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

Samba Integration Guide

October 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, 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

Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service centrally secures cross-platform data centers through Active Directory-based identity and access management for a wide range of heterogeneous systems, hypervisors and applications.

Built on an integrated architecture that leverages patented technology, the Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service of solutions help centralize ID, access privilege delegation and policy management to reduce the organization's IT expense and complexity, improve end-user productivity, strengthen security and enhance regulatory compliance initiatives. Key components of audit and monitoring service include integrated authentication, access control, role-based privilege management, user-level auditing and server protection solutions.

This book describes how to integrate the Samba open source file and print sharing program on a Linux or UNIX computer that has the DirectControl agent already installed.

Note: Beginning in calendar year 2016, Centrify no longer supports the Centrify-enabled version of Samba that was available for use with earlier Centrify Server Suite releases. If you are currently using Centrify-enabled Samba with Centrify Server Suite 2013.3 or later, you must uninstall Centrify-enabled Samba, install open-source Samba, and install the latest version of the `adbindproxy` package. Those steps are described in Installing the Centrify Samba integration components. After you perform those steps, Centrify Server Suite (2013.3 or later) is integrated with open-source Samba.

Intended audience

This book is written for an experienced system administrator familiar with the unpacking and installation of programs on Linux or UNIX computers. In addition, the instructions assume that you have a working knowledge of Samba

and how to perform common administrative tasks for creating and maintaining Samba shares.

This book also requires you to have a working knowledge of authentication, privilege elevation, and audit and monitoring services and how to perform common administrative tasks using the Access Manager console and the Active Directory Users and Computers administration tool. If you are unfamiliar with authentication, privilege elevation, and audit and monitoring services, see the Administrator's Guide for Linux and UNIX and other documentation.

Using this guide

The book guides you through the installation and configuration of the components necessary to integrate authentication, privilege elevation, and audit and monitoring services and Samba. It is organized as follows:

- Using authentication, privilege elevation, and audit and monitoring services technology with Samba provides a brief overview of Samba, and how Samba, Centrify Authentication Service, and Active Directory work together to provide a secure, integrated environment.
- Installing the Centrify Samba integration components describes how to unpack and install the Centrify `adbindproxy` package.
- Migrating existing Samba users to Centrify describes how to migrate your existing Samba users to Active Directory for use with authentication, privilege elevation, and audit and monitoring services.
- Configuring the Samba integration describes how to use the Samba configuration file and test your integration of Samba, Centrify Authentication Service, and Active Directory.
- Using adbindproxy.pl describes the `adbindproxy.pl` utility, which enables you to configure Samba for interoperability with Centrify Authentication Service.

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

Previous Product Offering	Previous Product Offering	Description	Current Product Offering
	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	

Previous Product Bundle	Previous Product Bundle	Current Product Bundle	Services Included	Description
	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.

Using authentication, privilege elevation, and audit and monitoring services technology with Samba

These topics describe how Samba integrates with authentication, privilege elevation, and audit and monitoring services, and highlights some integration issues that you might encounter.

What is Samba?

Samba is an open source file and printer sharing program that allows a Linux or UNIX host to participate as an Active Directory services domain member. When Samba is installed, Windows users can share files and printers on the Linux or UNIX computers.

Samba.org distributes the Samba files and expects users to download and build their own packages. All major Linux and free UNIX distributions have Samba as a native package. For a native install of Samba on your system, see your distributor's package or port system.

Also, the https://samba.plus web site offers Samba packages for Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server (SLES), and Debian systems. The http://en.opensuse.org/Samba web site offers Samba packages for all SuSE Linux products, including SLES.

What is Centrify-enabled Samba?

Centrify-enabled Samba is an adbindproxy module and PERL configuration script that enables authentication, privilege elevation, and audit and monitoring services and Samba to work together without UID, GID, or Active Directory conflicts.

In previous releases, Centrify would modify the Samba package and provide a unique, Centrify version of Samba for different operating systems. In this release, Centrify provides a couple of components that work with the stock Samba packages.

Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service is an integrated set of commercial identity management products that enable a Linux, UNIX, or Mac host to participate as an Active Directory domain member. When you install Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service products, you can manage the Centrify-managed computer's user and group accounts and privileges entirely through Active Directory.

When open-source Samba is configured as an Active Directory domain member and the DirectControl agent is installed together with Samba on the same Linux or UNIX host, two problems can arise:

- Samba and the DirectControl agent both attempt to create and manage the same Active Directory computer account object, causing one of the products to stop working.
- Conflicting UIDs and GIDs are generated by Samba and the Centrify Management Services tools for the same Active Directory users and groups. However, the two programs use different algorithms for generating these values. The result is file ownership conflicts and access control problems.

To resolve these issues, Centrify provides the following components:

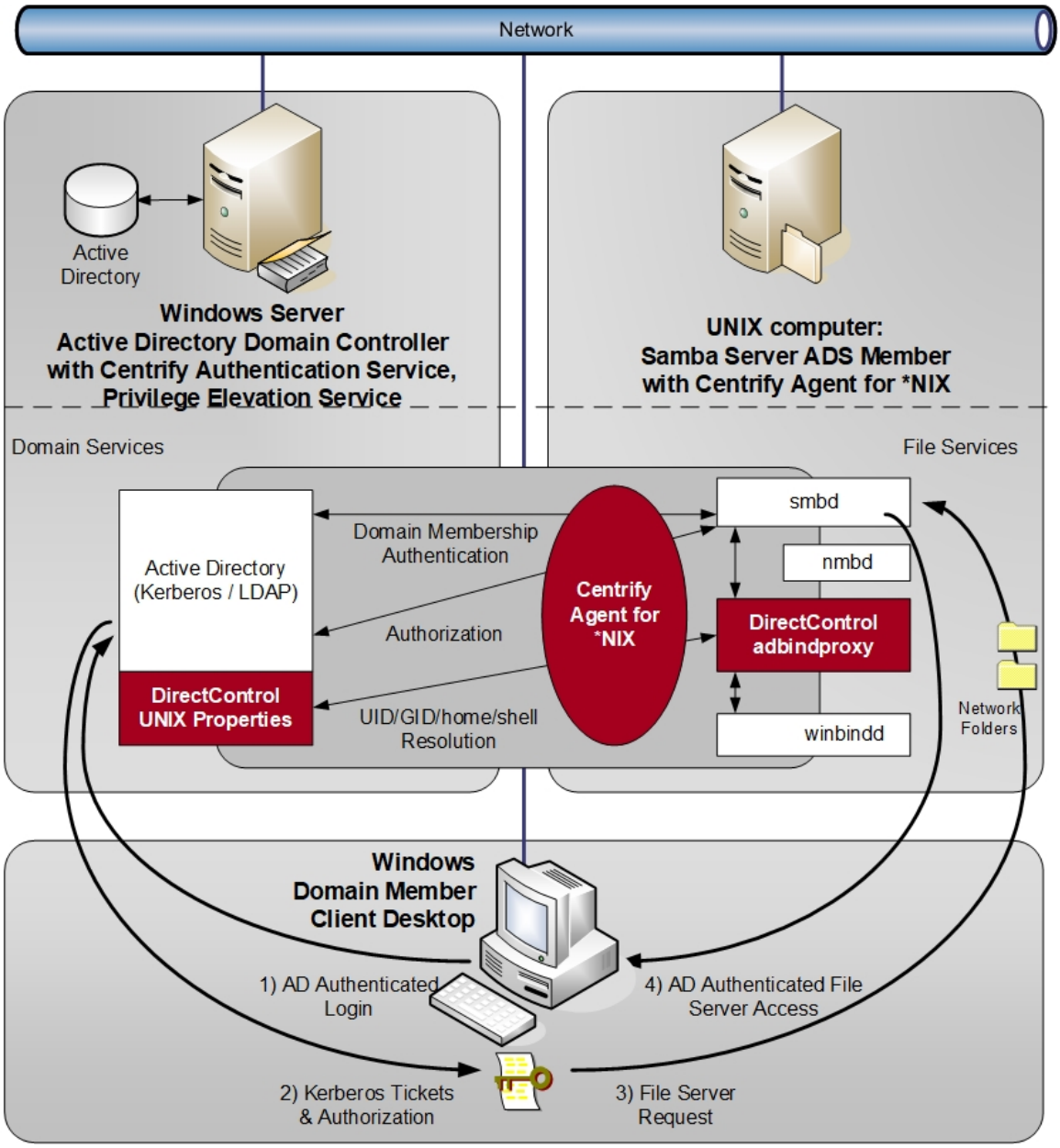
- **`adbindproxy` (`adbindd`) module:** The `adbindproxy` module uses the `adbindd` daemon. Unless otherwise noted, "adbindproxy" and "adbindd"

are used interchangeably in the documentation. The `adbindproxy` (`adbindd`) module intercepts Samba UNIX ID mapping requests and reroutes them to the DirectControl agent for processing. This module ensures that Samba and DirectControl agent agree on the UNIX attribute values.

- **`adbindproxy.pl` PERL configuration script:** Automates most of the setup process and designates the DirectControl agent as the manager of the shared computer object.

Centrify-enabled Samba architecture

The following figure provides a conceptual view of the complete solution architecture using Active Directory, Samba, and Centrify for Samba components.



If you have not been using Samba up to this point, or if you have been using an older Samba security method (such as user or server), the integration process makes it easy to configure Samba as an Active Directory member.

On the other hand, if you have already been using Samba as an Active Directory domain member and have assigned UIDs and GIDs to Active Directory users and groups, the PERL configuration script helps to resolve conflicts when Samba and authentication, privilege elevation, and audit and monitoring services are integrated.

The integrated solution, composed of the DirectControl agent (installed separately), open-source Samba, and `adbindproxy`, provides the following:

- Samba and the DirectControl agent use the same Active Directory computer object without conflicts.
- Consistent user and group attributes are applied on files across Windows, Linux and UNIX computers.
- All UNIX user identity attributes, including the UID, GID, home directory, and login shell in UNIX profiles, are centrally stored and managed in Active Directory.
- Both Kerberos and NTLM Samba authentication methods are supported.
- Standard Samba access-control features are implemented and augmented by the Centrify zones technology.

Installing the Centrify Samba integration components

This section explains how to install the Centrify adbindproxy package. You install the adbindproxy package on your Linux and UNIX computers so that the DirectControl agent works with Samba.

Installation process overview

Your Linux or UNIX computer can be in one of three main states regarding Samba and authentication, privilege elevation, and audit and monitoring services:

- New to both Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service and Samba:

  Samba is not in use and the computer does not have the DirectControl agent installed. The Samba packages might already be installed but you haven't configured Samba yet. For details, see Installation overview for computers new to both authentication, privilege elevation, and audit and monitoring services and Samba.

- Using Samba, new to Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service:

  Samba is in use but the computer doesn't have the DirectControl agent installed. For details, see Installation overview for computers new to Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service.

- Using the previous Centrify-enabled version of Samba:

  Samba is in use and the DirectControl agent is installed, and you're using the previous release of Centrify-enabled Samba. For details, see Upgrade overview for computers with Centrify-enabled Samba.

The installation process varies slightly depending on what kind of environment you're currently using.

Installation overview for computers new to both authentication, privilege elevation, and audit and monitoring services and Samba

If you're configuring a computer that does not yet have either Samba working nor the DirectControl agent, here's an overview of what you need to do.

Make sure that you have the software you need.	Make sure that you have the latest version of the DirectControl agent, the Centrify adbindproxy package, and the open source Samba files.
Install the DirectControl agent.	Refer to the Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service documentation for instructions.
Install open source Samba.	All major UNIX and Linux distributions have Samba as a native package. See your distributor's package or port system for a native install of Samba on your system. You can also visit https://samba.plus/ which offers Samba packages for Red Hat Linux, SUSE Linux Enterprise Server, and Debian.
Install the Centrify adbindproxy package.	See Installing the adbindproxy components
Run the adbindproxy.pl script.	See Configuring the Samba integration

Modify the Samba configuration file, as needed.	See Modifying the Samba smb.conf configuration file.
Test and verify the configuration.	See Verifying the Samba integration

Installation overview for computers new to Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service

If you're configuring a computer that has Samba configured but that does not yet have the DirectControl agent installed, here's an overview of what you need to do.

Make sure that you have the software you need.	Make sure that you have the latest version of the DirectControl agent, the Centrify adbindproxy package, and the open source Samba files.
Install the DirectControl agent.	Refer to the Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service documentation for instructions.
Make a backup copy of your smb.conf file.	
Install the Centrify adbindproxy package.	See Installing the adbindproxy components
Migrate Samba users to Active Directory.	See Migrating existing Samba users to Centrify **Note**: If you're using Auto Zone or Centrify Express, user migration is not supported.
Run the adbindproxy.pl script.	See Configuring the Samba integration
Modify the Samba configuration file, as needed.	See Modifying the Samba smb.conf configuration file.
Test and verify the configuration.	See Verifying the Samba integration

Upgrade overview for computers with Centrify-enabled Samba

Beginning in calendar year 2016, Centrify neither provides nor supports the Centrify-enabled version of Samba that was available earlier. Instead, Centrify now provides a standalone `adbindproxy` package containing the components that are necessary for Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service to integrate with open-source Samba.

If you are currently using Centrify-enabled Samba with Centrify Server Suite 2013.3 or later (Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service), not only do you need to upgrade to the latest DirectControl agent but there are some additional steps to migrate your users and settings. Below is an overview of what you need to do on each agent-controlled Linux and UNIX computer that was integrated with Samba.

Make sure that you have the software you need.	Make sure that you have the latest version of the DirectControl agent, the Centrify adbindproxy package, and the open source Samba files.
Make a backup copy of your smb.conf file.	
Uninstall Centrify-enabled Samba.	For example, on most Linux variants you would issue the following command: `rpm -e CentrifyDC-samba`
Upgrade the DirectControl agent so that it's either the latest version or a version later than 2013.3.	Refer to the Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service documentation for instructions.
Install open source Samba.	All major UNIX and Linux distributions have Samba as a native package. See your distributor's package or port system for a native install of Samba on your system. You can also visit https://samba.plus/ which offers Samba packages for Red Hat Linux, SUSE Linux Enterprise Server, and Debian.
Install the Centrify adbindproxy package.	See Installing the adbindproxy components
Migrate Samba users to Active Directory.	See Migrating existing Samba users to Centrify **Note**: If you're using Auto Zone or Centrify Express, user migration is not supported.
Run the adbindproxy.pl script.	See Configuring the Samba integration

Modify the Samba configuration file, as needed.	See Modifying the Samba smb.conf configuration file.
Test and verify the configuration.	See Verifying the Samba integration

What's in the adbindproxy package

After you download and extract the Centrify adbindproxy package, you'll see the following files:

```
./Centrify-Adbindproxy-Release-Notes.html
./CentrifyDC-adbindproxy-release-rhel5-x86_64.rpm
```

The software bundle has a name in this format: `centrify-adbindproxy-release-rhel5-x86_64.rpm` and it contains these components:

- **adbindproxy (adbindd) module:** The `adbindproxy` module uses the `adbindd` daemon. Unless otherwise noted, "adbindproxy" and "adbindd" are used interchangeably in the documentation. The `adbindproxy` (`adbindd`) module intercepts Samba UNIX ID mapping requests and reroutes them to the DirectControl agent for processing. This module ensures that Samba and the DirectControl agent agree on the UNIX attribute values.
- **adbindproxy.pl PERL configuration script**: This script automates most of the setup process and designates the DirectControl agent as the manager of the shared computer object.

Installing the adbindproxy components

Perform the following steps to install the integration components from the `adbindproxy` package. In these steps, the file name `CentrifyDC-adbindproxy-*.rpm` is used in place of the full file name. You can use the wildcard symbol (*) to substitute for a portion of the file name if there are no conflicting files in the directory.

> **Note:** If you are upgrading from a previous version of Centrify-enabled Samba, see Upgrade overview for computers with Centrify-enabled Samba before proceeding.

Be sure to enter the full path name in the command line if multiple versions of the same file exist in the same directory.

To install the Centrify Samba integration components:

1. Run the appropriate command for your platform to install the `centrifydc-adbindproxy` package.

   The following table shows sample commands using the common package installers for each platforms.

For this platform	You can run

Linux-based computers
Red Hat Enterprise Linux
	For 64-bit systems:
	`rpm -Uvh CentrifyDC-adbindproxy-`*`release`*`-rhel5.x86_64.rpm`
	For PowerPC systems:
	`rpm -Uvh CentrifyDC-adbindproxy-`*`release`*`-rhel5.ppc64.rpm`
	For Little-endian PowerPC systems (PPCLE):
	`rpm -Uvh CentrifyDC-adbindproxy-`*`release`*`-rhel7.ppc64le.rpm`

Sun Solaris	On SPARC systems, for example:
	`gunzip centrifydc-adbindproxy-`*`release`*`-sol10-sparc-local.tgz`
	`tar -xf centrifydc-adbindproxy-`*`release`*`-sol10-sparc-local.tar`
	`pkgadd -d CentrifyDC-adbindproxy`
	For other Solaris versions and platforms, the commands are the same but the filenames are different. For example, on a 64-bit system:
	`centrifydc-adbindproxy-`*`release`*`-sol10-x86-local.tgz`

HP-UX	For HP-UX 11.31 on PA-RISC:
	`gunzip centrifydc-adbindproxy-`*`release`*`-hp11.31-pa.depot.gz`
	`swinstall -s /path/centrifydc-adbindproxy-`*`release`*`-hp11.31-pa.depot CentrifyDC-adbindproxy`
	For other HP-UX versions and platforms the commands are the same but the file names are different. For example on HP-UX 11.31 Itanium 64-bit systems:
	`centrifydc-adbindproxy-`*`release`*`-hp11.31-ia64.depot.gz`

IBM AIX	For AIX 7.1 or later:
	`gunzip centrifydc-adbindproxy-`*`release`*`-aix7.1-ppc-bff.gz`
	`inutoc`
	`installp -aY -d centrifydc-adbindproxy-`*`release`*`-aix7.1-ppc-bff CentrifyDC.adbindproxy`

For this platform	You can run
Debian Linux Ubuntu Linux	Check that you have `libcupsys2-gnutls10` (1.1.23-1 or later) installed If you have the required libraries, run the following command to install: `dpkg -i centrifydc-adbindproxy-`*release*`-deb8-x86_64.deb`
SuSE Linux OpenSuSE Linux	For 64-bit systems: `rpm -ivh CentrifyDC-adbindproxy-`*release*`-suse11.x86_64.rpm`

2. (Optional) Join the computer to a zone using the `adjoin` command.

This concludes the installation of the `adbindproxy` package.

If you have existing Samba users to migrate, go to Migrating existing Samba users to Centrify. Otherwise, go to Configuring the Samba integration to continue.

Updating the Samba files

After you've installed the Centrify adbindproxy package, you might need to update your version of Samba. When you update the Samba files, the update will replace `smb.conf` and also restart Samba with its own startup script instead of the `adbindd` script.

Before you update your version of Samba, it's a good practice to make a backup copy of your `smb.conf` file.

After you update your version of Samba, perform the following tasks so that you can keep the Centrify adbindproxy package working.

To keep the Centrify adbindproxy package working after updating Samba:

- Do one of the following:
  - Run adbindproxy.pl to reconfigure the centrifydc-samba service (Recommended)

    After adbindproxy.pl finishes the setup, you may want to add back the customized settings from the smb.conf backup to the new smb.conf file. Restart the centrifydc-samba service after the change.

Note that the commands to restart the service are different on different platforms.

- Manually replace the smb.conf with the backup.

  After replacing the smb.conf file, restart the centrifydc-samba service. Note that the commands to restart the service are different on different platforms.

  This method may not work because the Samba upgrade may affect the configurations of the centrifydc-samba service and the Samba service itself.

Migrating existing Samba users to Centrify

This section describes how to migrate an existing user population from Samba servers to the integrated Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service.

Note: The information in this section is relevant to computers with the core authentication, privilege elevation, and audit and monitoring services components installed and for which you created a Centrify zone. These instructions do not apply to computers with Centrify Express installed or computers that are joined through Auto Zone. If you are using Centrify Express or if you have joined a computer using workstation mode, it is not possible to migrate existing Samba UID and GID settings.

Migrating UNIX profiles to Active Directory

If your current environment includes Samba servers that are joined to the Active Directory domain as member servers and existing Windows users access the data on those servers, you may want to migrate those existing users to authentication, privilege elevation, and audit and monitoring services to rationalize UIDs and GIDs and manage all of your network's conflicting identities in a single, centralized ID repository.

Note: Migrate your Samba users to Active Directory, as explained in this section, **before** integrating Samba and Centrify

Authentication Service as explained in Running the adbindproxy.pl script.

There are two ways to migrate your UNIX profiles to Active Directory:

- If `winbind` is currently configured in your `/etc/nsswitch.conf` file, you need to run the `getent` command to retrieve the user information.
- If you do not have `winbind` configured in your `/etc/nsswitch.conf` file, then run the `adbindproxy` perl script to migrate the users. See the instructions below.

Migrating users if winbind is configured in /etc/nsswitch.conf

To save the winbind information to a file:

1. If `winbind` is currently configured in your `/etc/nsswitch.conf` file, run the following commands to save the information to a file before installing the `adbindproxy` package:

   getent passwd | grep -v -f /etc/passwd > /tmp/passwd.winbind

   getent group | grep -v -f /etc/group > /tmp/group.winbind

2. Move the exported files to a computer where you have installed the Access Manager console.
3. In the Access Manager console, use the **Import from UNIX** wizard to import the users and groups (with their existing UID and GID mappings) into the zone.

   For more information on importing existing user and group information and mapping information to Active Directory, see the “Importing existing users and groups” chapter in the Administrator’s Guide for Linux and UNIX.

Migrating users with the adbindproxy perl script

If `winbind` is not currently configured in your `/etc/nsswitch.conf` file, follow the steps below after you’ve installed the adbindproxy package.

This script gets the UID andGID files from Samba. You then import them into Active Directory.

• • • • • •

To migrate UNIX user profiles to Active Directory using the adbindproxy.pl script:

1. Identify the Samba servers you want to update to integrate with authentication, privilege elevation, and audit and monitoring services.
2. On each of the Samba servers to be updated, locate the `winbindd_idmap.tdb` file and create a backup copy of the file.
   a. To locate the `winbindd_idmap.tdb` file, you can run a command similar to the following to view details about the Samba build:

      /CurrentSambaBInaryPath/smbd -b |grep -i lockdir

   b. In the output, you should see a line similar to the following that indicates the location of the `winbind_idmap.tdb` file:

      LOCKDIR: /var/lib/samba
3. Make a backup copy of the `winbindd_idmap.tdb` file.

   For example:

   cp /var/lib/samba/winbind_idmap.tdb /tmp/winbind_idmap.tdb.pre_adbindproxybackup
4. Run the `adbindproxy.pl` script with the following options to generate the export files.

   perl /usr/share/centrifydc/bin/adbindproxy.pl --export --groupFile filename --userFile filename --tdbFile filename

   See Using adbindproxy.pl for details about the command-line parameters for `adbindproxy.pl`.

   When you run these `adbindproxy.pl` options it generates export files for the users and the groups that are currently known by the Samba server. By default, these files are created as:

   /var/centrify/samba/passwd

   /var/centrify/samba/group
5. Move the exported files to a computer where you have installed the Access Manager console.
6. In the Access Manager console, use the **Import from UNIX** wizard to import the users and groups (with their existing UID and GID mappings) into the zone.

   For more information on importing existing user and group information and mapping information to Active Directory, see the “Importing existing

users and groups” chapter in the Administrator’s Guide for Linux and UNIX.

Migrating Samba servers to Centrify Zones

Samba generates UIDs and GIDs based on a range of values that have been defined for a specific server. In most cases, a user who has accessed two different Samba servers is likely to have two different UIDs: for example, a user could have UID `6003` on the server `mission` and UID `9778` on the server `dolores`.

Therefore, in an initial migration of existing users, each Samba server must join the Active Directory domain in separate Centrify Zones to accommodate the different UIDs and GIDs users and groups may have.

If you want users to have consistent GIDs and UIDs, then you need to put the Samba servers in the same zone.

Configuring the Samba integration

This section describes how to configure the DirectControl agent and Samba to work together properly after you have installed the integration components from the Centrify `adbindproxy` package and joined agent-controlled computers to a zone.

Running the adbindproxy.pl script

This section describes how to configure Samba using the `adbindproxy.pl` script.

> **Note:** If your current environment has Windows users accessing data on Samba member servers that are joined to the Active Directory domain, you may want to migrate those users to authentication, privilege elevation, and audit and monitoring services. This way, you can use Centrify Zones to manage conflicting identities and rationalize UIDs and GIDs. For details on how to migrate those users, see Migrating existing Samba users to Centrify Complete the migration **before** integrating Samba and Centrify Authentication Service.

The `adbindproxy.pl` script performs the following tasks:

- Determines the computer's operating system and adjusts accordingly.
- Confirms that the DirectControl agent is installed.

- Confirms that open-source Samba has been installed.
- Determines if you are joined to an Active Directory domain and, if you are, displays the domain name and Centrify Zone.
- Asks if you want to join Samba to the current Active Directory domain or another. If you choose another, the script guides you through the current domain leave and new domain join processes.

  Note: If you want to modify or set advanced join settings (for example, update PAM or NSS config, use DES for encryption, or use a computer alias), either run `adleave` before you run `adbindproxy.pl` or select a different domain when prompted in the script. Otherwise, the script does NOT prompt you to enter advanced join settings.

- If you have a previous Samba installation, asks if you want to keep the `smb.conf` settings or use new ones. `adbindproxy.pl` automatically saves the existing copy.

  Note: The script automatically looks for an existing `smb.conf` file using the `smbd -b` command. If your current version of `smbd` does not support the `-b` option or you have `smb.conf` in a custom directory the script will not find it. If you want to use your existing `smb.conf`, move it to `/etc/samba` before you run the script.

- Removes old state files from previous instances of Samba, including any existing `winbind` entries from the `/etc/nsswitch.conf` file.
- Restarts the necessary clients (`nmbd, winbindd, adbindd and smbd`).
- Installs scripts to automatically start the correct Samba and Centrify services each time the computer boots.
- Optionally can pass additional options for adjoin and adleave.
- Can generate a response file so that you can run the adbindproxy.pl script without any user interaction.

Before you run `adbindproxy.pl`, read through the prompts described below to make sure you're prepared with the answers. For example, before you run the script be sure you know the path where Samba is installed.

• • • • • •

To begin, log on and switch to the root user and proceed with the following steps:

To run the adbindproxy.pl script:

1. To start the script, from `root` enter the following:

   ```
   perl /usr/share/centrifydc/bin/adbindproxy.pl
   ```

2. Specify the path to the Samba installation:

   a. If Samba is not installed in the default location (/usr), enter the Samba path.

   b. If Samba is installed in /usr, press **Enter** to accept the default. Otherwise, enter your path.

3. Specify the domain to join.

   You proceed based on whether the computer is already joined to a domain or not:

   - If you **are already joined** to a domain when you initiated the script, the script displays the domain name and zone and asks you the following:

     ```
     Do you want to leave or join to another domain? [N]
     ```

     To continue to join the current joined Active Directory domain press `Enter` and skip ahead to Step 6.

     If you want to leave the current domain and join another OR change any advanced options (see the list below) in your current domain enter `Y` and then continue to Step 4.

   - If you **are not joined** to a domain, the script displays the following message:

     ```
     Not joined to any domain. Make sure you enter the
     correct domain and zone information in the next steps
     ```

     This initiates a set of prompts that ask you for the Active Directory domain name, the Centrify Zone and advanced options.

     Continue to Step 4.

4. Join the new Active Directory domain.

   You arrive at this step if you are not joined to an Active Directory Domain when you started `adbindproxy.pl` or if you decided to leave that domain

OR you decided to change advanced options in your current join. If none of these conditions apply to you, skip to Step 6.

a. At this prompt, enter the domain name:

```
Enter the Active Directory domain to join:
```

b. At the DNS health prompt, press **Enter** to verify that the domain exists.

```
Check DNS health for [domain]? Note: this may take
several minutes [Y]:
```

c. At the next prompt, enter the following domain properties:

Note: If you are running authentication, privilege elevation, and audit and monitoring services in Express Mode or need to join the domain through Auto Zone, enter NULL_AUTO for the zone name.

a. Centrify zone on the target Active Directory domain

b. Computer name on which the `adbindproxy` package is installed

c. Active Directory authorized user (default is Administrator)

5. (Optional) Specify advanced join options.

The script prompts you with the following message:

```
Do you wish to specify advanced join options? [N]:
```

The options are listed below. The defaults are in brackets.

a. If do not need any advanced join options, enter `N`. Otherwise, enter `Y` and make your selections.

```
Canonical name of Active Directory Computer Container
Preferred Domain Server to use (press Enter for none)
Update PAM and NSS Config [Y]
Trust computer for delegation? [N]
Use DES encryption only? [N]
Run adjoin in verbose mode? [N]
Addition computer alias (press Enter for none)
```

The script then displays the selections you made and asks if you want to proceed.

b. Enter `Y` to proceed or `N` to abort `adbindproxy.pl`.

If you were not joined to an Active Directory domain when you started the script, you are prompted to enter your password once.

c. Enter the password for the Active Directory Domain, computer and authorized user specified in the prompts.

> **Note:** If you choose to proceed **AND** you are leaving the current Active Directory domain to join another, the script prompts you **twice** to enter your password.

d. In response to the first prompt, enter the current Active Directory domain account password to leave that domain.

e. In response to the second prompt, enter the password for the Active Directory Domain, computer and authorized user specified in the prompts to join the new domain.

6. Enter the Samba winbindd path.

   At the next prompt, if the samba winbindd listen path is not in `/run/samba/winbindd`, enter the path or press **Enter** to accept the default.

7. If there is an existing `smb.conf` file, continue to Step 8.

   Otherwise, if there is no existing `smb.conf` file (which is true for new installations of Samba), the adbindproxy script searches for existing `smb.conf` files. If it **does not** find an existing `smb.conf` file, it automatically creates a new one, stores it in `/etc/samba`, and displays the following message:

   ```
   Updating smb.conf with Centrify recommended settings ...
   ```

   and finishes the script.

   This new `smb.conf` file has minimal global settings and a samba-test share.

   > **Note:** Regardless of whether you update an existing `smb.conf` or create a new one, you will need to modify the `/etc/samba/smb.conf` file to have the `[global]` section settings and the appropriate shares for your environment. See Modifying the Samba smb.conf configuration file for instructions. The file created by `adbindproxy.pl` should be used for verifying the Samba integration only.

   If you do have at least one existing `smb.conf` file, continue to Step 8.

8. Specify existing or new smb.conf settings:

If you have an existing `smb.conf` file, you next specify whether to update the settings in the existing `smb.conf` file or create a new, skeletal `smb.conf` file. If you choose to use the existing settings, you can also choose to do a backup of the existing `smb.conf` file.

If the script **does** find an existing `smb.conf` file, the script copies the `smb.conf` file to `/etc/samba` and asks the following question:

```
Do you want to keep the original samba settings? [Y]:
```

Note: If the script finds more than one `smb.conf`, it displays the list and asks you to select one. After you make the selection, it copies that one to `/etc/samba` and continues.

Note: Regardless of whether you update an existing `smb.conf` or create a new one, you will need to modify the `/etc/samba/smb.conf` file to have the `[global]` section settings and the appropriate shares for your environment. See Modifying the Samba smb.conf configuration file for instructions. The file created by `adbindproxy.pl` should be used for verifying the Samba integration only.

- **Don't keep the original Samba settings**: Enter `N` to not keep the original Samba settings and instead create the new, basic `smb.conf`.

The script creates a backup copy of your `smb.conf` in `/etc/samba`. The backup filename is in this format: `smb.conf.`yyyy-mm-dd-hh-mm. This new `smb.conf` file has minimal global settings and a samba-test share, if no shares exist.

Continue to Finishing Up .

- **Keep the original Samba settings**: Enter `Y` to modify the existing file and continue to Step 9.

9. If you've chosen to keep the original Samba settings, the script displays the following prompt about backing up the existing settings:

   ```
   Backup existing /etc/samba/smb.conf and add Centrify
   recommended settings? [Y]
   ```

   - Enter `Y` to create a backup in the form, `smb.conf.`yyyy-mm-dd-hh-mm.
   - Enter `N` to use the existing `smb.conf` without making a backup.

Note: If the existing `smb.conf` has Security = ADS and the workgroup and realm are set, the script does NOT modify the existing file; the original is left unchanged.

10. For ubuntu and Suse computers where AppArmor exists, the script displays the following prompt about updating the AppArmor policy profiles:

    ```
    Update AppArmor policy profiles? [Y]
    ```

    Use the default [Y], unless you don't want to update the AppArmor profiles now.

    If you don't update the AppArmor profiles now, be sure to update them manually later. Otherwise, winbindd might fail to start and you won't be able to access the samba share. For ubuntu systems, the profiles aren't updated because the winbind policy profile doesn't exist.

11. If you're configuring a Linux system that has SELinux enabled and Samba supports your system's version of samba_selinux, the script checks the configurations and, if needed, displays the following prompt:

    ```
    Update SELinux policy to allow r/w on non samba_share_t
    types? [Y]
    ```

    Use the default [Y] unless you have labeled all the share folders with the type samba_share_t.

    If you don't update the SELinux policy, Samba cannot read or write to the shared folder is not labeled with the samba_share_t type.

    For more information about samba_selinux, see the samba_selinux man page.

12. If you've chosen to keep the original Samba settings, the script displays the following prompt about resetting the Samba cache for user and group IDs.

    ```
    Reset the Samba User/Group ID Cache (Centrify Samba may
    create conflicting mappings) [Y]
    ```

    Unless you have created custom mappings, use the default [Y]. This flushes the cache and displays the following message:

    ```
    This prompt is only pertinent to the small set of Samba
    administrators who created custom user and group ID mappings.
    If you do have custom mappings, use the default to flush the
    cache and prevent potential conflicts. After adbindproxy.pl
    completes, re-add your mappings as necessary.
    ```

If you entered Y, the script creates new mappings in the Samba User/Group ID cache, which may result in conflicts if there are any mappings in place already.

Finishing Up

To complete the configuration, `adbindproxy.pl` stops any running versions of `smbd, adbindd, winbindd` and `nmbd`, starts the required Centrify processes, and displays a set of progress and configuration messages. You should see the following messages:

```
Init Samba start script ...
Restarting Samba daemons ...
Reloading systemd:                                  [  OK  ]
Restarting centrifydc-samba (via systemctl):        [  OK  ]
Current DirectControl Configuration:
...
Current Samba Configuration:
...
```

The adbindproxy script displays the following:

```
Press ENTER to continue ...
Notes: If you need to join another domain, please re-run this script and
enter the new domain name!
Done.
```

Note: If any service fails to start, you should run one of the following after the `adbindproxy.pl` script completes its execution.

On Linux or Solaris computers, run:

```
/etc/init.d/centrifydc-samba restart
```

On HP-UX computers, run:

```
/sbin/init.d/centrifydc-samba restart
```

On AIX computers, run:

```
stopsrc -g samba && startsrc -g samba
```

On Linux computers that support systemd, run:

```
systemctl restart centrifydc-samba
```

As a quick test, log off as the `root` user and log on with an Active Directory user account that has been granted access to the local computer's zone. If this is the first time that you are logging on with this user account, check that the user's home directory is created, which is created automatically by Centrify Authentication Service the first time you log on.

Verifying the Samba integration

To verify that Samba and authentication, privilege elevation, and audit and monitoring services are working together correctly, you test if you can access Samba shares. If you upgraded existing shares, then you can test those; otherwise, you can verify the connection using the test share.

There are two key scenarios for testing whether Samba is configured properly for integration with Centrify Authentication Service and Active Directory:

- Accessing Samba from a UNIX client session
- Accessing Samba shares from a Windows desktop

Accessing Samba from a UNIX client session

To test access to Samba shares on a Linux or UNIX computer, users should do the following:

To access Samba from a UNIX client session:

1. Log on to the Linux or UNIX computer using the Active Directory account that has been granted access to the local computer's zone.
2. Run the following command:

   ```
   smbclient -k -L host_name
   ```

   The `smbclient` program displays information about Samba and the SMB shares that are available on the local computer. For example, you should see a listing similar to the following (where s.s.s is the Samba version):

   ```
   OS=[Unix] Server=[Samba s.s.s]

         Sharename      Type      Comment
         ---------      ----      -------
         samba-test     Disk
         IPC$           IPC       IPC Service (Samba-CDC)
         sara           Disk      Home directories

   OS=[Unix] Server=[Samba s.s.s]

         Server               Comment
         ---------            -------
         Workgroup            Master
         --------             -------
         ARCADE               MAGNOLIA
   ```

If you are able to see the Samba shares as an Active Directory user logged on to the Linux or UNIX computer that is acting as the Samba server, you should next test accessing the Samba shares from a Windows desktop. For information about performing this test, see Accessing Samba shares from a Windows desktop.

Purging and reissuing Kerberos tickets on UNIX computers

If you see an error such as `NT_STATUS_LOGIN_FAILURE` instead of the expected results when you run the `smbclient` program, you may need to purge your existing Kerberos tickets and have them reissued. Try running the following command to remove all of your Kerberos tickets:

```
/usr/share/centrifydc/kerberos/bin/kdestroy
```

Then run the following command to reissue tickets after you provide your Active Directory password:

```
/usr/share/centrifydc/kerberos/bin/kinit
```

You can then run the following command to list the Kerberos tickets that have been issued to you:

```
/usr/share/centrifydc/kerberos/bin/klist
```

After verifying the Kerberos tickets you have been issued, try running the `smbclient` program again.

Verifying the version of Samba you are using

If purging and reissuing tickets does not resolve the problem, confirm the version of the `smbstatus` that is currently running using the following command:

```
smbstatus | grep version
```

The command should display the Samba version you have installed. For example:

```
Samba version s.s.s
```

(where `s.s.s` is the installed Samba version)

If the correct version of Samba is installed, run `smbstatus` again and note the names of any `*.tdb` files that do not exist, and try restoring them from your backup, then try running the `smbclient` program again.

• • • • • •

If you don't see the correct Samba shares

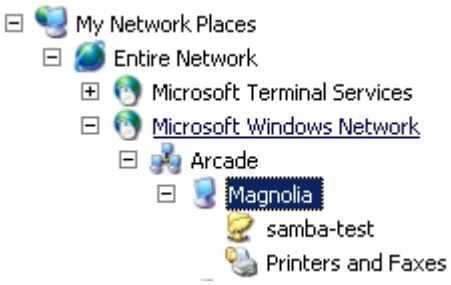
If the `smbclient` program does not display the Samba shares you have defined in the configuration file, you should review the settings in the `smb.conf` file and then restart the DirectControl agent and run the `adflush` command.

Accessing Samba shares from a Windows desktop

To test access to Samba shares on a Linux or UNIX computer from a Windows desktop:

1. Log on to a Windows computer that is joined to the domain with an Active Directory user account.
2. Click **Start > Windows Explorer**, then navigate to the domain.

   For example, open **My Network Places > Entire Network > Microsoft Windows Network > Arcade** to view the `Arcade.net` domain.
3. Select the Linux or UNIX computer that is integrated with Samba to view its Samba shares. For example:



4. Click `samba-test` or browse other available Samba shares to verify that you can open existing files and create new files.
5. Confirm from both Windows and the managed computer that the files in the share directories are owned by the correct users.

If you cannot browse the shares on the Linux or UNIX computer from the Windows desktop, you should:

- Verify that there is network connectivity between the two systems.
- Confirm that you do not have a firewall running on the managed computer that is blocking access to the SMB ports.
- Make sure there are no stale Kerberos tickets on your Windows system.

- `klist` and `kerbtray` programs.

Modifying the Samba smb.conf configuration file

The Samba configuration file, `/etc/samba/smb.conf`, defines important parameters for Samba-based file sharing. After you have verified the Samba integration with Centrify Authentication Service and Active Directory using a sample configuration file and the test share, you need to modify the `smb.conf` file so that it accurately represents your environment.

This `smb.conf` file must include the `[global]` section that defines the Active Directory domain, authentication methods, and other parameters. The file should also include a section for each directory you are making accessible as a SMB share.

At the beginning of a line, both the hash symbol (#) and the semi-colon (;) indicate lines to ignore. By convention, in this file, the hash indicates a comment and the semi-colon indicates a parameter you may wish to enable.

If you specify multiple users in `valid users`, user names can be separated by a comma or by white space.

The settings in the `[global]` section are required whether you use the sample configuration file or create your own `smb.conf` file. The settings in the `[homes]` section indicate that you want to share home directories, and the `[samba-test]` section describes the `samba-test` share as a publicly-writable share mapped to the `/samba-test` directory. For more information about editing the Samba configuration file and the supported parameters, see the Samba documentation.

A sample Samba smb.conf configuration file

The adbindproxy script tests to determine what operating system is running on the host and generates an `smb.conf` file appropriate to that platform.

In the following sample file, it runs on a CentOS computer in the arcade.net domain and the Samba share is called MyShare.

```
#
# This file was generated by Centrify ADBindProxy Utility
#
[global]
    security = ADS
    realm = ARCADE.NET
```

```
    workgroup = ARCADE
    netbios name = centos-6
    auth methods = guest, sam, winbind, ntdomain
    machine password timeout = 0
    passdb backend = tdbsam:/var/lib/samba/private/passdb.tdb
    #
    # Samba versions 3.4.0 and newer have replaced "use kerberos keytab"
    # with "kerberos method".  The directive "kerberos method = secrets
and keytab"
    # enables Samba to honor service tickets that are still valid but
were
    # created before the Samba server's password was changed.
    #
    kerberos method = secrets and keytab
    #
    # Setting "client use spnego principal" to true instructs SMB client
to
    # trust the service principal name returned by the SMB server.
Otherwise,
    # client cannot be authenticated via Kerberos by the server in a
different
    # domain even though the two domains are mutually trusted.
    #
  #  client use spnego principal = true
    #
    # Setting send spnego principal to yes .
    # Otherwise, it will not send this principal between Samba and
Windows 2008
    #
  #  send spnego principal = Yes
    # If your Samba server only serves to Windows systems, try server
signing = mandatory.
    server signing = auto
    client ntlmv2 auth = yes
    client use spnego = yes
    template shell = /bin/bash
    winbind use default domain = Yes
    winbind enum users = No
    winbind enum groups = No
    winbind nested groups = Yes
    idmap cache time = 0
  #  ignore syssetgroups error = No
    idmap config * : backend  = tdb
    idmap config * : range = 1000 - 200000000
    idmap config * : base_tdb = 0
    enable core files = false
    #  Disable Logging to syslog, and only write log to Samba standard
log files.
    #syslog = 0
[samba-test]
    path = /samba-test
    public = yes
    #  if set  public = No, we should  set parameter valid users .
    #  and when the user or group is in AD , the setting syntaxes is:
    #  valid users = CPUBS\username +CPUBS\group
    writable = yes
[MyShare]
        path = /samba-test
        browsable = yes
        writable = yes
```

```
        guest ok = yes
        read only = no
[homes]
    comment = Home directories
    read only = No
    browseable = No
```

SMB.conf file variations for different platforms

Some platforms will have slight variations in the `smb.conf` file, as follows:

- On HP-UX computers, the following line is added:

  ```
  guest account = smbnull
  ```

- On SuSE computers, the following lines are added:

  ```
  # Suse 11 CUPS printing appears to crash at start up
  # So we disable printing on this platform for now
  printing = BSD
  ```

- On AIX computers, the following comments are added:

  ```
  #
  # On AIX, the service NMBD may fail to start because Samba
  # cannot determine the correct IP subnet mask.
  # In this case, you can manually specify the correct subnet mask.
  # For example if you have the following configuration:
  #
  # Interface     = eth0
  # IP Address    = 192.168.97.199
  # Subnet mask   = 255.255.252.0
  #
  # then set the interfaces keyword as follows:
  #
  # interfaces = eth0 192.168.97.199/255.255.252.0
  #
  ```

Testing changes to the smb.conf file

When you make changes to the `smb.conf` file, you should run the Samba utility `testparm` to make sure there are no errors in your `smb.conf` file before putting it into production use. When you run the `testparm` utility, you should see output similar to the following:

```
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[samba-test]"
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
Press enter to see a dump of your service definitions

[global]
```

```
        workgroup = ARCADE
        realm = ARCADE.NET
                security = ADS
        auth methods = guest, sam, winbind, ntdomain
        passdb backend = tdbsam:/etc/samba/private/passdb.tdb
        syslog = 0
        enable core files = No
        server signing = auto
        machine password timeout = 0
        adbindproxy backend = cdc:/usr/share/centrifydc/lib/libcapi.so
        adbindproxy standard mappers = No
        template shell = /bin/bash
        winbind use default domain = Yes

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /usr/spool/samba
        printable = Yes
        browseable = No

[samba-test]
        path = /samba-test
        read only = No
        guest ok = Yes
```

Using adbindproxy.pl

This appendix describes the options available for the `adbindproxy` command-line tool. The `adbindproxy.pl` utility is used to configure Samba and Centrify Authentication Service to work together and provides specific functions, such as exporting UIDs and GIDs, creating symbolic links to Samba binaries and libraries, and restoring backed-up Samba files.

Note: For step-by-step instructions about running `adbindproxy.pl` to configure Samba and Centrify Authentication Service to work together, see Running the adbindproxy.pl script.

Synopsis

```
adbindproxy.pl [--help] [--info] [--restore] [--unconfig] [--
adjoinExtraOptions] [--adleaveExtraOptions] [--version] [--verbose]]
adbindproxy.pl [--export] [--groupFile filename] [--userFile filename] [--
tdbfile filename]
adbindproxy.pl  [--record] [--responseFile filename]
adbindproxy.pl  [--nonInteractive] [--responseFile filename]
adbindproxy.pl  [--service start|stop|restart|status]
```

adbindroxy.pl options

You can use the following options with this command:

Use this option	To do this
-c, --test ***filename***	Generate a test target Samba configuration file. With this option, the script generates a target Samba configuration file with the filename for review. This option is a review option and does not change any configuration or make any changes.
`-E, --export`	Export user IDs (UIDs) and group IDs (GIDs) that are stored in Samba's `winbindd_idmap.tdb` file. Use the `--groupFile` and `--userFile` options to specify the export files for the GIDs and UIDs. Use the `--tdbfile` option to specify the .tdb file that contains the GIDs and UIDs. After export, you can use the Centrify Authentication Service Administrator Console to import the users and groups with their existing UID and GID mappings into a zone.
-f, --responseFile filename	The filename specifies the response file for recording with the -x option or for non-interactive mode with the -n option. If you don't specify a filename, the default is /var/centrify/samba/adbindproxy.pl.rsp.
`-g, --groupFile filename`	Specify the file in which to write the Samba-created Active Directory group to GID mappings. Use this option with the `--export` option. By default, the file is: `/etc/group`
`-h, --help`	Display the `adbindproxy.pl` usage information.
`-i, --info`	Display Samba interoperability information.
-j, --adjoinExtraOptions adjoinoptions	The adjoinoptions are the additional options to be used for the adjoin command. Do not specify the domain or the following options with adjoinExtraOptions, because they're already handled in the response file: -u / --user -c / --container -V / --verbose -n / --name -s / --server -T / --trust -k / --des -z / --zone -a / --alias

Use this option	To do this
-l, --adleaveExtraOptions adleaveoptions	The adleaveoptions are the additional options to be used for the adleave command. Do not specify the domain or the following options with adleaveExtraOptions, because they're already handled in the response file: -u / --user -f / --force
-n, --nonInteractive	Run adbindproxy.pl in non-interactive mode using the response file. It is recommended to have the machine joined to the Active Directory domain before running this script in non-interactive mode. Otherwise, adbindproxy.pl needs to obtain the Active Directory authorized user password from the command line with the -j/-l option, or interactively from the terminal. **WARNING**: Typing the password in the command line NOT secure, do NOT do that unless you know what you are doing.
`-r, --restore`	Restore files backed up from the first time you configured Samba for interoperability with Centrify Authentication Service. Typically, you run `adbindproxy.pl` with the `--restore` option to restore Samba files before uninstalling the integration components that were provided in adbindproxy.
`-S, --symbol`	Force the creation of symbolic links to Centrify for Samba binaries and libraries without asking for confirmation.
--s, --service <start|stop|restart|status>	Control the CentrifyDC Samba service. If you haven't configured the CentrifyDC Samba service yet, this option has no effect. If you specify --service status", there will be a return value of 0 if the service is running and a return value of 1 if the service isn't running.
-T, --noTestShare	Specify to not create the test folder "/samba-test" and not add the "samba-test" share when updating the smb.conf file.
`-t, --tdbFile filename`	Specify the location of the `winbindd_idmap.tdb` file that contains Samba UID and GID information. This option is used during the UID and GID export process. If you omit this option, the default file to export from is: `/var/lib/samba/winbindd_idmap.tdb`
`-u, --userFile filename`	Specify the file in which to write Samba-created Active Directory user to UID mappings. Use this option with the `--exports` option. By default, the file is `/etc/passwd.`

Use this option	To do this
-v, --version	Display version information for the installed software.
-V, --verbose	Display detailed information for each operation.
-x, --record	Record the user input into the response file which can be used later in non-interactive mode.

Examples

To display basic information about the configuration of the Samba integration and interoperability with authentication service and Active Directory, you could type a command line similar to the following:

```
adbindproxy.pl --info
```

This command displays information similar to the following (where v.v.v is the Centrify version number and s.s.s is the Samba number):

```
The Samba base path is:          /usr
CentrifyDC version             = CentrifyDC v.v.v
CentrifyDC Architecture        = 64-bit
CentrifyDC Realm               = ARCADE.NET
CentrifyDC NTLM Domain         = ARCADE
CentrifyDC Host                = magnolia.arcade.net
CentrifyDC Short Host          = magnolia

Samba Version                  = s.s.s
Samba Architecture             = 64-bit
Samba Realm                    = ARCADE.NET
Samba NetBIOS Name             = MAGNOLIA

Samba Version Supported        = yes
Samba and CDC in same Realm    = yes
Samba and CDC share machine account = yes
Password sync using libtdb     = <not specified>
```

To export existing Samba GID and UID information that you want to import into a Centrify Zone, and to show details about the operation performed, type a command line similar to the following:

```
adbindproxy.pl --export --verbose
```

This command displays information similar to the following:

```
The existing UID mappings have been exported to
/var/centrify/samba/passwd.

The existing GID mappings have been exported to
/var/centrify/samba/group.
```

To record the user input to a response file:

```
# adbindproxy.pl -x
```

To run adbindproxy.pl in non-interactive mode with the response file that was generated previously at the default location:

```
# adbindproxy.pl -n
```