managing the audit store:

1. Open Audit Manager.
2. Expand the installation node, then expand Audit Stores and select a specific audit store name.
3. Right-click, then select **Properties**.
4. Click the **Security** tab.
5. Click **Add** to add Active Directory users or groups to the list of trustees who granted any type of rights on this audit store.
6. Select a user or group listed, then select the appropriate rights for that trustee, then click **OK**.

The following table lists the rights available.

| Select this permission | To grant these rights to a trustee |
|------------------------|-----------------------------------------------------------------------------------|
| Full Control | ■ All operations on the audit store. |
| Change Permissions | ■ Modify permissions on this audit store. |
| Modify Name | ■ Modify display name for this audit store. |
| Manage Scopes | ■ Add a subnet or Active Directory site to the audit store. |
| | ■ Remove a subnet or Active Directory site from the audit store. |
| Manage SQL Logins | ■ Set the allowed incoming collectors for this audit store's databases. |
| | ■ Set the allowed incoming management databases for this audit store's databases. |



| Select this permission | To grant these rights to a trustee |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manage Collectors | <ul style="list-style-type: none">■ Enable a trusted group of collectors for this audit store.■ Add a collector to the trusted group of collector in this audit store.■ Remove collector from the trusted collectors in this audit store.■ Remove disconnected collector records from this audit store. |
| Manage Audited Systems | <ul style="list-style-type: none">■ Enable trusted group of audited computers for this audit store.■ Add a computer to the trusted group of audited computers in this audit store.■ Remove a computer from the trusted group of audited computers in this audit store.■ Remove disconnected audited computer records from this audit store. |
| Manage Databases | <ul style="list-style-type: none">■ Add audit store databases to this audit store.■ Attach audit store databases to this audit store.■ Detach an audit store database from this audit store.■ Change the active database in this audit store.■ Modify the display name of an audit store database. |
| Manage Database Trace | <ul style="list-style-type: none">■ Enable or disable database trace.■ Export database trace. |

Managing audit store databases

During the initial deployment, your installation only has one audit store database. As you begin collecting audit data, however, that database can quickly increase in size and degrade performance. Over time, an installation typically requires several Microsoft SQL Server databases to store the data being captured and historical records of session activity, login and role change events, and other information. As part of managing an installation, you must manage these databases to prevent overloading any one database and to avoid corrupting or losing data that you want to keep.

One of the biggest challenges in preparing and managing Microsoft SQL Server databases for storing audit data is that it is difficult to estimate the level of activity and how much data will need to be stored. There are several factors to



consider that affect how you configure Microsoft SQL Server databases for auditing data, including the recovery method, memory allocation, and your backup and archiving policies.

For more complete information about managing and configuring SQL Server, however, you should refer to your Microsoft SQL Server documentation.

Selecting a recovery model

Standard backup and restore procedures come in three recovery models:

- **Simple**—The simple recovery model allows high-performance bulk copy operations, minimizes the disk space required, and requires the least administration. The simple recovery model does not provide transaction log backups, so you can only recover data to the point of the most recent full or differential backup. The default recovery model is simple, but is not appropriate in cases where the loss of recent changes is not acceptable.
- **Full**—The full recovery model has no work-loss exposure, limits log loss to changes since the most recent log backup, and provides recovery to an arbitrary time point. However, the full recovery model uses much more disk space.
- **Bulk-logged**—The bulk-logged recovery model provides higher performance and minimizes the log space used by disk-intensive operations, such as create index or bulk copy. With the bulk-logged recovery model, you can only recover data to the point of the most recent full or differential backup. However, because most databases undergo periods of bulk loading or index creation, you can switch between bulk-logged and full recovery models to minimize the disk space used to log bulk operations.

When a database is created, it has the same recovery model as the **model** database. Although the simple recovery model is the default, the full and bulk-logged recovery models provide the greatest protection for data, and the full recovery model provides the most flexibility for recovering databases to an earlier point in time. To change the recovery model for a database, use the ALTER DATABASE statement with a RECOVERY clause.

Regardless of the recovery model you choose, you should keep in mind that backup, restore, and archive operations involve heavy disk I/O activity. You should schedule these operations to take place in off-peak hours. If you use the simple recovery model, you should set the backup schedule



long enough to prevent backup operations from affecting production work, but short enough to prevent the loss of significant amounts of data.

Configuring the maximum memory for audit store databases

Because Microsoft SQL Server uses physical memory to hold database information for fast query results, you should use a dedicated instance to store auditing data. Because SQL Server dynamically acquires memory whenever it needs it until it reaches the maximum server memory you have configured, you should set constraints on how much physical memory it should be allowed to consume.

The maximum server memory (`max server memory`) setting controls the maximum amount of physical memory that can be consumed by the Microsoft SQL Server buffer pool. The default value for this setting is such a high number that the default maximum server memory is virtually unlimited. Because of this default value, SQL Server will try to consume as much memory as possible to improve query performance by caching data in memory.

Processes that run outside SQL Server, such as operating system processes, thread stacks, socket connections and Common Language Runtime (CLR) stored procedures are not allowed to use the memory allocated to the Microsoft SQL Server buffer pool. Because those other processes can only use the remaining available memory, they might not have enough physical memory to perform their operations. In most casts, the lack of physical memory forces the operating system to read and write to disk frequently and reduces overall performance.

To prevent Microsoft SQL Server from consuming too much memory, you can use the following formula to determine the recommended maximum server memory:

- Reserve 4GB from the first 16GB of RAM and then 1GB from each additional 8GB of RAM for the operating system and other applications.
- Configure the remaining memory as the maximum server memory allocated for the Microsoft SQL Server buffer pool.

For example, if the computer hosting the Microsoft SQL Server instance has 32GB of total physical memory, you would reserve 4 GB (from first 16 GB) + 1GB (from next 8 GB) + 1 GB (from next 8 GB) for the operating system, then set the Maximum server memory for Microsoft SQL server to 26 GB (32 GB – 4 GB – 1 GB – 1 GB = 26).



For more information about how to configure Microsoft SQL Server maximum memory setting and other memory options, see the following Microsoft article: [https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms178067\(v=sql.105\)](https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms178067(v=sql.105))

You should configure the maximum memory allowed for the Microsoft SQL Server instances hosting audit store databases and the management database. However, this setting is especially important to configure on the Microsoft SQL Server instance hosting the active audit store database.

Using Transact-SQL to configure minimum and maximum memory

You can control the minimum and maximum memory that the SQL Server buffer manager uses by issuing Transact-SQL commands. For example:

```
sp_configure 'show advanced options', 1
reconfigure
go
sp_configure 'min server memory', 60
reconfigure
go
sp_configure 'max server memory', 100
reconfigure
go
```

For more information about configuring SQL Server and setting minimum and maximum server memory using T-SQL, see <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-memory-server-configuration-options?view=sql-server-2017>

Estimating database requirements based on the data you collect

To determine how audit and monitoring service will affect database capacity, you should monitor a pilot deployment of 20 to 25 agents with representative activity to see how much data is produced daily. For example, some audited computers might have few interactive user sessions or only short periods of activity. Other audited computers might have many interactive user sessions or long sessions of activity on average.

During the pilot deployment, you want to the following information:



- How many interactive user sessions occur daily on each computer?
- How long do sessions last on average?
- What are the activities being captured, and what is the average size of each session being captured?
- How long do you need to store the captured data to balance performance and storage?
- What is the data retention period for audited data?

From the information you collect in the pilot deployment and the data retention policy for your organization, you can estimate the database size using the following guideline:

$$(\text{number of agents}) \times (\text{number of sessions per agent}) \times (\text{average data size per session}) \times (\text{retention days})$$

Results in the estimated size of the Microsoft SQL Server database for the number of days in the retention policy

For example, if an average session generated 100 KB in the database and the installation had 250 agents, 10 sessions per agent, and a six-month retention period (about 130 working days), the storage requirement for the audit store database would be 36.9 GB:

$$250 \text{ agents} \times 10 \text{ sessions/agent each day} \times 100 \text{ KB/session} \times 130 \text{ days} = 32,500,000 \text{ KB}$$

The following table shows examples of the data storage requirement in an installation with Windows agents, typical levels of activity with an average of one session per day on each audited computer, and the recovery mode set to Simple:

| Agents | Average session length | Average session size | Daily | Weekly | 6 Months |
|--------|------------------------|--------------------------|--------|---------|----------|
| 100 | 20 minutes | 806 KB - low activity | 79 MB | 394 MB | 10 GB |
| 50 | 25 minutes | 11.56 MB - high activity | 578 MB | 2.81 GB | 73.36 GB |
| 100 | 20 minutes | 9.05 MB - high activity | 905 MB | 4.42 GB | 115 GB |

In this example, an installation with 100 Windows agents with low activity would require approximately 10 GB for the audit store database to keep audit data for 6 months. An increase in the number of interactive sessions, session length, or average session size would increase the database storage required.

If SQL Server requires more space to accommodate the new data, it expands the database file immediately, which can cause degraded performance. To reduce the effect of database expansion on performance, allocate sufficient



space to support database growth. In addition, monitor database space and when space is low, schedule a database expand operation for an off-peak time.

Adding new audit store databases to an installation

When you first set up an installation, you also create the first audit store and audit store database. By default, that first database is the active database. As you begin collecting audit data, you might want to add databases to the audit store to support a rolling data retention policy and to prevent any one database from becoming a bottleneck and degrading performance.

Only one database can be the active database in an audit store at any given time. The computer hosting the active database should be optimized for read/write performance. As you add databases, you can change the older database from active to attached. Attached databases are only used for querying stored information and can use lower cost storage options.

Note: A single instance of Microsoft SQL Server can host multiple databases.

Audit store databases have the following characteristics:

- A database can be active, attached, or detached.
- Only one database can be actively receiving audit data from collectors.
- A database cannot be detached while it is the active database.
- A database that was previously the active database cannot again be the active database.
- If a detached database contains parts of sessions presented to the Audit Analyzer, a warning is displayed when the auditor replays those sessions.

Rotating the active database

Database rotation is a management policy to help you control the size of the audit store database and the performance of database operations. There are several reasons to do database rotation:

- It is more difficult to manage one large database than multiple small databases.



- Performance is better with multiple small databases.
- Backing up, restoring, archiving, and deleting data all take significantly more time if you work with one large database.
- Database operations take very little time when you work with multiple small databases.

For audit and monitoring service, you can implement a database rotation policy by having the collector write data to a new database after a certain period of time. For example, the collector in site A writes data to the database `siteA-2014-11` in November, then write data to database `siteA-2014-12` in December and to the database `siteA-2015-01` in January. By rotating from one active database to another, each database stays more compact and manageable.

Creating a new database for rotation

You can rotate from one active database to another at any time using the Audit Manager console.

To create a new database for rotation:

1. Open Audit Manager.
2. Expand the installation node, then expand Audit Stores and a specific audit store name.
3. Select Databases, right-click, then select **Add Audit Store Database** to create a new database.
4. Select the **Set as Active database** option so collectors start writing to the newly created database.

It is possible to write a script to automate the database rotation process. For details, see the SDK documentation.

Database archiving

To implement periodic archiving, add a new active database, leave one or more previous databases attached, and take the oldest database off-line for archiving.



Queries during rotation and archiving

If the database backup program supports online backup, the Audit Analyzer can still query the database while the backup is in progress. However, the backup program may block updates to the session review status. If the backup program does not support online backup, the database will be offline until the backup is complete.

Database backups

You can back up a database whether it is attached to the audit store or detached from the audit store.

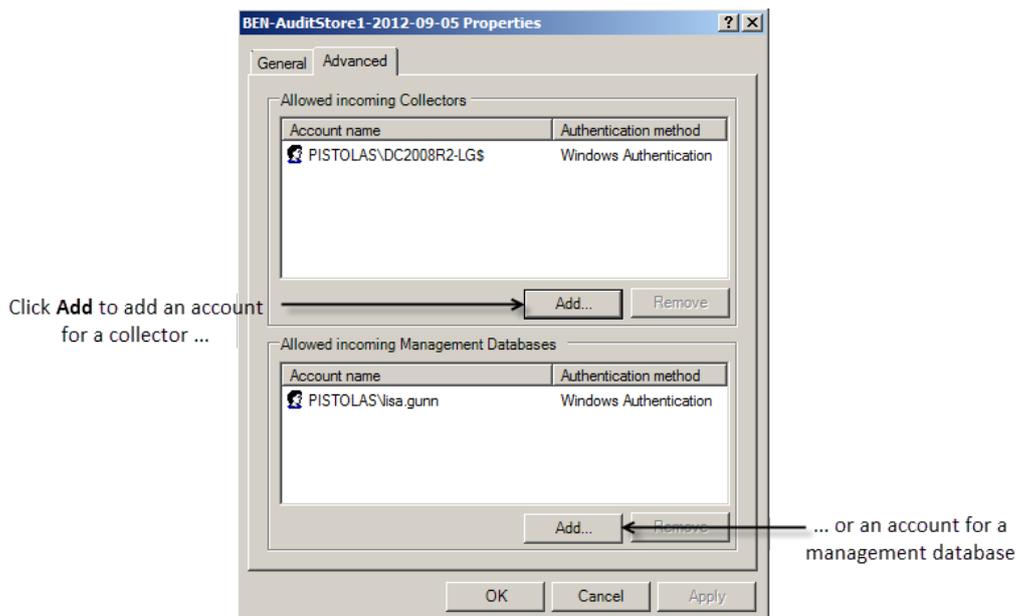
Allowed incoming accounts

You can specify the accounts that are allowed to access the audit store database. By configuring these accounts, you can control which collector computers can connect to the audit store database and which management databases have access to the data stored in the audit store database.

Your account must have Manage SQL Login permission to configure the incoming accounts.

To configure allowed accounts:

1. Open Audit Manager.
2. Expand the installation node, then expand Audit Stores and select a specific audit store name.
3. Select a database under the audit store, right-click, then select **Properties**.
4. Click the **Advanced** tab.
5. Click **Add** to add a collector or management database account. For example:



6. Select an authentication type.
 - If you select Windows authentication, you can browse to select a computer, user, or group to add.
 - If you select SQL Server authentication, you can select an existing SQL Server login or create a new login.

Connections should use Windows authentication whenever possible. However, computers in an untrusted forest cannot connect to an audit management database using Windows authentication. To allow connections from an untrusted forest, add a SQL Server login account as the incoming account for the management database.

Managing the management database

The audit management database keeps track of where components are installed and information about the installation. To connect to the database or manage its properties, select a specific installation name in Audit Manager, right-click, then select **Management Databases**.

Configuring the scope of the management database

The audit management database stores information about the set of Active Directory sites or subnets it supports. You can modify the scope of the management database if you are auditing computers in a large and widely



distributed network or have multiple Active Directory sites with computers you want to audit.

To configure the scope for a management database:

1. Open Audit Manager.
2. Select the installation name, right-click, then select **Management Database**.
3. Click **Properties**, then click the **Scope** tab.
4. Click **Add Site** to select an Active Directory site from the list of sites found or click **Add Subnet** to type a specific subnet address and mask.

Configuring permissions for the management database

If you are the Master Auditor or have Change Permission rights, you can modify the rights granted to Active Directory users or groups. When you enable rights for designated users and groups, you make them “trustees” with permission to perform specific operations.

To configure audit store security:

1. Open Audit Manager.
2. Select the installation name, right-click, then select **Management Database**.
3. Click **Properties**.
4. Click the **Security** tab.
5. Click **Add** to add Active Directory users or groups to the list of trustees who granted any type of rights on this management database.
6. Select a user or group listed, then select the appropriate rights for that trustee, then click **OK**.

The following table lists the rights available.



| Select this permission | To grant these rights to a trustee |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full Control | <ul style="list-style-type: none">■ All operations on the management database. |
| Change Permissions | <ul style="list-style-type: none">■ Modify permissions on the management database. |
| Modify Name | <ul style="list-style-type: none">■ Modify display name for this management database. |
| Manage Scopes | <ul style="list-style-type: none">■ Add a subnet or Active Directory site to the management database.■ Remove a subnet or Active Directory site from the management database. |
| Manage SQL Logins | <ul style="list-style-type: none">■ Set the allowed incoming accounts for the management database. <i>Database owner is by definition an allowed user.</i>■ Set the outgoing account for the management database. |
| Remove Database | <ul style="list-style-type: none">■ Remove this audit management database from the installation. |
| Manage Database Trace | <ul style="list-style-type: none">■ Enable or disable database trace.■ Export database trace. |

Managing collectors

You can view information about the collectors you have deployed in the Audit Manager console. For example, for each collector, you can see the location of the collector on the network, whether the collector is connected to or disconnected from the audit store, and how long a connected collector has been running since it was last restarted, the audit store to which the collector is assigned, and the active database to which the collector is currently sending audit data. You can also see the audited computers that currently connected to each collector and the audited computers that are not currently connected to this collector.

If you install the collector service on a computer but it has never connected to any agents or audit stores, it is not included in collector list on the Audit Manager console.

Monitoring collector status locally

In addition to the information available in the Audit Manager console, the Windows computers on which you have installed a collector provide a local

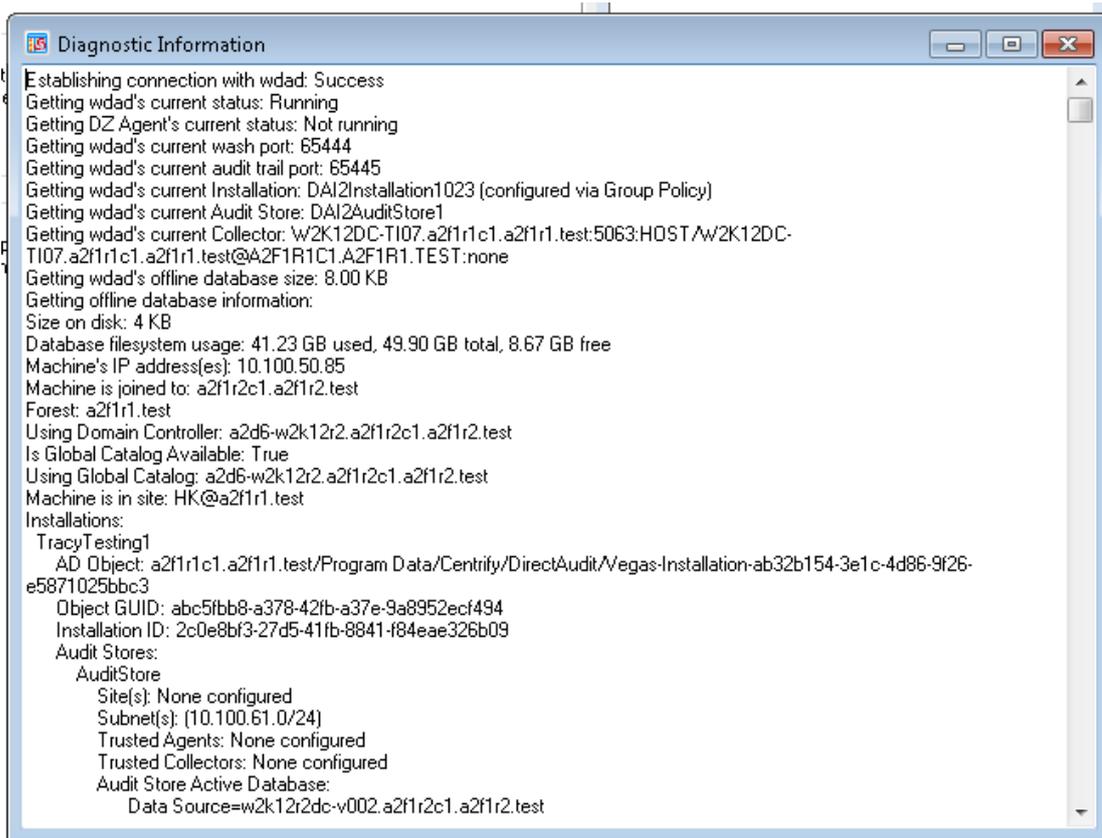


Collector Control Panel applet. The Collector Control Panel displays information about current connectivity and status for the local collector. You can use the control panel to configure the collector port number, installation, and authentication type if you want to make changes after the initial deployment. You can also use the control panel to start, stop, or restart the collector service, and to generate diagnostic information about the collector.

1. Log on to the computer on which you have installed a collector.
2. In the list of applications on the Windows Start menu, click **Audit Collector Control Panel** to open the audit collector control panel.
3. On the General tab, click **Configure** to change the port number, installation, or type of authentication to use when connecting to the audit store.

The General tab also displays current configuration and status for the local collector service. If you make changes, the new information is displayed after a short period of time.

4. Click **Stop** if you want to temporarily stop a running service, or **Restart** if you want to stop and immediately restart a running collector service.
5. Click the Troubleshooting tab, then click **Diagnostics** to generate diagnostic information about the installation the collector is part of, the Active Directory site or subnets associated with the audit store the collector connects to, the collector status, and other information. For example:



After you generate diagnostic information, you can right-click to select all of the text. With the text selected, right-click, and select Copy to copy and paste the diagnostic report into a text file.

6. Click **Options** to specify the level of detail to include in the log file or to turn off logging.

The default log level reports informational messages, warnings, and errors. You can click **View Log** to see information in the current log file.

7. Click **Close** to return to the agent configuration panel.

Removing collectors

If you want to remove a collector, you can use the Programs and Features > **Uninstall a program** control panel or the setup program you used to install the collector.

If you run the setup program, select the collector from the list of components, then click Next. Because a collector is installed, the wizard prompts you the Change, Repair or Remove the collector. Click **Remove**.



Managing audited computers and agents

You can see information about audited computers and the audit and monitoring service status of Centrify agents for Windows using the Audit Manager console. For example, for each audited computer, you can see the computer name and IP address, whether the audited agent is currently connected or disconnected, and how long the agent has been running since it was last restarted. You can also see the collector to which the agent is sending data and the audit store and audit store database where the audit data is stored.

Monitoring agent status locally

In addition to the information available in the Audit Manager console, the Windows computers on which you have installed a Centrify agent for Windows with audit and monitoring service enabled include a local agent configuration panel applet. The agent configuration panel displays information about current connectivity and status for the local agent. You can use the agent configuration panel to configure the color depth, offline storage, or installation if you want to make changes after the initial deployment. You can also use the agent configuration panel to generate diagnostic information about the agent.

To use the agent configuration panel:

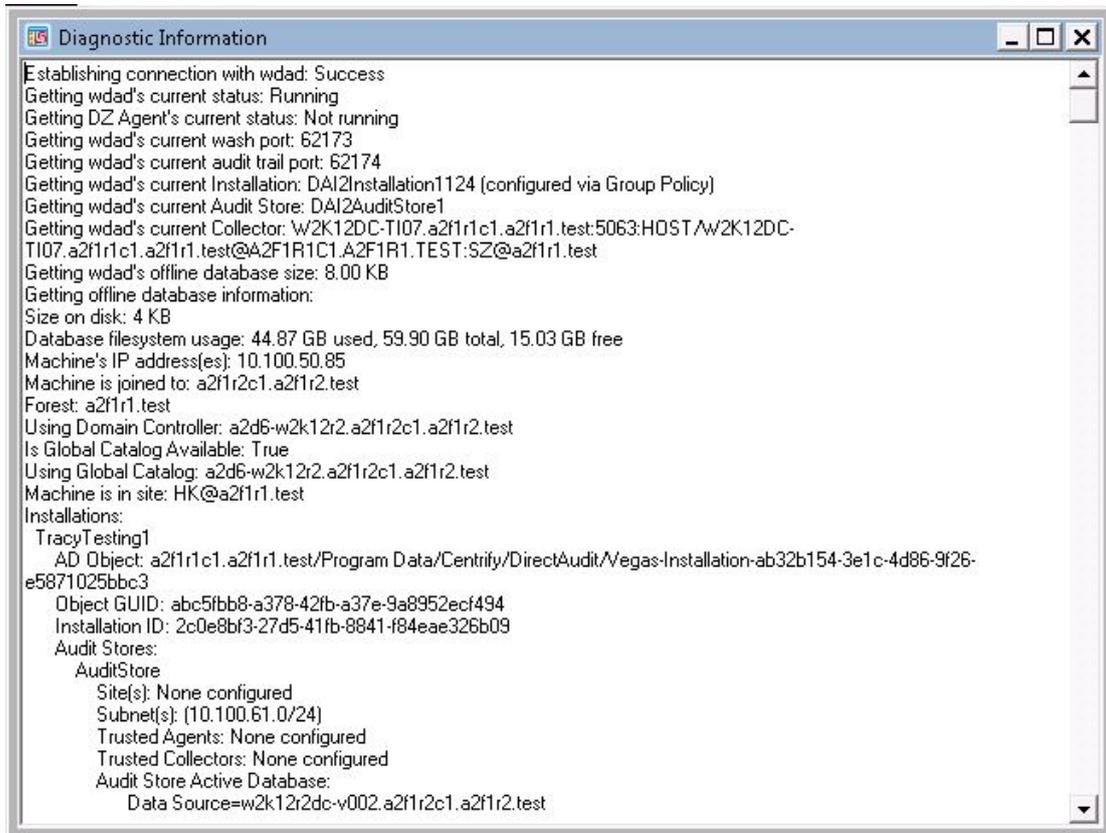
1. Log on to the computer on which you have installed a Centrify agent for Windows with audit and monitoring service enabled.
2. In the list of applications on the Windows Start menu, click **Agent Configuration** to open the agent configuration panel.
3. Click **Centrify Auditing and Monitoring Service**.
4. Click **Settings**.
5. On the General tab, click **Configure** to change the color depth, offline storage file location and maximum size, and the installation to use for the local agent.

Note: The offline storage location should be an empty folder. If you select a folder that contains any files other than the spooled audit data, those files may be moved or lost.



The General tab also displays current configuration and status for the local agent. If you make changes to the configuration, the new information is displayed after a short period of time. If the agent cannot connect to any collector, it spools audit data to the offline data location. When it finds a collector, the agent sends the spooled data to it. The offline storage space is not reclaimed until all of the spooled data has been sent to a collector.

6. Click the Troubleshooting tab, then click **Diagnostics** to generate diagnostic information about the installation the agent is part of, the collector the agent sends data to, the size of offline storage, and other information. For example:



After you generate diagnostic information, you can right-click to select all of the text. With the text selected, right-click, and select Copy to copy and paste the diagnostic report into a text file.

7. Click **Options** to specify the level of detail to include in the log file or to turn off logging.

The default log level reports informational messages, warnings, and errors. You can click **View Log** to see information in the current log file.

8. Click **Close** to return to the agent configuration panel.



Setting the color depth for captured sessions

Because audit and monitoring service 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 also increases the CPU overhead on audited computers but improves resolution when the session is played back. A lower color depth decreases the amount of data sent across the network and stored in the database. In most cases, the recommended color depth is medium (16 bit). The CPU and storage estimates in this guide are based on a medium (16 bit) color depth.

To change the color depth for captured sessions:

1. Log on to the computer where the Centrify agent for Windows is installed.
2. In the list of applications on the Windows Start menu, click **Agent Configuration** to open the agent configuration panel.
3. Click **Centrify Auditing and Monitoring Service**.
4. Click **Settings**.
5. On the General tab, click **Configure**
6. Select the maximum color quality for recorded sessions, then click **Next**.
7. Follow the prompts displayed to change any other configuration settings.

Removing an audited computer

If an audited computer has been removed from the installation, the audited computer will continue to be listed on the Audit Manager console as **Disconnected**. To remove the decommissioned audited computer, select **Delete** from its context menu.

Adding an installation

Although a single installation is the most common deployment scenario, you can configure multiple installations. For example, you can use separate installations to provide concurrent production and test-bed deployments or to support multiple administrative domains within your organization.



To create a new installation:

1. Open Audit Manager.
2. Select the root node, right-click, then select **New Installation**.
3. Follow the prompts displayed.
The steps are the same as the first installation. For more information, see [Creating a new installation](#).
4. Choose the appropriate installation for each collector using the Collector Configuration wizard.
5. Choose the appropriate installation for each agent using the Agent Configuration wizard.

Delegating administrative tasks for a new installation

The account you use to create a new installation is the default administrator and Master Auditor with full control over the entire installation and the ability to delegate administration tasks to other Active Directory users or groups. You can grant permission to perform administrative tasks to other users by opening the Properties for each component, then clicking the Security tab.

Opening an installation in a new console

If you create multiple installations at the same site, you can select the installation name, right-click, then select **New Window From Here** to keep consoles for different installations separate from each other. Creating a new window for each installation can help you avoid performing operations on one installation that you intended to perform on another.

Closing an installation

The Audit Manager console allows you to manage multiple installations. To remove the current installation from the console, but not physically remove the database or the information published to Active Directory, you can select the installation name, right-click, then select **Close**.



Publishing installation information

DirectManage Audit publishes installation information to a service connection point (SCP) object in Active Directory so that audited computers and collectors can look up the information. If the published locations for multiple SCPs in the same installation are not the same, or if collectors cannot read from at least one of the published locations, the collectors are unable to determine which audit store is the best match for the sites and subnets, and so they do not attempt to connect to an audit store.

Permission to publish to Active Directory

Only administrators who have been delegated permission to modify various attributes of the installation can publish those attributes to Active Directory.

If you do not have Active Directory permission to modify the installation, the updates are kept in the audit management database, and a message is issued to notify you that the installation information could not be updated in Active Directory.

Synchronizing installation information

If you have an Active Directory account with permission to publish information about the installation, you can update the service connection point.

To publish the service connection point for an installation:

1. Open Audit Manager.
2. Select the installation name, right-click, then click **Properties**.
3. Click the **Publication** tab, then click **Synchronize** to publish the information.

In a multi-forest or DMZ environment, this tab lists multiple Active Directory locations to which to publish.

4. Click **OK** to close the installation properties.

Removing or deleting an installation

Before you can remove or delete an installation, you must do the following:



- Run the setup program to remove all agents and collectors and collector service connection points (SCPs).
- Detach and remove all audit store databases.
- Open the Installation Properties and click the **Publications** tab to make sure only one installation service connection point (SCP) is listed.

Note: To remove service connection points on other sites, contact an administrator with publication permission on those sites.

To remove or delete an installation, select the installation in the Audit Manager console, right-click, then select **Remove** to open the Remove installation dialog box.

- Click **Remove** to remove the installation but not delete the management database from the SQL Server instance.
- Click **Delete** to remove the installation and delete the management database from the installation of SQL Server.

Note: All the publications published to Active Directory are removed when you remove or delete an installation.



Troubleshooting and common questions

Centrify includes diagnostic tools and log files to help you trace the source of problems if they occur. Diagnostic reports and log files allow you to periodically check for issues and view information about operations on the computers you manage. The information is useful for troubleshooting and in resolving cases with the help of Centrify Support.

This chapter describes how to 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 and authentication, privilege elevation, and audit and monitoring services components. This chapter also covers common questions to help you identify and correct problems on the computers you manage.

The following topics are covered:

| | |
|--------------------------------------------------------------------------|-----|
| Solving problems with logging on | 247 |
| Accessing network computers with privileges | 248 |
| Refreshing cached information on managed computers | 249 |
| Analyzing information in Active Directory | 249 |
| Running diagnostics and viewing logs for the agent | 251 |
| Enabling detailed logging for audit and monitoring service components .. | 255 |
| Tracking database activity | 258 |
| Controlling audit trail events | 261 |
| Offline MFA profile authentication | 263 |
| Centrify Authentication Service known issues | 263 |



Solving problems with logging on

After you have installed the Centrify agent for Windows and joined the computer to a domain, users cannot log on without a role assignment. The role, however, can be assigned to a local account or a domain account, or the role can be assigned the right to access a remote computer. Consequently, users might encounter problems logging on after the agent is deployed. For example, you might find that users can log on to the computer using a local account but cannot log on using their domain account or have trouble connecting to a remote server.

If users report problems logging on, there are some things you can try to troubleshoot the issue:

- Check the logon rights for the affected users.
To do this, log on as an administrator and execute `dzinfo user-name` (where *user-name* is the name of the user experiencing problems logging on). You can also check user logon rights using the Authorization Center.
- 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 users cannot log on to a remote computer, confirm that they have a role that has the remote logon system right and that the computer itself is configured to allow users to log on remotely. Open the Authorization Center to review the list of roles and their associated rights for any user.
- Check the computer's local security policy or applied group policies to verify whether the user is allowed to log on interactively or through a remote desktop connection. For example, most domain users are not allowed to log on locally on domain controllers.

Depending on how your organization has configured native Windows security policies, users might need to be members of a specific Windows security group—such as Server Operators or Remote Desktop Users—to log on to specific computers locally or remotely even if they have been granted access rights using the Windows Login role or a custom role definition.



- Check to see whether the computer is in Rescue mode.

In Rescue mode, access to a computer is granted only to users who have Rescue rights. For information about adding Rescue rights to a role, see [System rights allow users to log on](#). In general, a computer enters Rescue mode because the Windows agent authorization service has stopped. Possible causes include the following:

- The computer is not connected and the local authorization cache has not been initialized or is corrupt.
- The local authorization cache cannot be updated because the file system is full.

See [Working with the authorization cache on managed computers](#) for more information about the authorization cache and the conditions under which a computer is considered to be not connected.

Accessing network computers with privileges

Depending on how you have defined the roles users are assigned, it is possible for users to see potentially misleading information in certain applications or be unable to perform the administrative tasks as they expect. For example, if users 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 they have permission to start and stop services or perform other tasks. However, if the role does not include network access rights for the remote SQL Server instance, users will not have the appropriate permission to perform those tasks.

You can check whether the selected role includes network access rights using the Authorization Center. If the role being used does not include network access rights, check whether the user has additional network roles available to use in conjunction with the local role. If the role being used includes network access rights, you should check whether those rights are applicable on the network computer the user is attempting to manage. Users must be assigned to the role that has network access rights on the remote server.



Refreshing cached information on managed computers

Authorization information is cached on the local computer to improve performance and to allow the use of elevated privileges even if users are disconnected from the network. If you make changes to rights, role definitions, or role assignments, you can refresh the information stored in the cache on managed computers to ensure the agent has the most up-to-date information about current rights and roles. If users are experiencing authorization problems or issues with their access rights (for example, if the management console shows that a user has logon rights, but `dzinfo` or the authorization center does not show that the user has logon rights), you should try refreshing the cache to make sure any changes you have made take effect.

You can refresh the cache using agent configuration panel or the `dzrefresh` command line program in a Command Prompt window if you have the appropriate permissions.

Analyzing information in Active Directory

One important way you can troubleshoot your environment is by running the Analyze command. The Analyze command enables you to selectively check the integrity of information stored in Active Directory. With the Analyze wizard, you can check for a variety of potential problems, such as empty zones, invalid role assignments, or orphaned role assignments.

Note: When you run the Analyze command, only the zones that are open are checked.

To check for problems in the Active Directory forest:

1. Open Access Manager.
If you are prompted to connect to a forest, specify the forest domain or domain controller to which you want to connect.
2. Select the root node, right-click, then click **Analyze**.
3. Select the types of checks you want to perform, then click **Next** to generate the report.



You can select All to perform a complete check of the Active Directory forest. However, some of the analysis options are only applicable for Linux and UNIX computers or UNIX user and group profiles. For more information about any analysis option, see the Access Manager help or the *Administrator's Guide for Linux and UNIX*.

4. Review the result summary, then click **Finish**.
5. If the result summary indicates any issues, you can view the details by selecting **Analysis Results** in the console tree and viewing the information listed in the right pane. For example:

| Category | Status | Severity | Description |
|-------------------------------------------|--------|----------|----------------------------------------------------------------|
| Duplicate users in zones | New | Warning | Zone 'ajax.org/Program Data/Cenify/Zones/default' have 2 us... |
| Empty zones | New | Warning | Zone 'Manufacturing-EU' does not contain any computer. |
| Empty zones | New | Warning | Zone 'ConsumerServices-CA' does not contain any computer. |
| Empty zones | New | Warning | Zone 'IndustrialComponents-AP' does not contain any computer. |
| Insufficient permission for agent upgrade | New | Error | Computer 'ajax.org/Computers/Inagnolia' doesn't have permis... |

6. Select individual warnings or errors, right-click, then select **Properties** for additional information.

Common scenarios that generate errors and warnings

For most organizations, it is appropriate to check the data integrity of the Active Directory forest on a regular basis. Although running the Analyze command frequently may not be necessary for small networks with few domain controllers, there are several common scenarios that you should consider to determine how often you should check the forest for potential problems.

The most likely reasons for data integrity issues stem from:

- Multiple administrators performing concurrent operations.
- Administrators using different domain controllers to perform a single operation.
- Replication delays that allow duplicate or conflicting information to be saved in Active Directory.
- Insufficient permissions that prevent an operation from being successfully completed.
- Network problems that prevent an operation from being successfully completed.
- Partial or incomplete upgrades that result in inconsistency of the information stored in Active Directory.



- Using scripts or ADSI Edit rather than the console to create, modify, or delete objects in Active Directory, which may lead to corrupted or invalid information.

Running Analyze periodically helps to ensure that the scenarios that can cause problems are reported in the Analysis Results, enabling you to take corrective action.

Responding to errors and warnings

Depending on the type of warning or error generated in the Analysis Results, you might be able to take corrective action or access additional information. For example, if a computer account lacks the necessary permission to update Active Directory with the agent version it has currently installed, the Analysis Result will enable you to update the computer's account permissions to allow changes to that attribute.

To review additional information or take corrective action, select the error or warning in the list of Analysis Results after running the Analyze wizard, right-click, then select Properties. For more information about responding to analysis results, see the Access Manager help or the *Administrator's Guide for Linux and UNIX*.

Running diagnostics and viewing logs for the agent

The Centrify Agent for Windows provides logging and diagnostic services. If you have administrative access on a local computer, you can generate diagnostic information about the operation of the Centrify agent for Windows and view and save the current content of the log file from the agent configuration panel. For example, you can generate diagnostic information about user sessions, user roles, desktops, and elevated account access, as well as detailed information about auditing from the agent configuration panel.

There are three different types of diagnostics information available:

- **Centrify Audit & Monitoring Service** provides the diagnostic information related to the auditing and monitoring service.
- **Centrify Identity Services Platform** provides the diagnostic information related to Privileged Access Service, such as for MFA. This diagnostics



tool runs the following tests:

- **Agent Service Connectivity Check:** Checks to see if the agent is in service, and if the agent is running in a normal state. Also determines whether the agent is in a zone, or is configured to use zoneless mode.
- **Centrify Connector Connectivity Check:** Determines whether all connectors in the network can be connected properly.
- **Centrify Identity Services Platform Certificate Validation Check:** Checks whether the certificates (IWA and cloud) have been installed properly. Also determines whether the agent can be connected without a trusted certificate problem.
- **Centrify Identity Services Platform Connectivity Check:** Determines whether a connection to the cloud tenant is functional. Checks for problems with DNS, the firewall, and proxy server settings.
- **MFA Configuration Check:** Determines whether the local computer has been configured properly. If the computer is in a zone, the test also checks whether MFA complies with the configuration defined in the zone.
- **MFA Role and Permission Check:** Verifies whether role permissions are set properly in the Privileged Access Service Admin Portal.
- **Offline MFA Provisioning Check:** Determines if the computer has been configured with an offline MFA profile or not.
- **RADIUS Configuration Check:** If RADIUS authentication is enabled, this check determines if the RADIUS settings are configured correctly or not.
- **RADIUS Connectivity Check:** If RADIUS authentication is enabled, this check determines if the agent can connect to the RADIUS server or not.
- **Centrify Privilege Elevation Service** provides the diagnostic information related to privilege management.

You can view these diagnostics tools either from the Windows system tray or from the agent configuration panel.



To view diagnostics from the Windows system tray:

1. Log on to a computer where the Centrify agent for Windows is installed.
2. In the Windows system tray, right-click the Centrify icon and click **Troubleshooting**, then select the service for which you want to view diagnostic information (your options may vary depending on what services are enabled on the computer):
 - **Centrify Audit & Monitoring Service** opens a dialog box with a text-based summary of diagnostic auditing and monitoring information.
 - **Centrify Identity Services Platform** runs a series of connectivity tests and lists out the results of each test.
 - **Centrify Privilege Elevation Service** opens a dialog box with a text-based summary of diagnostic privilege elevation information.

To generate diagnostics or view the log file from the agent configuration panel:

1. Log on to a computer where the Centrify agent for Windows is installed.
2. In the list of applications on the Windows Start menu, click **Agent Configuration** to open the agent configuration panel.
3. Select the service for which you want to view information:
 - **Centrify Audit & Monitoring Service** opens a dialog box with a text-based summary of diagnostic auditing and monitoring information.
 - **Centrify Identity Services Platform** runs a series of connectivity tests and lists out the results of each test.
 - **Centrify Privilege Elevation Service** opens a dialog box with a text-based summary of diagnostic privilege elevation information.
4. Click **Settings**.
5. Click the **Troubleshooting** tab.
6. Click **Diagnostics** to generate diagnostic information.
7. Select the Diagnostic Information displayed, right-click, then select **Copy** to copy and paste the output to a file for further analysis.
8. Click **View Log** to display the current log file for the local agent.
9. Click **Options** to see or change the location of the log file or the level of detail recorded in the log file.



Sample diagnostic report

For example, if you are viewing information about the privilege elevation service, the diagnostic report might be similar to this:

```
Product:          Centrifly Infrastructure Services (Name and Version
information)
Computer:         DC2008R2-LG
Joined Domain:    finsterwald.org
Zone:            finsterwald.org/Centrifly Pubs/Zones/HeadquartersAgent
State:           Connected
Time:            2017-10-16 12:38:03.620 -08:00
Session information:
  Session 1
    SAM Name:      FINSTERWALD\anton.splieth
    Logon Type:    Console
    Always Audit:  Yes
    Desktops:
      Default
        GUID:      de1dd94a-b671-4b37-baa4-9b2c1b70e776
        DZ Logon Id: (0x0)
        Local Role: Self
        Network Roles: Self
        Always Audit: Yes
        Audit Flag: On
        UAC Restrictions: No
      SQL-DBA
        GUID:      fccb2382-3800-4f3c-9569-922048f91375
        DZ Logon Id: (0x9ba99)
        Local Role: SQL-DBA/Headquarters
        Network Roles: Self
        Always Audit: Yes
        Audit Flag: On
        UAC Restrictions: No
        Network Drives: No

Logon information:
  Logon ID (0x9ba99)
    Logon GUID:    38407dd1-0165-458e-b45d-686a07e87805
    Base Logon ID: (0x77163)
    Base SAM Name: FINSTERWALD\anton.splieth
    ElevatedAccount: (ElevatedSelfAccount, AdditionalGroups=(count=1,
items=(S-1-5-32-544)))
    Local Role:    SQL-DBA/Headquarters
    Network Roles: None
    Should Audit:  Yes
  Logon ID (0x22bfee)
    Logon GUID:    1b50b739-461c-410e-803c-ed52d4ba1e80
    Base Logon ID: (0x77163)
    Base SAM Name: FINSTERWALD\anton.splieth
    ElevatedAccount: (ElevatedSelfAccount, AdditionalGroups=(count=1,
items=(S-1-5-32-544)))
    Local Role:    SQL-DBA/Headquarters
    Network Roles: None
    Should Audit:  Yes

Domain last access information:
  Forest finsterwald.org: Connected
  Domains: finsterwald.org: Connected
```



Multi-factor Authentication information: None

Done.

Enabling detailed logging for audit and monitoring service components

In addition to the log files for Centrify agents for Windows, there are log files for other audit and monitoring service components to record information about operations performed by those components on a local computer. If you have audit and monitoring service components installed, you can view the log files or change log file options for those components to assist Centrify Support when troubleshooting issues.

Enabling detailed logging for an audited computer

If you are troubleshooting an audit and monitoring service-related issue, you should enable detailed logging for the audit and monitoring service on the computers being audited. For Windows computers, you can enable detailed logging using the agent configuration panel.

To enable detailed logging on an audited computer:

1. Log on to an audited computer.
2. In the list of applications on the Windows Start menu, click **Agent Configuration** to open the agent configuration panel.
3. Click **Centrify Audit & Monitoring Service**.
4. Click **Settings**.
5. Click the **Troubleshooting** tab.
6. Click **Options**, change the logging level to **Trace messages**, then click **OK**.
7. Note the log folder location or click **Browse** to specify a different location for the log file, then click **OK**.
8. Click **View Log** to view the current log file.

From the log file window, you can also click **File > Save As** to save the log file.



9. Send an email to Centrify Support with the log file from the location specified in Step 7 as an attachment.
10. Click **Options**, change the logging level back to its default setting of **Informational messages**, then click **OK**.
11. Click **Close** to return to the agent configuration panel.

Enabling detailed logging for the collector service

If you are troubleshooting an audit and monitoring service-related issue, you should enable detailed logging for the collector service on the computers where the collector service runs.

To enable detailed logging on a collector:

1. In the list of applications on the Windows Start menu, click **Audit Collector Control Panel** to open the audit collector control panel.
2. Click the **Troubleshooting** tab.
3. Click **Options**, change the logging level to **Trace messages**, then click **Apply**.
4. Note the log folder location or click **Browse** to specify a different location for the log file, then click **OK**.
5. Click **View Log** to view the current log file.
From the log file window, you can also click File > Save As to save the log file.
6. Send an email to Centrify Support with the log file from the location specified in Step 4 as an attachment.
7. Click **Options**, change the logging level back to its default setting of **Informational messages**, then click **OK**.
8. Click **Close** to return to the Collector Control Panel.

Enabling detailed logging for audit and monitoring service consoles

In most cases, troubleshooting audit and monitoring service-related issues requires information about the operation of the agent and the collector or



database activity. However, in some cases, it might be necessary to capture detailed information about the operation of Audit Manager or Audit Analyzer.

To capture detailed information for Audit Manager or Audit Analyzer:

1. Log on to a computer where the Audit Manager or Audit Analyzer console is installed.
2. In the list of applications on the Windows Start menu, click **Agent Configuration** to open the agent configuration panel.
3. Click **Centrify Audit & Monitoring Service**.
4. Click **Settings**.
5. Click the **Troubleshooting** tab.
6. Click **Options**.
7. In the Log Settings tab, change the logging level to **Trace messages**, then click **OK**.
8. Note the log folder location or click **Browse** to specify a different location for the log file, then click **OK**.
9. Send an email to Centrify Support with the log file from the location specified in Step 8 as an attachment.
10. Click **Options**, change the logging level back to its default setting of **Warning messages**, then click **OK**.
11. Click **Close** to return to the agent configuration panel.

Enabling audit and monitoring service performance counters for the collector

If you have enabled audit and monitoring service and installed the collector service on a local Windows computer, you can add audit-specific performance counters to Performance Monitor to help you analyze and resolve audit-related issues. When you install the collector, the performance counters are added automatically. When you uninstall the collector, the counters are automatically removed from Performance Monitor.

For more information about troubleshooting in an audit installation, see the *Auditing Administrator's Guide*.



Tracking database activity

Database traces are used to help diagnose problems in the management database or audit store databases. For example, database traces can help to identify inconsistencies caused by hardware errors or network interruptions. After you enable database tracing, DirectManage Audit tracks all of the SQL statements and debug messages from the audit management database or audit store, and records the information in the database server.

Note: Tracing database operations affects database performance. You should only activate a database trace if you require this information for troubleshooting. Before you start a database trace, try to reduce the load on the database instance as much as possible, then only perform the actions needed to reproduce the issue you are troubleshooting. Turn off database tracing as soon as you have logged the activity you need for the analysis of database operations. The trace for each database can take up to 800MB of server disk space. After you turn off database tracing, restart the SQL Server instance to reset the disk space.

Starting a database trace

You can start a database trace for a management database or an audit store database.

To start database tracing:

1. Open Audit Manager.
2. Select an installation name, right-click, then click **Properties**.
3. Click the **Database Trace** tab.
This tab displays basic information about the management databases and audit store databases for the selected installation. In the Trace Status column, you can see whether tracing is enabled or disabled for each database.
4. Select a management or audit store database in the list, then click **Enable** to start tracing on the database selected.
5. Click **OK**, then perform the database actions for which you want to capture information.



Stopping the database trace

You should turn off database tracing immediately after you have logged the activity you need for the analysis of database operations.

To stop database tracing:

1. Open Audit Manager.
2. Select the installation name, right-click, then click **Properties**.
3. Click the **Database Trace** tab.
4. Select the management or audit store database that has tracing enabled, then click **Disable** to stop tracing on the database selected.
5. Click **Export** to save the database trace from the selected databases to a file with comma-separated values (.csv).
6. Follow the prompts displayed in the Export Database Trace wizard to save the information to a file.

Exporting the database trace for a management database

The Export Database Trace wizard prompts you for different information depending on whether the database trace is for a management database or an audit store database. For example, if you generate a database trace for a management database then click **Export**, the Export Database Trace wizard prompts you for user accounts.

To export the database trace:

1. Select a start date and time for the **From** filter and an end date and time for the **To** filter, then click **Next**.
2. Click **Add** to search for and select users, then click **Next**.
By default, you can search for users in the entire directory, you can click **Object Types** or **Locations** to change the scope of the search scope, or click **Advanced** specify other criteria.
3. Accept the default folder location or click **Browse** to select a different location, then click **Next**.
4. Review your selections, then click **Next**.



By default, the wizard save the file as *installation_name.csv* and opens the file location.

5. Click **Finish**, then click **OK** to close the installation properties.

Exporting the database trace for audit store databases

When you select an audit store from the lower area of the **Database Trace** tab on the **Properties** page and click the lower **Export** button, the wizard opens with a date/time **Export Criteria** page. On the second page, the wizard asks you to pick the domain and computer.

To export the database trace:

1. Select a start date and time for the **From** filter and an end date and time for the **To** filter, then click **Next**.

2. Click **Add** to search for and select collectors, then click **Next**.

By default, you can search for computers in the entire directory, you can click **Object Types** or **Locations** to change the scope of the search scope, or click **Advanced** specify other criteria.

3. Click **Add** to search for and select management database computers, then click **Next**.

4. Accept the default folder location or click **Browse** to select a different location, then click **Next**.

5. Review your selections, then click **Next**.

By default, the wizard save the file as *audit_store_name.csv* and opens the file location.

6. Click **Finish**, then click **OK** to close the installation properties.

Delegating database trace management

You can delegate the authority to manage database tracing by granting the Manage Database Trace permission to other users for a management database or an audit store database.



Controlling audit trail events

By default, audit trail events are recorded when users log on, open applications, select roles that elevate their privileges, and perform other tasks. You can use domain group policies to control the global location of the audit trail events. For example, you might want to store audit trail events in the audit store database instead of the Windows event Application log if you want to make them available for querying and reports.

You can also override domain group policy and configure local or category-specific audit trail targets using a local administrative template or group policy.

To configure global or per-category audit trail targets using an ADM administrative template:

Note: These settings override the settings defined in the **Set global audit trail targets** group policy.

1. Open the Group Policy Object Editor to display Local Computer Policy, and select **Computer Configuration > Administrative Templates**.
2. Right-click, select **Add/Remove Templates**, then click **Add**.
3. Navigate to the `AuditManager` folder, select `audittrail.adm`, click **OK**, then click **Close**.
4. Open the Classic Administrative Templates folder and select **AuditTrail**.
5. Specify global or separate targets for audit trail events:
 - Enable **Set global audit trail target settings** to configure a single location for audit trail events for Access Manager and the Centrify agents.
 - If you want to have separate targets for audit trail events, you can enable the other audit trail group policies to override the global policy setting with a different target.
6. Specify the location for saving audit trail events, and then click **OK**:
 - 0 to disable audit trail events
 - 1 to store audit trail events in the audit store
 - 2 to send audit trail events to the Windows event Application log
 - 3 to send audit trail events to both the audit store and the Application log.



To configure per-category audit trail targets using a local group policy from an XML template:

Note: These settings override the settings defined in the Set global audit trail targets group policy.

1. Ensure that the Centrify Audit Trail Settings were updated with the most recent XML template.
2. Open the Group Policy Object Editor to display **Local Computer Policy**, and select **Computer Configuration > Centrify Audit Trail Settings**.
3. In **Centrify Audit Trail Settings**, separate folders for each audit trail category contain **Send audit trail to Audit database** and **Send audit trail to log file** group policies. Enable these group policies in each category that you want to configure to use a specific audit trail target. The target that you specify for each category is used instead of the target specified in the **Set global audit trail targets** group policy.

Summary of audit trail events

Different components log different audit trail events. For example, the auditing and authorization services on a managed Windows computer track successful logon attempts and the use of Window access rights. Access Manager audit trail events record changes to the configuration of zones, such as the delegation of administrative tasks, the assignment of roles, and changes to the user and group profiles in a zone. For your reference, the following sections summarize the audit trail events recorded by Centrify agents on managed Windows computers.

Additional audit trail events for Access Manager, Audit Analyzer, Audit Manager, and UNIX commands can be recorded in the target you specify for the audit trail. The event message provides detailed information about the operation performed or unsuccessfully attempted, including in most cases the reason the operation was unsuccessfully.

For a complete list of audit trail event identifiers and their corresponding descriptions, see the `AuditTrailEvent.xml` file provided in the Documentation folder. This file is generated directly from the underlying source code and provides the most up-to-date information about the events on which you can query and report.



Offline MFA profile authentication

In some environments, using an offline MFA profile for multi-factor authentication is not compatible with FIPS mode. See the *Multi-factor Authentication Quick Start Guide* for details about this restriction.

Centrify Authentication Service known issues

When troubleshooting, be aware of the following issues and constraints:

- Import users and groups before importing the sudoers file (Ref: IN-90001).

Sudoers Import creates user roles but not the users. It is recommended that you import users and groups prior to importing the sudoers file. Otherwise, no sysRights are created for the users.

- Pre-create computers before importing computer role from sudoers file (Ref: IN-90001).

The computers contained in the sudoers file must either be joined to a zone or pre-created.

- Delegating zone administration permissions for SFU zones (Ref: IN-90001)

Delegate permissions to add, remove or modify users for SFU zone are not supported.

- Users with rights to import user and groups into a zone also gain rights to modify profiles (Ref: IN-90001)

Any users who are given the right to "Import users and groups to zone" are automatically also given the right to "Modify user/group profiles".

- Using domain local groups to manage resources (Ref: IN-90001)

Domain local groups can only be used to manage resources in the same domain as the group. So, for instance, a domain local group in domain A may be used to manage a computer in domain A but not one in domain B, despite a trust relationship between the two domains.

- Domain local groups from other domains shown in search dialog (Ref: IN-90001)

When using the search dialog in the Access Manager to delegate zone control to a group, domain local groups from child domains will be shown



incorrectly in the results and should be ignored. The search results when using the ADUC extension do not show these domain local groups.

- Analyze forest and SFU zones (Ref: IN-90001)

The analyze forest feature in the Access Manager does not report empty zones or duplicated users or groups in a SFU zone.

- Working with users that have more than one UNIX mapping (Ref: IN-90001)

Centrify Authentication Service supports Active Directory users that have more than one UNIX profile in a zone. However, if you are upgrading from DirectControl 4.x or earlier and have existing users with more than one UNIX mapping, you should use DirectControl Access Manager 5.0.0 or later to remove all but one of the UNIX profiles for each of these Active Directory users and then re-add them.

In addition, you should always use DirectControl console 5.0.0 or later when modifying these users.

- In the Centrify Profile tab of the Properties page of a computer joined to a hierarchical zone, you cannot move this computer to a classic zone. Nor can you move it to a zone in another domain. There are no such limitations with a computer joined to a classic zone. (Ref: IN-90001)

- Extra results when analyzing duplicate service principal names (Ref: IN-90001)

When running the Analyze / Duplicate Service Principal Names report, kadmin/changepw is incorrectly returned as a duplicate. The SPN is actually found multiple times, but this is by Microsoft design as it is the default account for the Key Distribution Center service in all domains.

- Secondary groups not imported from XML files (Ref: IN-90009)

Using the Import Wizard to import user information from XML files does not import secondary group membership.



Using Windows command line programs

This chapter provides a summary of the command line programs you can run on computers that have the Centrify agent for Windows installed to perform troubleshooting and administrative operations.

The following topics are covered:

| | |
|-------------------------------------------|-----|
| Using CopyGroup and CopyGroupNested | 265 |
| Using dzinfo | 266 |
| Using dzjoin | 270 |
| Using dzleave | 271 |
| Using dzdiag | 271 |
| Using dzrefresh | 273 |
| Using dzflush | 274 |
| Using dzdump | 274 |
| Using runasrole | 276 |

Using CopyGroup and CopyGroupNested

The CopyGroup and CopyGroupNested commands help you provision users when there are trust relationships between domains. You can use them to mirror group membership and group hierarchy from a trusted domain and forest to a target domain and forest.

These utilities are located in the Zone Provisioning Agent's **Tools** folder.



To use these command line utilities, you must have an account that can log on to the trusted source domain and the target domain. The account should also have read permission on the source domain and permission to update the target domain.

For example, assume you have configured the AJAX domain to have a one-way trust with the DEVOPS domain and you have your Active Directory users and groups defined in the DEVOPS domain. If you want to allow the users and groups in the DEVOPS domain to log on to computers that are joined to the AJAX domain, you can log on to the AJAX domain controller with an account that has administrative privileges in both the AJAX and DEVOPS domains, then run the `CopyGroup` utility to mirror the group membership from a group in the DEVOPS source domain as zone users in the AJAX target domain.

For more information about the command line arguments and options for these utilities, see the usage message displayed for each utility.

Using `dzinfo`

The `dzinfo` command line program provides detailed information about the effective rights, role definitions, and role assignments for a specified user. The command output includes all of the same information that you can view using the Authorization Center as described in [Using the Authorization Center directly on managed computers](#). However, using `dzinfo` as a command line utility allows you to view and capture all of the output from the command in a single window, which you can then save as a text file for troubleshooting and analysis or in reports.

The syntax for the `dzinfo` program is:

```
dzinfo [/v] [user_name] [/h]
```

The `/v` is an optional argument that enables you to view verbose output for the command. The `user_name` is an optional argument that enables you to view information for the specified user account. However, you must be logged on as a local administrator to specify the `user_name` argument. If you log on with an account that does not have local administrative privileges you cannot return authorization information for another user account.

If you run the `dzinfo` command without the `user_name` argument, the command returns authorization information for the currently logged-on user account.



The command returns detailed information about the rights, roles, and role assignments for the specified user (rich1 in the AJAX domain) similar to the following:

From the Centrify Access Manager

Effective roles for AJAX\rich1:

Domain Admin/portland

Zone: CN=portland,CN=global,CN=Zones,OU=Centrify,DC=ajax,DC=org

Status: Active

windows Login/global

Zone: CN=global,CN=Zones,OU=Centrify,DC=ajax,DC=org

Status: Active

Effective Login Rights for AJAX\rich1:

Console Login: Permitted

Audit Level: Audit if possible

Remote Login: Permitted

Audit Level: Audit if possible

PowerShell Remote Access: Permitted

Audit Level: Audit if possible

Role Assignments for AJAX\rich1:

Domain Admin/portland

Status: Active

Account: AJAX\rich1

Scope: Zone

Zone: ajax.org/Centrify/Zones/global/portland

Local Role: No

Network Role: Yes

Effective: Immediate

Expires: Never

windows Login/global

Status: Active



Account: AJAX\Domain Admins
Scope: Zone
Zone: ajax.org/Centrify/Zones/global
Local Role: Yes
Network Role: No
Effective: Immediate
Expires: Never

Role Definitions:

Domain Admin/portland

Status: Active
Description: None

Zone:
CN=portland,CN=global,CN=Zones,OU=Centrify,DC=ajax,DC=org

Login Permitted: No
Audit Level: Audit if possible
Rescue Right: No

Require MFA: No

Available Hours: All

Rights:

ADUC/portland

Type: Application
Description: None
Priority: 0
Run As: AJAX\Administrator
Application: mmc.exe
Path: C:\windows\system64
C:\windows
C:\Program Files
C:\Program Files (x86)
C:\windows\syswow64
Arguments: "C:\windows\system64\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/global

Status: Active

Description: Predefined system role for general windows login users.

Zone: CN=global,CN=Zones,OU=Centrify,DC=ajax,DC=org

Login Permitted: Console & Remote & PowerShell Remote

Audit Level: Audit if possible

Rescue Right: No

Available Hours: All

Rights:

None

Computer is joined to zone ajax.org/Centrify/Zones/global/portland

Auditing for AJAX\richl:

Session ID 2:

Desktops:

Default: Not currently auditing.

Auditing is not available on this computer.



Using dzjoin

The `dzjoin` command line program enables you to automatically join users to the zone in which their roles and rights are assigned, or to join them to a specific zone by zone name, when they log on to their computer. 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 [/c <domain controller>] [/d] [/u <username>] [/f] [/h] [/r  
[y|n|yes|no]] {/z <zonenumber> | /s | /v}
```

Note: If the `u` option is specified but no password is found in the redirected input, you will be prompted for a password.

| Use this option | To do this |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/c</code> | Specify a domain controller to connect to. |
| <code>/d</code> | Retrieve zone data before restarting |
| <code>/u</code> | Specify the user name to join zone using custom credentials. The user name must be in the format: <code>USER@DOMAIN</code> or <code>DOMAIN\USER</code> . The credentials are for remote access only. For the password, you can specify by redirected input. Otherwise, this tool will prompt user for password. |
| <code>/f</code> | Suppress any warnings and/or questions. |
| <code>/h</code> | Displays the command help. |
| <code>/r</code> | Suppress the restart warning and specify to restart machine, if required, after joining zone. If no restart is required, this option is ignored. If no argument is provided, e.g. <code>'/r'</code> , the default is to restart (example: <code>'/r yes'</code>). |
| <code>/z</code> | Join a zone using the zone name. If the zone name is not unique, use the canonical name instead. |
| <code>/s</code> | Join to the zone where this computer is already pre-created in the zone or had previously been joined to the zone (but remotely left in a disconnected situation). |
| <code>/v</code> | Display the agent version. |

Note: You can also use the PowerShell command `Join-CdmZone` to join a zone.



Using dzleave

To leave a zone, use the `dzleave` command. The syntax for the `dzleave` command is:

```
dzleave [/c <domain controller>] [/u <username>] [/a|/f] [/r  
[y|n|yes|no]] [/v] [/h]
```

| Use this option | To do this |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /a | Remove the role assignment from the computer zone. |
| /c | Specify a domain controller to connect to. |
| /u | Specify the user name to leave zone using custom credentials. The user name must be in the format: USER@DOMAIN or DOMAIN\USER. The credentials are for remote access only. For the password, you can specify by redirected input. Otherwise, this tool will prompt user for password. |
| /f | Suppress any warning and/or question(s). In case the domain cannot be contacted, this tool will perform a local zone leave automatically. |
| /h | Displays the command help. |
| /r | Specify whether to restart machine, if required, after leaving zone without prompt. If no restart is needed, this option is ignored. If no argument is provided, example: '/r', the default is to restart ('/r yes'). |
| /v | Show the agent version. |

Note: You can also use the PowerShell command `Exit-CdmZone` to leave a zone.

Using dzdiag

The `dzdiag` command line program provides detailed diagnostic information for the local computer. The command output includes all of the same information that you can view by clicking **Diagnostics** on the **Troubleshooting** tab as described in [Running diagnostics and viewing logs for the agent](#).

The syntax for the `dzdiag` command is:

```
dzdiag [/h] [/o]
```

The `/h` is an optional argument that displays the command help.

The `/o` is an optional argument that allows you to output just the offline MFA provisioning information. You can use this option to see if a user has configured an offline MFA profile or not and details about their offline MFA configuration.



You must be logged on as a local administrator to run the `dzdiag` command.

The command returns detailed information about desktop sessions similar to the following:

```
Product:          Centrifify Infrastructure Services version-number (build-number)
Computer:         CENTRIFY01
Joined Domain:    acme.local
Zone:            acme.local/Program Data/Centrify/Zones/global
Auditing:        Available
Agent State:     Connected
Time:           2018-10-04 17:41:41.491 -07:00
Session information:
  Session 3
    SAM Name:     CENTRIFY01\Administrator
    Logon Type:   Console
    Always Audit: Yes
    Desktops:
      Default
        GUID:          3e2c9799-b398-459f-a7a2-ed3a5359af3f
        DZ Logon Id:   (0x0)
        Local Role:    Self
        Network Roles: Self
        Audit Status:  Currently Auditing
        UAC Restrictions: No
        Network Drives: No

Logon information:
  Logon ID (0x5bd925)
    Logon GUID:     50972030-e9ed-45dc-b7b7-ecf588ef152d
    Base Logon ID:  (0x1aff6e)
    Base SAM Name:  ACME\admin
    ElevatedAccount: (ElevatedSelfAccount, AdditionalGroups=(count=1,
items=(S-1-5-32-544)))
    Local Role:     windows
Login/CN=global,CN=Zones,CN=Centrifify,CN=Program Data,DC=acme,DC=local
  Network Roles:   None
  Should Audit:    Yes
  Logon ID (0x5c2fe6)
    Logon GUID:     053ef6cd-10cc-4383-b614-437c1a2067e3
    Base Logon ID:  (0x1aff6e)
    Base SAM Name:  ACME\admin
    ElevatedAccount: (ElevatedSelfAccount, AdditionalGroups=(count=1,
items=(S-1-5-32-544)))
    Local Role:     windows
Login/CN=global,CN=Zones,CN=Centrifify,CN=Program Data,DC=acme,DC=local
  Network Roles:   None
  Should Audit:    Yes
  Logon ID (0x5deca8)
    Logon GUID:     ce0da851-90f5-4cb6-a71b-25e2b116be75
    Base Logon ID:  (0x1aff6e)
    Base SAM Name:  ACME\admin
    ElevatedAccount: (ElevatedServiceAccount, ServiceAccount=S-1-5-21-
1132289714-2257106472-2904894658-500)
    Local Role:     windows
Login/CN=global,CN=Zones,CN=Centrifify,CN=Program Data,DC=acme,DC=local
  Network Roles:   None
  Should Audit:    Yes
```



```
Logon ID (0x613c40)
  Logon GUID:      8ca4e342-4f4a-4e85-8e05-4d1332272c31
  Base Logon ID:   (0x1aff6e)
  Base SAM Name:   ACME\admin
  ElevatedAccount: (ElevatedServiceAccount, ServiceAccount=S-1-5-21-
1132289714-2257106472-2904894658-1108)
  Local Role:      windows
Login/CN=global,CN=Zones,CN=Centrify,CN=Program Data,DC=acme,DC=local
  Network Roles:   None
  Should Audit:    Yes
```

Domain last access information:

```
Forest acme.local:      Connected and Agent can authenticate
Domains:
  acme.local (ACME): Connected
```

The offline MFA provisioning information:

None

Multi-factor Authentication information:

```
Platform Instance:      https://tenant.my.centrify.net/
Last Used Platform Instance: <none>
Platform Certificate Exists: No
Disable Web Proxy:      No
AD Site:                 Default-First-Site-Name
Platform Instance Override: <none>
Centrify Connector Override: <none>
MFA Enabled (NotJoined): No
Platform Instance (NotJoined): <none>
Web Proxy:               <none>
```

Centrify Connectors:

```
Connector: centrify01.acme.local
  FQDN:                centrify01.acme.local
  Tenant:               https://tenant.my.centrify.net/
  Last Known Availability: Yes
  Last Access Time:    -
  IWA Enabled:         Yes
  IWA HTTPS Port:      8443
  Proxy Enabled:       Yes
  Proxy Server:        centrify01.acme.local:8080
  AD Site:              Default-First-Site-Name
```

Using dzrefresh

The dzrefresh command line program enables you to refresh the authorization cache from a Command Prompt window. Running the dzrefresh command provides the same functionality as clicking Refresh on the Troubleshooting tab in the local agent configuration panel as described in [Performing cache operations](#).

The syntax for the dzrefresh command is:



dzrefresh

You must be logged on as a local administrator to run the `dzrefresh` command. The command output indicates whether the refresh of the authorization cache is successfully initiated.

Using dzflush

The `dzflush` command line program flushes the authorization cache and reloads all authorization information from Active Directory. Depending on the size of the authorization store, users might experience a temporary loss of the ability to use the rights granted to them while the authorization information is reloaded. To prevent any loss of access privileges, in most cases you should use the `dzrefresh` command instead of the `dzflush` command to ensure that the agent is using the latest authorization information. You should only use the `dzflush` command if Centrify Support recommends you do so.

The syntax for the `dzflush` command is:

```
dzflush [/h] [/1]
```

| Use this option | To do this |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| /h | Show the command usage. |
| /1 | Synchronize local Windows account information between Access Manager and the Windows systems where local account management is enabled. |

Note: Local account management is not supported on domain controllers.

You must be logged on as a local administrator to run the `dzflush` command. The command output indicates whether the authorization cache is successfully flushed.

Using dzdump

The `dzdump` command line program enables you to view and capture the current content of the authorization cache. You can use command line options to control the information contained in the output for the command.

The syntax for the `dzdump` command is:

```
dzdump [/d directory-path ] [/w=screen-width] [/s] [/n] [/g] [/1] [/a] [/r] [/i] [/t] [/z] [/u] [/h]
```



If you specify no command line arguments, the `dzdump` command returns complete in-memory information from the authorization agent (`dzagent`) cache. You can use the following command line arguments to refine the output for the command:

| Use this option | To do this |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | Dump cache files from the default location or a specified location. You can use this option with a directory path to dump cache files from a specified location. For example, to dump cache files from the directory <code>C:\CentrifyAZstore:/d=C:\CentrifyAZstore</code> |
| <code>/d</code> | Note that you cannot use the <code>/d</code> option to dump cache files directly on a computer where the Centrify agent for Windows is currently running. However, you create a copy of the cache, then dump the cache from the saved copy. For example, copy all files in the cache directory—the default location for cache directory is <code>c:\ProgramData\Centrify\DirectAuthorize\Cache</code> —to a temporary directory. You can then dump the authorization cache by running <code>dzdump</code> and specifying the temporary location. |
| <code>/w</code> | Use the specified <i>screen-width</i> for word-wrapping the command output. If you don't specify this options, the default screen width is 80 characters. To disable word-wrapping of the command output, specify a <i>screen-width</i> of zero. For example: <code>/w=0</code> |
| <code>/s</code> | Display security identifier (SID) mappings |
| <code>/n</code> | Display name mappings |
| <code>/g</code> | Display assignee mappings |
| <code>/l</code> | Display assignments in the joined zone hierarchy |
| <code>/a</code> | Display assignments for security identifiers (SID) |
| <code>/r</code> | Display role definitions |
| <code>/i</code> | Display right definitions |
| <code>/t</code> | Display access token information |
| <code>/z</code> | Display zone hierarchy |
| <code>/u</code> | Display recent user logon activity |
| <code>/h</code> | Displays the command help |

You can use any combination of display options to display only the information of interest. If you do not specify any display options, the `dzdump` command displays all of the information in the authorization cache.

You must be logged on as a local administrator to run the `dzdump` command. You should note that the command output from a `dzdump` command can contain sensitive information. You should only use the `dzdump` command if Centrify Support recommends you do so.



Depending on the display options you specify, the command returns detailed information about the authorization cache.

Using runasrole

The `runasrole` command-line program enables you to run a specified Windows application 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 and options with the `runasrole` command:

| Use this option | To do this |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/role</code> | 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. |
| <code>/localrole</code> | You should only use this option if the role you are assigned and want to use has both local and network access rights defined. |
| <code>/networkrole</code> | Use the role name you specify as a network role. |
| <code>/env</code> | Use the current environment variables instead of the environment variables associated with the "Run As" user account. |



| Use this option | To do this |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/netdrives</code> | <p>Use mapped network drives when running an application with the selected role.</p> <p>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 <code>/netdrives</code> option in the command line.</p> |
| <code>/removetimestamp</code> | <p>Remove the grace period on Windows authentication and MFA for the current user session.</p> |
| <code>/wait</code> | <p>Prevents the <code>runasrole</code> program from exiting immediately after opening the specified application.</p> <p>If you specify this option, the <code>runasrole</code> program starts the specified application and waits until the application session ends before exiting. When the application session ends, the <code>runasrole</code> program exits and returns the same result code as the application.</p> <p>If you specify this option and the application is a command line utility, the <code>runasrole</code> program redirects the application's input and output to the command line console.</p> <p>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 <code>/wait</code> option has no effect and is ignored.</p> |
| <code>/h</code> | <p>Displays the command help.</p> |

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\system64\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\system64\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\system64\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\System64\control.exe printers`, the application executable `C:\windows\System64\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.



Working with Server Core and Windows Server 2012

The Centrify agent for Windows 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 is no Centrify notification area applet or desktop rights available on Server Core computers. However, you can access the Authorization Center, agent configuration panel, 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 agent configuration panel from Start menu shortcuts because the Windows desktop and Windows Explorer are not available on Server Core.



You should note that only the Centrify agent for Windows is supported for the Server Core environment. A small number of other Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service components for Windows support a command line interface, but are not configured to support a Server Core environment.

The following topics are covered:

| | |
|--------------------------------------------------------------|-----|
| Server Core supported platforms | 281 |
| Installing the agent on a computer running Server Core | 282 |
| Opening consoles on Server Core computers | 283 |
| Joining a zone | 283 |
| Viewing authorization details | 284 |
| Configuring auditing options | 284 |
| Running command line programs | 285 |
| Unsupported Windows Server 2012 features | 286 |

Server Core supported platforms

Centrify supports the following versions of the Server Core environments:

- 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.



For general information about Server Core on Windows Server 2008 R2, see: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753802\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753802(v=ws.10))

For general information about Server Core on Windows Server 2012 R2, see: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831786\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831786(v=ws.11))

Installing the agent on a computer running Server Core

You cannot use the `autorun.exe` or the `setup.exe` program to install components on a computer that is configured to run as a Server Core environment. Instead, you must install from Microsoft Installer (`.msi`) files using the `msiexec` command-line program.

To install the Centrify agent for Windows on Server Core:

1. Use the Deployment Image Servicing and Management (DISM) or another command-line tool to enable the .NET Framework.

For example, if you are using Windows Server 2012 or later and the .NET Framework is located on the installation media in the `D:\sources\sxs` folder, use the following command:

```
DISM /Online /Enable-Feature /FeatureName:NetFx3 /All /LimitAccess /Source:D:\sources\sxs
```

To install .NET Framework on Windows Server 2008 R2, run the following commands to enable the required features:

```
Dism /Online /Enable-Feature /FeatureName:NetFx2-ServerCore-WOW64
Dism /Online /Enable-Feature /FeatureName:NetFx3-ServerCore-WOW64
Dism /Online /Enable-Feature /FeatureName:NetFx2-ServerCore
Dism /Online /Enable-Feature /FeatureName:NetFx3-ServerCore
```

2. Copy the Centrify agent for Windows files to the Server Core computer.

For example:

```
copy D:\Common\Centrify* C:\CentrifyAgent
copy D:\Agent\* C:\CentrifyAgent
```



3. Install the Centrify Common Component service using the `.msi` file.
For example, to install the Centrify Common Component on a computer with 64-bit architecture, you might use the following command:

```
msiexec /i "Centrify Common Component64.msi" /qn
```
4. Install the Centrify agent for Windows using the `.msi` file.
Run the following command:

```
msiexec /i "Centrify agent for windows64.msi" /qn
```
5. Restart the computer with the appropriate shutdown options to complete the installation and start agent services.
For example, you might run the following command:

```
shutdown /r
```

Note that restarting the computer is not required if you install only auditing features.

Opening consoles on Server Core computers

Because the primary interface for the Server Core environment is a command prompt with only limited support for graphical user interface features, you must use the command line to open the consoles that enable you to join or leave a zone, view your rights and roles, and configure agent settings.

Joining a zone

One of the first tasks after installing the Centrify agent for Windows is to join a zone. You can do by launching the agent configuration panel from the command prompt.

To open the agent configuration panel to join a zone:

1. Navigate to the Centrify agent installation directory.
2. By default, the agent files are installed in the `C:\Program Files\Centrify\Centrify agent for windows` directory.
3. Run `Centrify.DirectAuthorize.Agent.Config.exe`.
4. Click **Change**.
5. Click **Browse**.



6. Type all or part of the zone name, click Find Now, then select the zone to join and click **OK**.
7. Click **Close** to exit the agent configuration 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, identity management, privilege management, and audit and monitoring service 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, identity management, privilege management, and audit and monitoring service features are enabled when you install the Centrify agent for Windows. To configure audit and monitoring service options and specify the audit installation for the agent, you can launch the agent configuration panel from the command prompt.

To open the agent configuration 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\Audit\Agent` 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 exit the agent configuration 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`
- `dzjoin`
- `dzdiag`
- `dzrefresh`
- `dzflush`
- `dzdump`
- `runasrole`

For more information about the command line options or output for these commands, see [Using Windows command line programs](#) or run the command with the `/help` option.



Unsupported Windows Server 2012 features

Windows Server 2012 includes support for claims, compound authentication, and Kerberos armoring. The core Centrify agent for Windows does not provide support for these advanced authentication features. To take full advantage of these advanced authentication services, however, requires you to make the following changes to your environment:

- Deploy Dynamic Access Control.
- Upgrade all of your domain controllers and application servers to Windows Server 2012 or later.
- Upgrade all of your workstations to Windows 8 or later.
- Raise the domain functional level to Windows Server 2012.

If you have a mixed environment that includes Windows 7 and Windows 8 or later workstations and Windows Server 2008 or Windows Server 2008 R2 domain controllers, you can configure the administrative template for claims, compound authentication, and Kerberos armoring to use the Not supported option (default).

To use the Supported configuration option, you must deploy Dynamic Access Control, configure Windows 8 and later client-side support for claims, compound authentication and Kerberos armoring, and ensure you have domain controllers running Windows Server 2012 to handle the authentication requests for those computers. You should not install the Centrify agent for Windows on any computers configured to support claims, compound authentication and Kerberos armoring to prevent authentication failures.

In addition, Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service does not provide any specific support for authenticating access to Server Message Block 3.0 (SMB3.0) file shares that are supported in Windows Server 2012. The SMB protocol operates as an application layer for providing shared access to computers, printers, and other devices. This protocol has been extended to provide shared access to virtual machines and SQL user databases.