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

Express Administrator's Guide for Linux and UNIX

August 2019 (release 19.6)

Centrify Corporation

Legal Notice

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

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

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

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

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

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

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

Contents

About this guide

The *Express Administrator's Guide for Linux and UNIX* describes how to install, configure, and use the components in Centrify Express for UNIX and Linux. Centrify Express products are available for free to provide identity and access control for cross-platform data centers using Active Directory. With support for a wide range of operating systems, hypervisors, and applications, Centrify agents can help your organization strengthen security and regulatory compliance while reducing IT expenses and costly interruptions to user productivity.

Centrify agents provide simplified cross-platform integration with Active Directory. In most cases, Centrify Express agents require little or no configuration, and are available for download directly from the Centrify web site. By installing Centrify agents, you can add UNIX and Linux computers to Active Directory, authenticate user credentials from a central identity store, and support local and remote cross-platform single sign-on at no cost.

Intended audience

This guide is intended for system and network administrators who are responsible for managing user access to servers, workstations, and network resources.

This guide assumes you have a working knowledge of Microsoft Active Directory and how to perform common administrative tasks on the UNIX and Linux platforms you support. This guide also assumes basic, but not expert, knowledge of how to perform common administrator tasks. If you are an experienced administrator, you may be able simplify or automate some tasks described in this guide using platform-specific scripts or other tools.

Using this guide

Depending on your environment and role as an administrator or user, you may want to read portions of this guide selectively. The guide provides the following information:

- Introduction provides an overview of Centrify Express products, how those products compare with other Centrify product offerings, and how UNIX-style user and group profiles are automatically generated for Active Directory users and groups.
- Installing Centrify agents describes the options available for installing Centrify agents on computers to be managed.
- Working with managed computers explains how to perform common tasks on computers that have the Centrify agent installed.
- Troubleshooting tips and tools describes basic troubleshooting steps and how to use diagnostic tools and log files to retrieve information about the operation of the Centrify agent.
- Using command-line programs provides reference information for the command-line programs available with the Centrify agent.
- Customizing operations using configuration parameters provides a quick reference for the configuration parameters that you can set to control operations on managed computers.

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 Zero Trust Privilege Services	Privileged Access Service
	Gateway Session Audit and Monitoring
	Authentication Service
	Privilege Elevation Service
	Audit and Monitoring Service
	Privilege Threat Analytics Service

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

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

Previous Product Offering	Previous Product Offering	Description	Current Product Offering
DirectSecure (DS)	Isolation and Encryption Service		Still supported but no longer being developed or updated
	User Analytics Service		Privilege Threat Analytics Service

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

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

Contacting Centrify

You can contact Centrify by visiting our website, www.centrify.com. 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

This chapter provides an introduction to Centrify Express for Linux and UNIX, including a brief overview of how Centrify can help you take advantage of your investment in Active Directory.

Key components

Centrify bundles products and features in different editions to address different customer requirements. The Centrify Express family of products provides the most basic set of functionality and is available for free from the Centrify website.

The main Centrify components that enable cross-platform authentication and authorization services using Active Directory are platform-specific agents. Agents are packaged in compressed platform-specific files that you can download and extract to enable non-Windows computers to join an Active Directory domain. After you install an agent and join a domain, Active Directory users are authenticated on the UNIX or Linux computer without any further configuration.

The Centrify Express family of products also includes Kerberos-enabled versions of OpenSSH and PuTTY packages.

Features not supported by Centrify Express

Taken together, Centrify Express products provide a solid foundation of functionality that is suitable for many organizations without upgrading to Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service. However, Centrify Express does not provide central management of policies, delegated administration, identity control, role-based access rights, or auditing services.

If your organization outgrows the basic functionality of Centrify Express, you can upgrade to Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service to take advantage of these additional features.

The following table describes features that are limited or not enabled in Centrify Express.

Feature	Limitation in Centrify Express
Centralized identify and access management	You cannot centrally manage user and group profiles, control access privileges on specific computers, or delegate administrative activities.
Group policies	You cannot centrally manage configuration settings for non-Windows computers and users.
Auditing	You cannot audit user session activity.
Role-based authorization and access rights	You cannot define rights, roles, and role assignments to enforce role-based access to privileged commands and other operations.
Unlimited Centrify managed computers	The number of Centrify-managed computers that can be connected to the Active Directory domain at the same time is limited. The limit is described in the End User License Agreement (EULA) that is specific to Centrify Express.
User login controls	You can only use a limited set of parameters to control which users or groups are granted or denied access.
Active Directory lookup filtering	You cannot use the NSS override parameters to filter Active Directory lookups requests.
The adcert command	You cannot use the `adcert` command, which enables certificate operations to be performed directly on agent-managed UNIX computers.
Data isolation and encryption	You cannot dynamically isolate and encrypt data in motion.

You must upgrade to a license version of Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service to use any of these features.

Managed computers are Active Directory clients

The agent enables non-Windows servers and workstations to participate in an Active Directory domain as Active Directory clients. You install the agent on each computer that you want to make part of an Active Directory domain. After you install the agent and join a domain on a computer, the computer is considered a Centrify managed computer. The agent then manages the connection to Active Directory domain controllers when users log on or connect to the computer remotely.

What the agent does

The agent makes a computer look and behave like a Windows client computer to Active Directory. The agent performs the following key tasks:

- Joins the computer to an Active Directory domain.
- Communicates with Active Directory to authenticate users when they log on.
- Caches users credentials for offline access.
- Enforces Active Directory authentication and password policies.
- Provides a Kerberos environment so that existing Kerberos applications work transparently with Active Directory.

Agents consistent of multiple components

Agents provide an integrated set of services that enable programs and applications to use Active Directory. The core agent service is the `adclient` process. The `adclient` process handles all of the direct communication with Active Directory and coordinates with other services to process requests for authentication, authorization, directory assistance, or policy updates.

Other services handle specific types of operations. For example, the `pam_centrifydc` module enables any PAM-enabled program, such as `ftpd`, `telnetd`, `login`, and `sshd`, to authenticate using Active Directory. A custom NSS module modifies the `nsswitch.conf` configuration file so that system look-up requests use the information in Active Directory. A configurable local cache stores user credentials and other information for offline access and network efficiency.

In addition to the core agent services, agents can include Centrify-compiled versions of other programs, such as OpenSSH and OpenLDAP, to work with Active Directory.

Provisioning is automatic

When you deploy an agent on a computer, the agent adds the computer account to Active Directory and automatically creates consistent UIDs across the joined domain for Active Directory users with access to the computer. The agent authenticates all valid Active Directory users without any configuration or account management. Because there is only one zone for the forest, you can deploy without creating any zones of your own. Because profiles are generated automatically, you do not need to configure any zone properties or manage who has access to which subsets of UNIX and Linux computers.

Deciding whether to use zones

The primary reason to use Centrify Express is that it enables Active Directory authentication without any planning, manual configuration, or account management. A primary limitation to using Centrify Express is that all computers are placed in a single, automatically defined zone.

Zones provide a powerful and flexible structure for managing user identities, role-based access controls, and delegated administrative authority. However, deciding on the best strategy for using zones requires some planning and preparation. If your organization does not require more than one zone, you can begin deploying agents immediately.

Working with a single zone

Centrify Express is designed for organizations that do not want to centrally manage user profiles, role assignments, or administrative activities. After the agent is installed, all valid Active Directory users and groups in the entire Active Directory forest are automatically assigned a unique UNIX profile that allows them to log on. Because the Centrify Express agent requires no configuration or central management, it is most suitable for organizations that:

- want to add computers to a domain quickly without configuring any zones.
- do not need to maintain or manage existing UIDs and GIDs.
- have a limited number of users and domains.
- have a relatively flat organizational structure.

If a single zone suits the needs of your organization, Centrify Express provides a no-cost, cross-platform solution for authentication services. If your organization grows in size and complexity or if you want more granular access controls, you can upgrade to a licensed version of Centrify software at a later time. For more information about centrify service offerings and authentication, privilege elevation, and audit and monitoring services, see Comparing Centrify Express to other services.

All Active Directory users have access

After you install an agent and join an Active Directory domain, all of the users and groups in the Active Directory forest automatically become valid users and groups for the joined computer. In addition, all Active Directory users defined in any forest with a two-way trust relationship with the forest of the joined domain are valid users for the joined computer.

Note If a computer joins a domain and the domain has a one-way trust relationship with another domain, users and groups in the trusted domain **do not** become valid users and groups on the computer.

By default, all valid users can perform the following tasks:

- Log on interactively to the shell or a desktop program and use standard programs such as `telnet`, `ssh`, and `ftp`.
- Log on to a computer that is disconnected from the network or unable to access Active Directory, if they have successfully logged on and been authenticated by Active Directory previously.
- Manage their Active Directory passwords directly from the command line, provided they can connect to Active Directory.

How the agent generates profile attributes

Computers with a Centrify Express agent always connect to the domain through the Auto Zone. In the Auto Zone, user profile attributes, such as the UID, default shell, and home directory are automatically derived from user attributes in Active Directory or from configuration parameters. No local account information is used or migrated into Active Directory.

When an Active Directory user logs on to a UNIX or Linux computer for the first time, the agent automatically creates a 31-bit UID for the user and a 31-bit GID for any groups to which the user belongs. To create unique GIDs and UIDs, the agent creates a prefix from the last 9 bits of the user or group Security Identifier and combines it with the lower 22 bits of the user or group relative identifier (RID).

Although the agent caches these UID and GID values, they are not stored in Active Directory. You cannot edit or change them in any way with Active Directory Users and Computers (ADUC). If the cache expires, the agent uses the same algorithm to create the same UID and GID the next time the user logs on so you are guaranteed consistent ownership for files and resources. In addition, users who log on to more than one computer will have the same generated UID on each managed computer.

Note All profile attributes—including the UID and GID values—are stored in Active Directory. If you upgrade to a licensed version of Centrify software, you can migrate and manipulate UID and GID properties for individual computers. You can also map multiple UIDs to a single Active Directory account to allow different UIDs settings on different computers for the same user account. This type of manipulation is not possible when using Auto Zone and Centrify Express agents.

In addition to the UID and GID, the agent automatically creates a home directory for the user with all the associated profile and configuration files. The location for the home directory is:

- UNIX or Linux: `/home/`username
- Mac OS X: `/Users/`username

Deploying an agent does not affect local users. User accounts that are defined in the local `/etc/passwd` directory can still log on. If you want to control access through Active Directory, however, you should create Active Directory accounts for each user. After you verify user access for the Active Directory user, you can then either delete the local account, or map the local users on each computer to an Active Directory account to preserve access to current home directories and files. For more information about mapping accounts, see Mapping local accounts to Active Directory.

Using Centrify Express to deploy agents

With Centrify Express, you can discover and analyze computers on your network or in the cloud, then download and install or update the correct agent for each discovered computer. You can also use Centrify Express to manage account information for remote UNIX users and groups, and run programs on the computers discovered.

Like other Centrify products, you can download Express agents from the Centrify website.

Comparing Centrify Express to other services

Centrify Express provides a subset of the features available in authentication and privilege elevation services. Over time, this basic set of functionality may be insufficient. Depending on the needs of your organization, you may want to upgrade the authentication, privilege elevation, and audit and monitoring services you use to take advantage of additional feature sets. The following table provides a brief description of the services available.

Product offering	Description
Centrify Express	Free software that provides basic integration with Active Directory for authenticating users.
Application services	Commercial offering that enables you to secure every user's access to web and mobile applications. With application services, you can provide single sign-on capability and enforce multi-factor authentication when and where it is needed. You can also define policies to control access to applications and the use of mobile devices.
Endpoint services	Commercial offering that enables you to manage and secure Mac, Windows, and Linux endpoints. With endpoint services, you can establish common cross-platform policies for remote access, the use of smart cards and

Product offering	Description
	derived credentials, and multi-factor authentication.
Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service	Commercial offering that provides a full complement of services to ensure the security of your infrastructure and prevent the breaches that can result when privileged accounts are compromised. With Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service, you can protect your organization in a variety of ways. For example, you can:: ▪ Require users to log in as themselves. ▪ Enforce least-privilege access for administrators and end-users. ▪ Control shared access to privileged accounts. ▪ Audit and monitor user activity and what takes place during privileged sessions. ▪ Isolate and encrypt sensitive information transmitted over the network.

Installing Centrify agents

This section provides step-by-step instructions for installing the Centrify agent on a computer and joining the computer to the Active Directory domain.

Selecting a deployment option

The agent must be installed on each computer you want to manage. You must also specify an Active Directory domain for the agent to join either during the installation process or after the agent files are installed.

You can install and manage agent packages independently by running an installation script, package management program, or software distribution tool locally or remotely on individual computers.

For more information, see Options for deploying agent packages.

Installing and using CentrifyExpress

Centrify Express provides a Windows-based MMC console and a self-contained database that stores information about the computers and accounts discovered on the network or in the cloud.

Minimum hardware requirements

You can install Express on a single Windows computer with a 64-bit operating system.

In general, Centrify recommends the following minimum hardware configuration:

- 2 GB RAM
- 1 GB free disc space
- 2 GHz processor

Network connectivity requirements

To download and deploy software, you must have network connectivity or an Internet connection between the Windows computer where Access Manager is installed and the computers where you want to deploy the agent. Centrify recommends that you install Access Manager on a computer that allows outbound Internet connections and connectivity between the Windows computer and each computer you want to manage.

Account credential requirements

To install software on remote computers and join Active Directory domains, you must have access to an account with appropriate permissions:

- To run privileged commands, you should have access to the `root` account, the local Administrator account, or an account that has been granted escalated privileges using `su` or `sudo` and settings in a `sudoers` configuration file.
- To join a domain, you need an Active Directory account and password that has permission to add computers to the domain.

Depending on your organization, the Active Directory account might be required to be a member of the Domain Admins group. If you are not sure whether you have permission to add computers to the domain using your own Active Directory account, check with the Active Directory administrator for your site.

Download the software and run the setup program

If you have a computer that meets the requirements and the appropriate account information, you can download Express.

To download and install Centrify Express:

1. Go to the Centrify website and register an account, if you have not previously registered
2. Click the **Download** link.
3. Open the downloaded file to start the setup program.
4. Follow the prompts displayed to accept the license agreement and select a location for program files.
5. Install the agents on the desired computers. For details, see Options for deploying agent packages.

Options for deploying agent packages

You can download individual Centrify agent packages for the platforms you support and install the software in one of the following ways:

- Run the installation script (`install-express.sh`) locally on any computer and respond to the prompts displayed.
- Create a configuration file and run the installation script remotely on any computer in silent mode.
- Use the install or update operations in the native package installer for your operating environment.

If you want to use one of these installation options and need more information, see the appropriate section.

Install interactively on a computer

You must install a platform-specific agent on each computer you want to manage through Active Directory.

The installation script automatically checks the operating system, disk space, DNS resolution, network connectivity, and other requirements on a target computer before installing. You can run this script interactively on any supported UNIX, Linux, or Mac computer and respond to the prompts displayed.

To install agent packages on a computer interactively:

1. Go to the Centrify website and download the Centrify Express agent for the platform you want to support.
2. Select the file you downloaded and unzip and extract the contents using the appropriate operating system commands. For example:

   ```
   gunzip -d centrify-package-platform-arch.tgz
   tar -xf centrify-package-platform-arch.tar
   ```

3. Run the `install-express.sh` script to start the installation on the local computer. For example:

   ```
   ./install-express.sh
   ```

4. Follow the prompts displayed to check the computer for potential issues, install the agent, and join a domain automatically at the conclusion of the installation.

   If the `adcheck` program finds potential issues, you might see warning or error messages. Depending on the issue reported, you might have to make changes to the computer before continuing or after installation.

   For most prompts, you can accept the default by pressing Enter. When prompted for the Active Directory domain, type the fully qualified name of the Active Directory domain to join.

   You must also type the user name and password for an Active Directory user with permission to add computers to the domain.

5. After you have responded to all of the prompts displayed, review your selections, and then enter **Y** to continue with the installation and reboot the computer.

Using other programs to install

If you want to manually install a software package using a native installation program instead of the installation script, use the installation commands and options that are appropriate for the local operating environment. For example, if your operating system supports a package installer, such as Red Hat Package Manager (`rpm`), SMIT or YAST programs, you can use any of those programs to install the agent.

Note Centrify recommends that you use the installation script to automatically check a computer for issues and join the computer to a domain.

To install an agent using a native installation program:

1. Log on as or switch to the `root` user.
2. If the software package is a compressed file, unzip and extract the contents. For example, on Red Hat Linux:

   ```
   gunzip -d centrify-*-rhel5-x86_64.tgz
   tar -xf centrify-*-rhel5-x86_64.tar
   ```

3. Run the appropriate command for installing the package based on the local computer's operating system or package manager you want to use. For example, on Red Hat Linux:

   ```
   rpm -Uvh centrifydc-*-rhel5-x86_64.rpm
   ```

4. Disable licensed features by running the `adlicense --express` command:

   ```
   adlicense --express
   ```

   Note You must run the `adlicense` command to set the agent to run in Express mode.

5. Join the domain by running the `adjoin --workstation` command, which connects you to Auto Zone:

   ```
   adjoin --workstation domainName
   ```

   Note If you do not specify the `--workstation` option, the join operation will fail because `adjoin` will attempt to connect you to a specific zone rather than Auto Zone.

Verifying the installation

When a computer is joined to Active Directory, all Active Directory users and groups defined for the forest, as well as any users defined in a two-way trusted forest, are valid users or groups for the joined computer. Therefore, after running the agent and joining the computer to a domain, you can log on as any Active Directory user.

1. Log on using an Active Directory user account.

   When a user logs in for the first time, the agent automatically creates a home directory for the new user.

2. Run the `adinfo` command to see information about the Active Directory configuration for the local computer. You should see output similar to the following:

   ```
   Local host name:   QA1
   Joined to domain:  sales.acme.com
   Joined as:         QA1.sales.acme.com
   Pre-win2K name:    QA1
   Current DC:        acme-dc1.sales.acme.com
   Preferred site:    Default-First-Site
   Zone:              Auto Zone
   Last password set: 2014-04-01 12:01:31 PST
   CentrifyDC mode:   connected
   Licensed Features: Disabled
   ```

   Note that licensed features are disabled and that the zone is Auto Zone. Creating actual zones requires a licensed copy of Centrify software.

Troubleshooting adcheck errors

You can run `adcheck` before, during, or after installation to verify that your computer is configured properly. This utility performs three sets of checks that are controlled by the following options:

- `-t os` checks the operating system, disk size, and Perl and Samba installations.
- `-t net` checks DNS to verify that the local computer is configured correctly and that the DNS server is available and healthy.
- `-t ad` includes the `-t net` checks and verifies that the domain has a valid domain controller.

Correcting errors for the operating system check

The `-t os` option performs a series of checks that verify operating-system basics for the computer on which you are installing the agent. If your computer fails one of these checks, upgrade the computer with a new operating system version, required patch, a new Perl or Samba version, or free up sufficient disk space.

Correcting warnings and errors for the network check

The `-t net` option performs a series of checks that verify that DNS is correctly configured on your local computer and that the DNS server is running properly. There is also a check to verify that you are running a supported version of OpenSSH.

Note A supported version of OpenSSH is not automatically installed. You must choose to install it during a custom installation.

Because the agent uses DNS to locate the domain controllers for the Active Directory forest, the appropriate DNS nameservers need to be specified in the local `/etc/resolv.conf` file on each computer before the computer can join the domain. If you receive errors or warnings from these checks, you need to correct them before joining a domain. Each warning or error message provides some help to resolve the problem.

Correcting errors for the domain controller check

The `-t ad` option locates each domain controller in DNS and then does a port scan and DNS lookup of each. The checks for this option also verify the global catalog and verify clock and domain synchronization.

If you receive errors or warnings from these checks, you need to correct them before joining a domain. Each warning or error message provides some help to resolve the problem.

Joining a domain after installation

When you install the agent using `install-express.sh`, you can automatically join that computer to an Active Directory domain. If you do not join the domain when you run the installation script, or if you leave a domain and want to rejoin, you can manually join a domain by using the `adjoin` command.

To manually join a domain, you must use the `--workstation` option to connect to Auto Zone.

To join an Active Directory domain manually on a Linux or UNIX computer:

1. Log in as or switch to the root user.
2. Run adjoin to join an existing Active Directory domain. You should join the domain using a fully-qualified domain name. You must specify the --workstation option.

   For example, to join the sales.acme.com domain with the user account dylan:

   ```
   adjoin --user dylan --workstation sales.acme.com
   ```

   The user account you specify must have permission to add computers to the specified domain. In some organizations, this account must be a member of the Domain Admins group. In other organizations, the account simply needs to be a valid domain user account. If you don’t specify a user with the --user option, the Administrator account is used by default.
3. Type the password for the specified user account.

If the agent can connect to Active Directory and join the domain, a confirmation message is displayed. All Active Directory users and groups defined for the forest, as well as any users defined in a two-way trusted forest are valid users or groups for the joined computer.

Restarting services

You may need to restart some services on computers where you have installed the agent so that those services will reread the name switch configuration file. For example, if you typically log on to the computer through a graphical desktop manager such as gdm, you need to either restart the gdm service or reboot the workstation to force the service to read the updated configuration before Active Directory users can log on.

The most common services that need to be restarted are sshd and gdm. If you are using these services, you should restart them. For example, to restart sshd:

```
/etc/init.d/sshd restart
```

As an alternative to restarting individual services, you can reboot the system to restart all services.

Note Because the applications and services on different servers may vary, Centrifyrecommends you reboot each computer to ensure all of the applications and services on the system read the configuration changes at your earliest convenience.

Upgrading Centrify Express

To take advantage of features that are part of Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service—for example to define roles that control access rights and apply group policies to computers and users—you must upgrade from Centrify Express to a licensed copy of Centrify Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service. Upgrading to a licensed version of the product is a three-stage process that involves:

- Installing and upgrading components on Windows.
- Upgrading the agent to enable licensed features on managed UNIX and Linux computers.
- Adding optional packages that are not included in Centrify Express.

Upgrading Windows components

If you are upgrading to a licensed version of authentication, privilege elevation, and audit and monitoring services, there are several additional components available for you to install depending on the services you want to deploy. For example, there are console extensions that enable you to edit group policies and manage NIS maps through Active Directory.

To install and upgrade licensed components on Windows:

1. Obtain a license key and media for Centrify Management Services.

You can also download an evaluation copy directly from the Centrify website, but you must have a license key to use the software for more than a limited period of time.

2. On a Windows computer that is joined to the Active Directory domain, connect to the distribution media.

   If you received the software on a CD, the Getting Started page is displayed automatically or when you double-click the `autorun.exe` program.

3. Click Authentication & Privilegeto start the setup program for authentication and privilege elevation components.
4. Follow the prompts displayed to accept the license agreement, select the components to install, and a location for files.
5. When setup is complete for the selected packages, click **Finish** to close the setup program.

Upgrading agents on managed computers

To upgrade agents to a licensed product, you must run a command line program to enable licensed features on each managed computer.

To enable licensed features on managed computers:

1. Log on to the computer that is running a Centrify Express agent.
2. Run the following command to search the Active Directory forest for the license key and to enable licensed features.

   ```
   adlicense --licensed
   ```

3. Run the following command to verify that licensing has been enabled:

   ```
   adinfo
   ```

   ```
   Local host name:   qa1
   Joined to domain:  acme.com
   Joined as:         qa1.acme.com
   Pre-win2K name:    qa1
   Current DC:        acme-dc1.acme.com
   Preferred site:    Default-First-Site
   Zone:              Auto Zone
   Last password set: 2014-04-01 12:01:31 PST
   CentrifyDC mode:   connected
   Licensed Features: Enabled
   ```

Note After enabling licensed features, the computer is still connected to Auto Zone. If you are not using zones to migrate existing user populations or define role-based access controls, you can leave the computer in Auto Zone. If you want to take advantage of zones, you must:

- Create at least one zone using Access Manager, `adedit`, or another tool.
- Run `adleave` to leave the Active Directory domain and Auto Zone.
- Run `adjoin` to rejoin the Active Directory domain and a specified zone.

For information about creating and managing zones, using group policies, and other features, see the *Planning and Deployment Guide* and the *Administrator's Guide for Windows*.

Adding optional packages after installation

Depending on the services you choose to deploy, there are several optional packages that might be available for you to use. To add these packages, you must rerun the installation script and select which packages to install.

To add optional packages on computers where the agent is installed:

1. Change to the appropriate directory on the CD or to the directory where you have copied or downloaded the agent package.
2. Run the standard installation script for the agent and follow the prompts displayed:

   ```
   ./install.sh
   ```

3. When you are prompted whether to keep, erase, or reinstall the currently installed packages:
   - Accept the default (**K**, keep) for the currently installed packages.
   - Type Y (**Y**, yes) for each package you want to add.
4. Follow the prompts displayed to set installation options, such as the

option to run adcheck and reboot the computer after installation.

The computer remains joined to the domain you previously joined, your existing /etc/centrifydc/centrifydc.conf file is backed up, and any modifications you have made to the file are migrated to the new version of the file.

5. Restart running services, such as login, sshd, or gdm, or reboot the computer to ensure all services use the updated configuration.

Removing Centrify Express

On most managed computers, you can remove the agent and related files by running the uninstall.sh script. The uninstall.sh script is installed by default in the /usr/share/centrifydc/bin directory on each managed computer.

To remove the agent on a managed computer:

1. Log on to the computer where the agent is installed.
2. Run the uninstall.sh script. For example:

   ```
   /bin/sh /usr/share/centrifydc/bin/uninstall.sh
   ```

   The uninstall.sh script will detect whether the agent is currently installed on the local computer and will ask you whether you want to uninstall your current installation.
3. To uninstall, enter Y when prompted.

If you cannot locate or are unable to run the uninstall.sh script, you can use the appropriate command for the local package manager or operating environment to remove the agent and related files.

Working with managed computers

This chapter explains how to perform common administrative and end-user tasks on managed computers that have the Centrify agent installed.

Logging on to your computer

You log on to a joined computer in the same way you log on locally. For example, you type a user name and password to start a console session, remote shell session, or a desktop manager. In most cases, you do not have to specify the domain name when you log on. However, you do need to type the Active Directory password for your account and the password must conform to the password policies defined for the domain.

You can use any of the following formats for the user name when you log on:

- Active Directory `samAccountName` or Mac OS X short name (`jcool`)
- Active Directory `userPrincipalName` (`jcool@acme.com`)
- Windows NTLM format for domain and user name (`acme.com\jcool`)

You can also use any of these formats to locate users in Active Directory.

By default, the Centrify agent uses the Active Directory `samAccountName` attribute or the Mac OS X short name for the UNIX profile user name. You can specify a different form for the UNIX user name by setting the value of the auto.schema.name.format parameter in the `/etc/centrifydc/centrifydc.conf` configuration file.

Getting configuration information

After you log on to a computer, you can use the `adinfo` command to see information about the Active Directory configuration for the local computer. For example, type `adinfo` to display a summary similar to the following:

```
Local host name:   QA1
Joined to domain:  sales.acme.com
Joined as:         QA1.sales.acme.com
Pre-win2K name:    QA1
Current DC:        acme-dc1.sales.acme.com
Preferred site:    Default-First-Site
Zone:              Auto Zone
Last password set: 2014-04-01 12:01:31 PST
CentrifyDC mode:   connected
Licensed Features: Disabled
```

For Centrify Express, licensed features are disabled and the only zone supported is Auto Zone. If you upgrade at a later time, the licensed features will be enabled, and you will be able to use zones to provide secure, granular access control and delegated administration for computers joined to a domain.

Applying password policies

The agent enforces all of the password policies you have defined in Active Directory for all valid user accounts in the forest. For example, if your policy requires that new users must change their password the next time they log on, they are prompted to change the password at the next log-on whether they use a Windows or UNIX computer.

The agent also checks passwords to make sure that they conform to Active Directory policies for length and complexity. If a new or changed password meets all of the criteria, the account is updated with the new information in Active Directory and the user logs on successfully.

If you have defined additional policies, such as a maximum duration, reuse policy, failed attempt and account lock out policy, workstation restrictions, and logon hour restrictions, the agent also enforces those policies. Like Windows, the agent displays a warning message each time a user logs on if the user’s password is set to expire in a given number of days.

Changing passwords

As an administrator, you can set, reset, or change the password for other users using Active Directory or from the UNIX command line. Individual users can also change their own password at any time using the `adpasswd` command.

Changing your own password

If you attempt to log on but your password has expired, you are prompted to provide your old password, a new password, and to confirm your new password. You can also change your own password at any time using `adpasswd`.

To change your own password

1. At the UNIX command line, run the following command:

   ```
   adpasswd
   ```

2. Type your old password. When changing your own password, you must always provide your old password.
3. Type the new password. The password should conform to Active Directory password policies.
4. Retype the new password.

For more information about using `adpasswd`, see the `adpasswd` man page.

Changing another user's password

You can use the `adpasswd` command to change the password of another Active Directory user if you provide the user name and password of an administrative account with the authority to change another user's password.

To change the password for another user

1. At the UNIX command line, run the adpasswd command and specify an Active Directory administrative account name with the authority to change the password for users in the domain. For example, to use the admin user account to change the password for the user jane in the sales.acme.com domain:

   ```
   adpasswd --adminuser admin@acme.com jane@sales.acme.com
   ```

2. Type the password for the administrative account. For example:

   ```
   Administrator password: xxx
   ```

3. Type the new password for the user specified. Because you are changing another user’s password, you are not prompted for an old password. For example:

   ```
   New password:
   ```

4. Retype the new password.

   ```
   Repeat password:
   ```

For more information about using adpasswd, see the adpasswd man page.

Working in disconnected mode

After an Active Directory user logs on to a computer successfully, the authentication is cached on the local computer. These credentials can then be used to authenticate the user in subsequent log on attempts if the user is disconnected from the network or if an Active Directory domain controller is not available.

If there are changes to an account while the account is running in disconnected mode, the changes do not take effect until the user reconnects to Active Directory to start a new session or access a new service. For example, if a user account is disabled or has its password changed in Active Directory while the user is disconnected from the network, the user can still log on and use the old password until reconnected to the network. After the user reconnects to Active Directory, the changes take effect and the user is denied access or prompted to provide an updated password. Because changing the password for an Active Directory account requires a connection to an Active Directory domain controller, users cannot change their own Active Directory password when working in disconnected mode.

Note If users log out of a session while disconnected from Active Directory, they can be authenticated using the information in the cache when they log back on because they have been successfully authenticated in a previous session. They cannot, however, be authenticated automatically to any additional services after logging back on. To enable automatic authentication for additional services, the user's credentials must be presented to the Key Distribution Center (KDC) then issued a ticket that can be presented to other services for unprompted, single sign-on authentication. Because the KDC is unavailable when disconnected from Active Directory, single sign-on authentication is also unavailable.

You can configure many aspects of how credentials are handled, including how frequently they are updated or discarded, through parameter settings in the `centrifydc.conf` configuration file. To configure how credentials are handled using group policies, you must upgrade to a licensed version of Centrify software.

Mapping local accounts to Active Directory

By default, local user accounts are valid on the computers that join the Active Directory domain. In some cases, you may want to manually map a local user account to an Active Directory account instead of using a generated profile. Mapping a local user account to an Active Directory account gives you Active Directory-based control over password policies, such as password length, complexity, and expiration period.

Note Mac OS X users can always log on using their local account password. Therefore, you cannot enforce Active Directory password policies for local Mac OS X user accounts.

Mapping local accounts to Active Directory is especially useful if you want to preserve access to a user's current home directory and files. For example, if a local user has a UID of 518 but the Centrify agent generates a different UID for the user's profile, that user will not have file ownership permissions for his home directory and files.

To map a local account to an Active Directory account, you can set the `pam.mapuser.username` configuration parameter on any individual local computer. To configure account mapping using group policies, you must upgrade to a licensed version of Centrify software.

Using the pam.mapuser parameter

To map a local user account to an Active Directory user by modifying the local `centrifydc.conf`configuration file:

1. Create the Active Directory user account to use.

   On your Windows Active Directory computer, open Active Directory Users and Computers (ADUC). Navigate to the Users node, right click and select **New > User**.

   You should create a user logon name with the same name as the local user.

2. On the computer with the local account, open the `centrifydc.conf` configuration file.

3. Locate the `pam.mapuser.`*username* configuration parameter and un-comment the line to change the default setting.

4. Modify the local account mapping to identify the local user account you want mapped to the Active Directory user you created. For example:

   ```
   pam.mapuser.joe.cool: joe.cool
   ```

5. Save the changes to the configuration file, then run the `adreload` command to reload the configuration file and have the changes take effect.

Setting a local override account

In most cases, every computer should have at least one account that can be authenticated locally to ensure that you can access the system when the network or Active Directory is not available or `adclient` is not running. By default, the local override account is set to the `root` user so that even if you map the `root` account to an Active Directory account, you can always log on locally using `root@localhost` and the local `root` account password.

You can change the default `root` override account or add additional local users by modifying the computer’s `centrifydc.conf` configuration file. To configure a local override account using group policies, you must upgrade to a licensed version of Centrify software.

Using native telnet, ssh, and ftp programs

By default, authorized users can use standard programs and services such as `telnet`, `ssh`, and `ftp`. For `telnet` and `ftp`, you can use the packages installed with the operating system. For `ssh` operations, however, Centrify recommends that you install the Centrify-compiled version of OpenSSH instead of using the package provided with the operating system. You can download a free copy of OpenSSH from the Centrify website.

Using Samba

Centrify Express supports the `adbindproxy` package, which contains the components to enable an open-source Samba file server to use the Centrify agent and Active Directory to handle identity management and user credentials.

For more information, see the *Samba Integration Guide*.

Setting Auto Zone configuration parameters

Centrify agents support a set of configuration parameters specifically intended for computers that are connected to a domain through Auto Zone.

Because Auto Zone is a single zone for an entire forest, you can encounter problems such as UID and GID conflicts and slow searches. If you encounter these problems, you may need to modify the default configuration. For information about how to set specific parameters to resolve UID and GID conflicts or improve search performance, see Customizing operations using configuration parameters

Troubleshooting tips and tools

This chapter describes how to use diagnostic tools and log files to retrieve information about the operation of Centrify agents and provides tips to help you identify and correct problems on managed computers.

Addressing log on failures

In most cases, valid Active Directory users should be able to log on to computers where you have deployed the agent without any configuration. If an attempt to log on fails, the problem is typically caused by one of the following:

- Users attempting to log on to a computer they are not authorized to use.
- Users do not have a valid Active Directory user account in the appropriate forest.
- Users have typed their non-Active Directory password or typed the wrong password more times than allowed.

If users report that they cannot access computer resources they think they should have access to, take the following steps to troubleshoot the problem:

1. Verify that the user has an Active Directory user account in the forest or in a forest with a two-way trust relationship.
2. Check that the account is not disabled or locked out because of repeated log-on failures.
3. Verify that there is an Active Directory domain controller available and

that the computer a user is unable to log on to can connect to it and open a communication channel.

For example, log on to the UNIX computer using a locally authenticated user, and run the `ping` command with the name of a domain controller in the forest. If the command receives a reply from the domain controller, the DNS service is functioning and the local computer is able to locate the domain controller on the network.

If the `ping` command does not generate a reply, check your DNS configuration and check whether the local computer or the domain controller is disconnected from the network.

4. Use `adinfo` or Active Directory Users and Computers to check that the computer is joined to the domain.

5. Use `adinfo` to check whether the agent is currently running or disconnected.

   If the `adinfo` command reports the mode is `disconnected`, try restarting `adclient` and testing network response time. On a slow network, `adclient` may drop the connection to Active Directory if there is a long delay in response time.

   If the `adinfo` displays an `<unavailable>` error, try running `adleave` to leave Active Directory, re-run the `adjoin` command to re-join the domain. If a problem still exists, check the DNS host name of the local computer and the domain controller, the user name joining the domain, and the domain name you are using.

6. Check the clock synchronization between the local computer and the Active Directory domain controller.

   If the clocks are not synchronized, reset the system clock on the managed computer using the `date` command.

7. Check the contents of the system log files or the `centrifydc.log` file after the user attempts to log on. You can use information in this file to help determine whether the issue is with the configuration of the software or with the user’s account.

8. Check for conflicts between local user accounts and the user profile generated by the agent.

If these steps do not reveal the problem, you can enable detailed logging of `adclient` activity using the `addebug` command. You can use the information in the `/var/log/centrifydc.log` file to further diagnose the problem or to provide information to Centrify Support.

Understanding diagnostic tools and log files

The agent includes some basic diagnostic tools and a comprehensive logging mechanism to help you trace the source of problems if they occur. These diagnostic tools and log files allow you to periodically check your environment and view information about agent operation, Active Directory connections, and the configuration settings for individual computers you manage.

Logging is not enabled by default for performance reasons. Once enabled, however, log files provide a detailed record of agent activity. This information can be used to analyze the behavior of `adclient` and communication with Active Directory to locate points of failure. However, log files and other diagnostic tools provide an internal view of operation and can be difficult to interpret. The log files are primarily intended for Centrify Support and technical staff.

In most cases, you should only enable logging when you need to troubleshoot unexpected behavior, authentication failures, or problems with connecting to Active Directory or when requested to do so by Centrify Support. Other troubleshooting tools, such as command line programs, can be used at any time to collect or display information about your environment.

Configuring logging

By default, the agent logs errors, warnings and informational messages in the `syslog` and `/var/log/messages` files along with other kernel and program messages. Although these files contain valuable information for tracking system operations and troubleshooting issues, occasionally you may find it useful to activate Centrify-specific logging and record that information in a log file.

Enabling logging for the agent

To enable logging on the agent:

1. Log in as or switch to the `root` user.
2. Run the `addebug` command:

   ```
   /usr/share/centrifydc/bin/addebug on
   ```

   Note You must type the full path to the command because `addebug` is not included in the path by default.

   After you run this command, all of the agent activity is written to the `/var/log/centrifydc.log`file. If the `adclient` process stops running while you have logging on, the `addebug` program records messages from PAM and NSS requests in the `/var/centrifydc/centrify_client.log` file. Therefore, you should also check that file location if you enable logging.

For performance and security reasons, you should only enable logging when necessary. For example, if you open a case with CentrifySupport, the Support representative may request that you enable logging and submit log files to investigate your case. You should also limit logging to short periods of time while you or Centrify Support attempt to diagnose a problem. You should keep in mind that sensitive information may be written to this file and you should evaluate the contents of the file before giving others access to it.

When you are ready to stop logging activity, run the `addebug off` command.

Setting the logging level

You can define the level of detail written to the log by setting the `log` configuration parameter in the `centrifydc.conf` configuration file:

```
log: level
```

With this parameter, the log level works as a filter to define the type of information you are interested in and ensure that only the messages that meet the criteria are written to the log. For example, if you want to see warning and error messages but not informational messages, you can change the log level from `INFO` to `WARN`. By changing the log level, you can reduce the number of messages included in the log and record only messages that indicate a problem. Conversely, if you want to see more detail about system activity, you can change the log level to `INFO` or `DEBUG` to log information about operations that do not generate any warnings or errors.

You can use the following keywords to specify the type of information you want to record in the log file:

Specify this level	To log this type of information
`FATAL`	Fatal error messages that indicate a system failure or other severe, critical event. In addition to being recorded in the system log, this type of message is typically written to the user’s console. With this setting, only the most severe problems generate log file messages.
`ERROR`	System error messages for problems that may require operator intervention or from which system recovery is not likely. With this setting, both fatal and less-severe error events generate log file messages.
`WARN`	Warning messages that indicate an undesirable condition or describe a problem from which system recovery is likely. With this setting, warnings, errors, and fatal events generate log file messages.
`INFO`	Informational messages that describe operational status or provide event notification.

Logging details for a specific component

By default, when you specify a logging level, it applies to all of the agent components that log activity. The logging system, however, provides a hierarchical organization of logical log names for the components within the agent and each of these logical logs can be configured to provide more targeted analysis of it specific operations. For example, if you set your base logging level to only report serious errors but you want to see informational, warning, and error messages for `adclient`, you can add a separate logging level parameter for the log messages generated by `adclient`:

```
# Use the following setting to set the base level of detail
# for logging to record Error messages:
log: ERROR


# Add the name of the adclient logical log and specify the
# logging level to use for it and its children:
log.com.centrify.adclient: INFO
```

Logging to the circular in-memory buffer

If the adclient process is interrupted or stops unexpectedly, a separate watchdog process (cdcwatch) automatically enables an in-memory circular buffer that writes log messages passed to the logging subsystem to help identify what operation the adclient process was performing when the problem occurred. The in-memory buffer is also mapped to an actual file, so that if there is a system crash or a core dump, the last messages leading up to the event are saved. Messages from the in-memory circular buffer have the prefix _cbuf, so they can be extracted from a core file using the strings command.

The in-memory circular buffer allows debug-level information to be automatically written to a log file even if debugging is turned off. It can be manually enabled by restarting the adclient process with the -M command line option. The default size of the buffer is 128K, which should be sufficient to log approximately 500 messages. Because enabling the buffer can impact performance, you should not manually enable the circular buffer or modify its size or logging level unless you are instructed to make the changes by Centrify Support.

Collecting diagnostic information

You can use the adinfo command to display or collect detailed diagnostic and configuration information for a local computer. Options control the type of information and level of detail displayed or collected. The options you are most likely to use to collect diagnostic information are the --config, --diag, or --support options, which require you to be logged in as root. You can redirect the output from any adinfo command to a file for further analysis or to forward information to CentrifySupport.

For more information about the options available and the information returned with each option, see the adinfo man page.

To display the basic configuration information for the local computer, you can type:

```
adinfo
```

If the computer has joined a domain, this command displays information similar to the following:

```
Local host name:   magnolia
Joined to domain:  ajax.org
Joined as:         magnolia.ajax.org
Current DC:        ginger.ajax.org
Preferred site:    Default-First-Site-Name
Zone:              Auto Zone
Last password set: 2014-04-01 14:47:57 PST
CentrifyDC mode:   connected
Licensed Features  Disabled
```

Resolving Domain Name Service (DNS) issues

In some cases, you may encounter problems with authentication, authorization, or lookup requests because of your DNS configuration. The most common scenarios are:

- The Windows DNS server role is not configured to dynamically update service locator (SRV) records. These records enable Active Directory to find the nearest domain controller, Key Distribution Center (KDC), and Global Catalog (GC) for the site.
- The DNS servers do not publish the SRV records for the domain controllers that provide Active Directory service to the enterprise. These records must be available for computers to connect to Active Directory and locate required services.
- The DNS servers for the enterprise run on UNIX servers that are not configured to locate Active Directory domain controllers. In many cases, DNS servers for an enterprise are configured with a different domain namespace than Active Directory or Active Directory domain controllers are considered internal servers and not registered in the enterprise DNS.

If you encounter problems, you should contact your Active Directory administrator to determine whether the DNS server role is being used and if it is configured to allow dynamic updates. If the Active Directory DNS server role is not being used to provide DNS to the enterprise, you should contact the DNS administrator to resolve the issue.

There are several possible scenarios:

- If the enterprise uses UNIX-based DNS servers instead of Active Directory-based DNS servers and DHCP, computers should have a `snameserver` entry in `/etc/resolv.conf` file that points to a valid DNS server.

- Forward and reverse lookup zones should be configured to allow enterprise DNS servers to locate Active Directory domain controllers.
- If the Active Directory domain namespace is different from the namespace registered in enterprise DNS servers, you should use the `--name` and `--alias` join option to resolve the namespace differences.
- If the enterprise DNS servers do not include records for Active Directory domain controllers, you can manually set the location of the Active Directory domain controller using parameters in the `centrifydc.conf` configuration file.

Using command-line programs

Command-line programs allow you to perform basic Active Directory administrative tasks directly from a UNIX shell or using a shell script. These commands use the underlying agent service library to enable you to perform administrative tasks, such as adding computers to an Active Directory domain, leaving the Active Directory domain, changing Active Directory passwords, and returning detailed Active Directory, network, and diagnostic information for a host computer.

Understanding when to use command-line programs

Command-line programs are installed by default when you install the agent on a computer. Depending on the operating system, the commands are typically installed in one of the following directories:

```
/usr/sbin
/usr/bin
/usr/share/centrifydc/bin
```

In general, you should only use command-line programs when you must take action directly on a local computer. For example, if you want to join or leave a domain or set a new password while logged on to a shell, you may want to run a command interactively from that shell. You can also use command-line programs in scripts to perform administrative tasks programmatically.

Supported command-line programs

Centrify Express supports the following command-line programs:

Program	Description
`adcache`	The `adcache` program enables you to manually clear the local cache on a computer or check a cache file for a specific key value.
`adcheck`	The `adcheck` program verifies whether a local computer meets the system requirements for joining an Active Directory domain. This command checks whether the computer has sufficient disk and memory, a supported operating system and patch level, required libraries, and network connectivity to an Active Directory domain.
`adclient`	The `adclient` program manages most agent operations, and is normally started automatically when a computer starts up. In most cases, you should only run adclient directly from the command line if Centrify Support recommends you do so.
`addebug`	The `addebug` program starts or stops logging activity for agent operations.
`addns`	The `addns` program enables you to dynamically update DNS records on an Active Directory-based DNS server in environments where the DHCP server cannot update DNS records automatically.
`adedit`	The `adedit` program enables you to manage Active Directory and the agent through command-line commands and scripts.
`adfinddomain`	The `adfinddomain` program displays the domain controller associated with the Active Directory domain you specify.
`adfixid`	The `adfixid` program resolves UID and GID conflicts and enables you to change the ownership of a local user's files to match the user and group IDs defined for the user in Active Directory.
`adflush`	The `adflush` program clears the cache on a local computer.
`adid`	The `adid` program displays the real and effective UIDs and GIDs for the current user or a specified user.
`adinfo`	The `adinfo` program displays summary or detailed diagnostic and configuration information for a computer and its Active Directory domain.
`adjoin`	The adjoin program adds a computer to an Active Directory domain. This command configures a local computer to use Active Directory. No changes are made to authentication services or configuration files on a computer until you run the adjoin command. This command requires you to be logged on as root.
`adkeytab`	The `adkeytab` program enables you to create and manage Kerberos key tables (*.keytab files) and coordinate changes with the Kerberos key distribution center (KDC) provided by Active Directory.
`adleave`	The `adleave` program enables you to remove a computer from its current Active Directory domain or from the Active Directory forest entirely.

Program	Description
`adlicense`	The `adlicense` program enables or disables licensed features on a local computer. This command requires you to be logged on as root.
`adpasswd`	The `adpasswd` program changes the Active Directory account password for a user from within a UNIX shell.
`adquery`	The `adquery` program enables you to query Active Directory for information about users and groups from the command line on an agent-managed computer.
`adreload`	The `adreload` program forces the `adclient` process to reload configuration properties in the `/etc/centrifydc.conf` file and in other files in the `/etc/centrifydc` directory.
`adrmlocal`	The `adrmlocal` program reports and removes local user names that duplicate Active Directory user names.

Other commands that support Centrify operations are also installed in the directory with the commands shown in the preceding list, but they are not applicable to Centrify Express agents.

Displaying usage information and man pages

To display a summary of usage information for a command-line program, type the command and the `--help` or `-h` option. For example, to see usage information for the `adleave` command, type:

```
adleave --help
```

The usage information includes a list of options and arguments, and a brief description of each option.

For more complete information about any command, you can review the information in the command's manual (`man`) page. For example, to see the manual page for the `adleave` command, type:

```
man adleave
```

Customizing operations using configuration parameters

In most organizations, the default settings in the `/etc/centrifydc/centrifydc.conf` configuration file are appropriate and do not require any customization. In some cases, however, you may find it useful to modify the default settings to optimize operations for your environment.

This chapter provides reference information for the configuration parameters that control the operations on managed computers. Parameters are also documented in comments within the `centrifydc.conf` file.

Auto Zone configuration parameters

The following configuration parameters affect how user and group profiles are generated and the operation of a local host computer when the computer joins the Active Directory domain using Auto Zone.

This parameter	Does this
`auto.schema.primary.gid`	Specifies the primary GID to use in the profiles automatically generated for users. To use this parameter: ▪ You should identify an existing group, such as Domain Users, to use as the primary group. ▪ You should verify that the `auto.schema.private.group` parameter is set to `false`. The default values for this parameter are platform-dependent, for example, `20` on Mac OS X computers and `65534` on Linux, HP-UX, Solaris, and AIX computers.
`auto.schema.private.group`	Specifies whether the agent should create dynamic private groups. If you set this parameter to `true`, the primary GID is set to the user's UID and a group is automatically created with a single member. The default value is `false`, enabling you to set the primary GID using the `auto.schema.primary.gid` parameter.
`auto.schema.shell`	Specifies the default shell for the logged in user. The default value is `/bin/bash` on Centrify Express for Linux and UNIX and Linux and `/bin/sh` on other platforms, including Solaris, HP-UX, and AIX.
`auto.schema.homedir`	Specifies the home directory for logged in users. The default, if you do not specify this parameter, is: ▪ Mac OS X: `/Users/%{user}`. ▪ Linux, HP-UX, and AIX: `/home/%{user}` ▪ Solaris: `/export/home/%{user}` The variable `%{user}` is substituted at runtime and replaced with the logon name of the user who is logging on. For example, if the user `jsmith` logs on to a Centrify Express for Linux and UNIX computer, the default home directory is set to:

This parameter	Does this

	`/Users/jsmith`
	For example:
	`auto.schema.homedir:/allusers/home/%{user}`
	This parameter is not used if the parameter `auto.schema.use.adhomedir` is set to `true` and a home directory is defined in Active Directory for the user.
	If `auto.schema.use.adhomedir` is `false` or no home directory is defined for the user in Active Directory, the home directory is set to the value defined for this parameter.

`auto.schema.use.adhomedir`	Specifies whether or not to use the Active Directory value for the home directory on Centrify Express for Linux and UNIX computers. Set this parameter value to `true` to use the home directory defined in Active Directory. If you set this parameter to `true` but do not define a home directory in Active Directory, the value for `auto.schema.homedir` is used. Set this parameter to `false` if you do not want to use the home directory defined in Active Directory.

`auto.schema.remote.file.service`	Specifies the type of remote file service to use for mounting a network home directory on Mac OS X computers. The valid options are:
	▪ SMB
	▪ AFP
	For example:
	`auto.schema.remote.file.service:SMB`
	On Mac OS X computers, mounting a network directory requires that you specify the remote file service type. By identifying the remote file-service type using this parameter, you can type the network path in the format required by Active Directory:
	`/server/share/path`

This parameter	Does this
	The agent then converts the Active Directory path into the format required by Mac OS X.
`auto.schema.name.format`	Specifies how Active Directory user names are transformed into UNIX login names. The valid options are: ■ Active Directory samAccountName or Mac OS X short name (`jcool`) ■ Active Directory userPrincipalName (`jcool@acme.com`) ■ Windows NTLM format for domain and user name (`acme.com\jcool`)

`auto.schema.domain.prefix.`*`domain`*	Specifies a unique prefix for a trusted domain.
	You must specify a whole number in the range of 0 - 511.
	The agent combines the prefix with the lower 22 bits of each user or group RID (relative identifier) to create unique UNIX user identifier (UID) and group identifier (GID) for each user and group.
	In most cases, this parameter is not necessary because the agent automatically generates the domain prefix from the user or group Security Identifier (SID). However, in a forest with a large number of domains or with cross-forest trusts, domain prefix conflicts are possible.
	If you attempt to join a computer to a domain and the agent detects conflicting domain prefixes, the join fails with a warning message. You can then set a unique prefix for the conflicting domains.
	To set this parameter, append the domain name and specify a prefix in the range 0 - 511.
	For example:
	`auto.schema.domain.prefix.acme.com: 3`
	`auto.schema.domain.prefix.finance.com: 4`
	`auto.schema.domain.prefix.corp.com: 5`

This parameter	Does this
`auto.schema.search.return.max`	Specifies the maximum number of users to returned in search results. Because Auto Zone enables access to all users in a domain, a search could potentially return tens of thousands of users. This parameter causes the search to truncate after the specified number of users. The default is 1000 entries.
`auto.schema.name.lower`	Converts all user names and home directory names to lower case in Active Directory. Set to `true` to convert user names and home directory names to lowercase. Set to `false` to leave user names and home directories in their original upper, lower, or mixed case. The default for a new installation is `true`. The default for an upgrade installation is `false`.

This parameter	Does this
`auto.schema.iterate.cache`	Specifies that user and group iteration take place only over cached users and groups. The valid options are: ▪ `true` restricts iteration to cached users and groups. ▪ `false` iterates over all users and groups. The default value is `false`.

`adclient.ntlm.separators`	Specifies the separators that can be used between the domain name and the user name when NTLM format is used.
	For example:
	`adclient.ntlm.separators: +/\\`
	The default allows the following formats for the user `joe` in the `acme.com` domain:
	`acme.com+joe`
	`acme.com/joe`
	`acme.com\joe`
	Note The backslash character (\\) can be problematic on some UNIX shells, in which case you may need to specify domain\\`user`.
	The first character in the list is the one that `adclient` uses when generating NTLM names.

DNS-related configuration parameters

If computers cannot find the Active Directory domain controller, you can use parameters in the `centrifydc.conf` configuration file to manually identify the domain controllers and the Global Catalog server. You can also use configuration parameters to control how the DNS client processes DNS requests.

This parameter	Does this

`dns.dc.`*`domain_name`*	Specifies one or more domain controllers to contact.
	You must specify the name of the domain controller, not its IP address. In addition, the domain controller name must be resolvable using either DNS or in the local `/etc/hosts` file. Therefore, you must add entries to the local /etc/hosts for each domain controller if you are not using DNS or if the DNS server cannot locate your domain controllers.
	For example, to manually specify the domain controller `dc1.mylab.test` in the `mylab.test` domain, you would add the following to the /etc/centrifydc/centrifydc.conf file:
	`dns.dc.mylab.test: dc1.mylab.test`
	To specify multiple servers for a domain, use a space to separate the domain controller server names. For example:
	`dns.dc.mylab.test: dc1.mylab.test dc2.mylab.test`
	The agent will attempt to connect to the domain controllers in the order specified.

`dns.gc.`*`domain_name`*	Specifies the domain controller that hosts the Global Catalog for a domain. If the Global Catalog is on a different domain controller than the domain controllers you specify with the dns.dc.*domain_name* parameter, you can use this parameter to specify the location of the Global Catalog. For example: `dns.gc.mylab.test: dc3.mylab.test`
`dns.alive.resweep.interval`	Controls how frequently the DNS client checks whether there is a faster DNS server available. The default interval for this check is one hour.
`dns.sweep.pattern`	Specifies the protocol and response time to use when the DNS client scans the network for available DNS servers. The `dns.tcp.timeout` and `dns.udp.timeout` parameters determine the amount of time to wait if the current server does not respond to a request. If the current server does not respond to a request within the specified time out period, it is considered down and the agent looks for a different server. If the DNS subsystem cannot find a live server, DNS is considered down, and the agent waits for the period of the `dns.dead.resweep.interval`

This parameter	Does this
	parameter before performing a sweep to find a new server.
`dns.tcp.timeout`	Specifies the amount of time to wait if the current server does not respond to a TCP request. If the current server does not respond to a request within the specified time out period, it is considered down and the agent looks for a different server.
`dns.udp.timeout`	Specifies the amount of time to wait if the current server does not respond to a UDP request. If the current server does not respond to a request within the specified time out period, it is considered down and the agent looks for a different server.
`dns.dead.resweep.interval`	Specifies the amount of time to wait if DNS is before performing a sweep to find a new DNS server to use.