

WHITE PAPER  
CENTRIFY CORP.  
DECEMBER 2009

## Centrifify-Enabled Samba

---

*The easy-to-manage enterprise solution for Active Directory-enabled Samba file sharing*

---

### ABSTRACT

Samba is one of the most popular open source technologies in use on UNIX and Linux systems. Samba allows customers to share directories and files to users on other systems, using the native Windows-based CIFS or SMB protocol. However, for most businesses, sharing any type of data across the network immediately raises concerns that the information will not be protected and may be vulnerable to unauthorized access. Fortunately, a solution exists to enable enterprise-level access control and centralized authentication and authorization for customers with Samba deployments.

In most enterprises, Microsoft's Active Directory is now the de facto standard for providing authentication, authorization, account information, computer policy and infrastructure management for Windows systems and applications. Centrifify's DirectControl extends Active Directory's reach to UNIX, Linux, Mac and Java-based environments. The Centrifify-enabled Samba solution goes one step further by enabling Active Directory identity and access management for Samba-based file servers.

This paper describes how Centrifify-enabled Samba delivers new capabilities for your Samba deployments and how these unique features translate into major benefits in the form of increased security, ease of use and enterprise readiness.

*Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrifify Corporation.*

*Centrifify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrifify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*© 2006-2009 Centrifify Corporation. All rights reserved.*

*Centrifify and DirectControl are trademarks of Centrifify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.*

*The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

*[WP008-2009-12-10]*

## Contents

<b>1</b>	<b>Introduction</b> .....	<b>1</b>
<b>2</b>	<b>Challenges with Other Samba Solutions</b> .....	<b>2</b>
<b>3</b>	<b>Addressing Samba Challenges with DirectControl</b> .....	<b>3</b>
	3.1 Centralized Attribute Mapping in Active Directory .....	4
	3.2 Automated Installation and Deployment.....	5
<b>4</b>	<b>Samba and DirectControl Integration: Step-by-Step</b> .....	<b>6</b>
<b>5</b>	<b>Summary</b> .....	<b>8</b>
<b>6</b>	<b>How to Contact Centrify</b> .....	<b>10</b>

## 1 Introduction

The open source Samba project is a popular solution for serving up UNIX files and directories to Windows clients using native Windows file sharing protocols. Windows users can access the file shares using the same software and procedures they would use to access Windows systems. This allows customers to seamlessly share data between Windows and UNIX/Linux systems. Some of the scenarios where Samba might be used include:

- **Windows users accessing application data on UNIX.** Customers may have line-of-business server applications running on UNIX, which are accessed from Windows desktops using a Windows-based client. Users often need to access the application's data files or output report files from Windows as well. Samba allows the Windows user to browse to a shared directory on the UNIX server and open the file using the same methods that are used with Windows file servers.
- **Leverage old UNIX hardware for use as a Windows file server.** A popular use for old UNIX hardware is to set up the system as a file server for Windows users. Samba can transform these systems into virtual network attached storage (NAS) devices for Windows users.
- **Centralized file storage for UNIX and Windows users.** Certain types of corporate data need to be accessed from users on all types of systems. Customers will often centralize this information in a UNIX system directory. This directory can then be shared to UNIX users using NFS (the native file sharing system for UNIX) and shared out to Windows users using Samba.

These are just a few of the popular uses of Samba. However, in every business scenario, the question of security must be addressed.

- How do I enable centralized access control for each share?
- How do I provide centralized authentication for users accessing data?
- How can I provide reporting on who has access rights for each share?
- How do I turn off access to a share when a user no longer needs it?
- How can I leverage my existing security and access control infrastructure?

To address these and other issues, customers should consider the use of an enterprise security solution coupled with the Samba technology. Fortunately, Centrify has such a solution.

Centrify DirectControl provides Active Directory-based identity, access control and policy services for UNIX, Linux and Mac systems. With DirectControl, UNIX user information such as user IDs (UID), group IDs (GID), UNIX home directories and UNIX shell settings, are all centrally stored in Active Directory. Users can log into UNIX and Linux systems using their

Active Directory passwords and are able to take full advantage of their Active Directory-issued Kerberos credentials to securely run Kerberos-based applications with a single sign-on experience.

The Centrify-enabled Samba solution goes further by tying Samba to Active Directory for user and group identity management, authentication, access and policy management. The result is a secure, single sign-on experience for Windows users accessing Samba file shares.

However, before discussing the details of the DirectControl solution, it is worth exploring the issues that exist with alternative solutions or with Samba on its own.

## 2 Challenges with Other Samba Solutions

Samba is a mature technology that has been widely used on Linux, UNIX and embedded systems for many years. However, Samba is an open source project, and the technology is built by volunteers. As with any open source project, customers may find that Samba has some shortcomings when compared to traditional commercial software:

- For the most part, support is provided through online forums staffed by volunteers.
- While there is a published future roadmap for Samba, there are no promised dates for future releases or fixes for issues encountered by users.
- Samba can be difficult to set up and manage, and often companies need to hire a Samba expert to maintain the system.
- Many UNIX and Linux operating system vendors bundle Samba with their systems, but their bundled versions are often substantially out of date.
- The binary Samba packages shipped with some platforms are built without Active Directory support. If customers want this important feature, they are forced to build custom versions from the Samba sources.

Samba includes basic support for integration with Active Directory, but well known limitations exist with these features. Since by default Active Directory does not include UNIX-specific information (such as a UNIX user ID), there is no obvious method for storing this information centrally. Samba's **winbind** program runs as a daemon and handles information lookups related to user and group properties. By default, **winbind** stores additional UNIX-specific information locally on each UNIX system running Samba. Because there is no easy way to synchronize multiple different local data stores, users can have inconsistent credential mapping from one Samba server to the next.

Attempts have been made to overcome these issues by using various layered technologies such as OpenLDAP, Microsoft's Services for UNIX (SFU) or UNIX's Network Information Service (NIS). All of these methods tend to be difficult to set up, and each approach has its own shortcomings. For example, many UNIX systems have limits on the number of groups that a user can be a member of (for example, Solaris has a limit of 32 groups). However, many users in a typical enterprise Microsoft Active Directory environment will be members of dozens or hundreds

of groups. In order to provide accurate and consistent group membership information, Samba needs to bypass the host UNIX operating system and work directly with Active Directory.

Other challenges arise when customers need enterprise-quality end-to-end support. For example, Microsoft will support the Windows side of Services for UNIX but does not support access of these services from UNIX applications such as Samba.

Other higher-end enterprise features such as cross-domain authentication, failover support for NTLM, domain controller failure support, large group-based access control, and access rights reporting are simply not supported with most other approaches.

Based on feedback from Samba users who needed true, enterprise-level capabilities for working with Active Directory, Centrify has built a dedicated solution that integrates Samba with Active Directory.

### 3 Addressing Samba Challenges with DirectControl

The Centrify-enabled Samba solution consists of the following components:

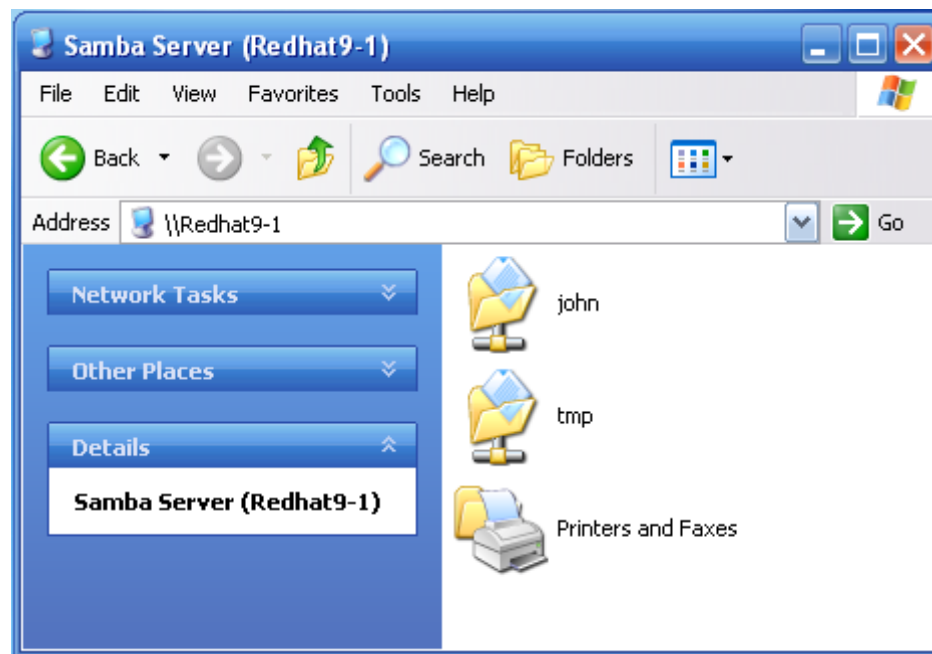
- **Samba binaries.** Centrify has built Active Directory-enabled binary versions of one of the latest releases of Samba for each of the supported operating systems. This means you will be running an up-to-date version of Samba that has been thoroughly tested to integrate with Active Directory via DirectControl. The distribution for each operating system also includes other components that are required by Samba.
- **Centrify Winbind Proxy.** A new “proxy” component has been developed by Centrify for Active Directory integration. This plugs into the supported Samba system, enabling Centrify to manage user identity mapping from Windows to UNIX for consistent identity and permissions.
- **Automation scripts.** Scripts are included to assist with the setup of the Centrify-enabled Samba environment. Samba can be set up and operational in minutes instead of days. Scripts are also provided to automatically start up Samba and the DirectControl Agent each time the system boots.
- **Documentation.** Centrify-enabled Samba includes an installation and deployment guide. There is also guidance related to testing your Samba environment.
- **Solution support.** Licensed Centrify customers who have support and maintenance contracts and are running Centrify-enabled Samba can get support for the integration of DirectControl with Samba.

By packaging a Samba product, installation scripts, documentation and integration of the DirectControl and Samba products into a single comprehensive package, Centrify can help elevate Samba to a solution that better interoperates with your enterprise. Not only do you get a finished product that works – you know who to contact if you encounter problems.

In addition, Centrify addresses a number of issues related to central attribute storage, enterprise functionality and complete integration with Active Directory, as mentioned earlier in this paper.

### 3.1 Centralized Attribute Mapping in Active Directory

New functionality is mainly supported through the Centrify Winbind **Proxy** for Samba. This is unique new technology that Centrify has developed specifically for Samba. Centrify Winbind **Proxy** allows **Samba** to talk directly to Centrify's DirectControl daemon when user or group information is needed. Since Centrify DirectControl stores all UNIX user and group attributes in Active Directory, Samba now has a painless way to access all user and group information centrally. The result is a consistent, accurate mapping of all user and group attributes whenever a user accesses a Samba file share. Users accessing a Samba share are first authenticated using their Active Directory credentials. Standard Active Directory access management methods, such as group-based access control, Group Policy, user access rights, and time-of-day restrictions can all be used to control which users have access to individual shares.



An Active Directory-authenticated Windows user can securely access file shares on UNIX/Linux servers using Centrify-enabled Samba.

With Centrify Zones, Samba environments can be further secured by restricting Zone membership to only the users and groups that need access to the machines in a Samba Zone. For example, the Finance Department could set up a Samba server and join that server to a "Finance Zone" in Active Directory. Using the Centrify Administrator's Console, IT administrators can enable users in that Zone and grant them the appropriate access rights based on their group memberships. If a user leaves the Finance Department and moves to the Sales Department, he or she can be easily removed from the Finance Zone and added to the Sales Zone. This user would no longer have access to the Finance Department shares. Note that the default Samba behavior without

DirectControl would allow all Active Directory users the ability to authenticate with any Active Directory-enabled Samba servers. Thus Centrifys Zone technology can be used as an additional line of defense against the unauthorized access of data.

## 3.2 Automated Installation and Deployment

The automation scripts included with Centrifys-enabled Samba simplify the installation and configuration of DirectControl and Samba. The script operates in one of two modes. On a fresh installation it will join your computer to the domain and then configure Samba. On systems that are already running DirectControl and joined to the domain, the script will simply configure Samba as an Active Directory domain member. The installation script will do the following automatically for you:

- Any existing instances of the Samba services will be stopped.
- The script checks for old or conflicting Samba installations.
- The script checks to make sure you have installed DirectControl.
- On new installs the script prompts for the domain, Centrifys Zone, username to be used for joining to Active Directory, and the Active Directory password for that user. On existing DirectControl installs, the script asks if you want to rejoin or just configure Samba based on the existing join. The script offers defaults based on your current configuration. The script also finds and validates your current Samba installation.
- Checks are made to ensure that DNS is set up correctly on your system.
- Based on the domain information that is provided, the script creates or modifies your existing smb.conf file. The existing smb.conf file is automatically saved before it is modified.
- Old Samba system files from previous instances of Samba are moved aside, unless you have removed them manually beforehand.
- PAM and NSS modules are configured correctly.
- Symbolic links for key Samba programs are created, so they can be run from /usr/bin and /usr/sbin.
- For new installs, the machine is joined to the Active Directory domain and Centrifys Zone for both Samba and DirectControl. For existing installs, Samba is configured at this time.
- The Samba services and the DirectControl adclient service are started.
- Scripts are created to automatically start the correct Samba and DirectControl services each time the system boots.
- The configuration information for both DirectControl and Samba is output to the screen.



4. The Samba file service, `smbd`, validates the user and checks to ensure that the user is a member of the Samba server's Centrify Zone and ...
5. ... calls `winbindd` to look up information for the user (such as the user's UID). The Centrify Winbind Proxy intercepts the user lookup functions ...
6. ... and the DirectControl adclient agent looks up the user's information in Active Directory.
7. This information is passed back to `smbd`, and the user continues with the file-sharing session based on their authenticated Active Directory credentials.

In this example, the user's experience while accessing the Samba file server is totally consistent with the experience they have accessing Windows-based file servers. Full Active Directory-based ownerships and permissions are enforced, and users can securely access the file server without re-entering their Active Directory credentials.

In addition, Centrify adds an extra level of security for Samba file servers through its Centrify Zone membership model. Samba servers join a particular Centrify Zone as well as joining the Active Directory domain. For example, the Finance Department might have a Zone named Finance. Users and groups associated with the Finance Department can be added as members of this Finance Zone. Only users who are members of the Finance Zone can access the file shares on that server. Other Active Directory users will be denied access to the file shares if they are not members of the Finance Zone. Zone memberships can be established based on roles, organizational models, operating system type, or any logical grouping that meets the organization's needs. It is important to note that users and groups can be members of multiple Zones, based on the requirements of their roles and access needs. It is also important to note that managers and administrators can run reports from the Centrify DirectControl Administrator's Console at any time to verify access rights for users and resources.

3/15/2006

AD User Name	Unix Name	Zone	UID	Shell	Home Directory
<b>Fred Thomas</b>	fred	samba-servers	10002	/bin/bash	/home/fred
<b>Jane Does</b>	jane	finance	10001	/bin/bash	/home/jane
<b>John Smith</b>	john	finance	10000	/bin/bash	/home/john
	john	samba-servers	10000	/bin/bash	/home/john
<b>Sally Jones</b>	sally	samba-servers	10001	/bin/bash	/home/sally

Current Page No.: 1      Total Page No.: 1      Zoom Factor: 100%

Centrify DirectControl

File Action View Favorites Window Help

User	Unix Name	UID	Shell	Home Directory	Primary Group	AD User Enabled	Unix Profile Enabled	Canou
Enter text h...	Ente...	E...	Ent...	Enter tex...	Enter te...	Enter text here	Enter text here	Enter
Sally Jones	sally	10001	/bin/bash	/home/sally	10000	Y	Y	sales.
Fred Thomas	fred	10002	/bin/bash	/home/fred	10000	Y	Y	sales.
John Smith	john	10000	/bin/bash	/home/john	10000	Y	Y	sales.

Access to Samba servers is restricted to members of the “samba-servers” Zone as shown in the DirectControl reports and Zone management view from the Centrify DirectControl Administrator’s Console.

## 5 Summary

In summary, Centrify-enabled Samba provides a number of unique features to allow Samba to be fully integrated with Microsoft Active Directory:

- UNIX users can be managed from Active Directory and they now use their Active Directory username and password to log into UNIX. This capability is provided by DirectControl.
- UNIX authentication is managed securely, using the Kerberos technology that is part of DirectControl and Active Directory.
- UNIX systems are securely joined to the Active Directory domain and Centrify Zone and can be controlled and managed centrally through DirectControl.
- Users can create file shares on UNIX or Linux that can be shared out to Windows systems, using the SMB protocol. This capability is provided by Samba.
- UNIX file servers can now be secured with advanced centralized authorization and access control capabilities, using Active Directory and DirectControl.

- Consistency is maintained for user and group attributes on files across Windows and UNIX – regardless of whether files are created or managed from UNIX or Windows. User identity attributes, such as UID, home directory and login shell, are now stored and managed in Active Directory using DirectControl.
- Access control to Samba shares can be managed centrally using both Centrify Zone and Active Directory group membership, simplifying management and ensuring appropriate access is granted to files on the system for both SMB-based access as well as interactive access. This provides a more consistent for group management across an array of platforms that have individual limitations on group memberships.

The resulting benefits for customers include:

- **More secure.** Samba is now tightly coupled with Active Directory authentication and authorization. In addition, Centrify Zone technology gives users the ability to create secure logical groups of computers to help with enforcement of role-based access control. DirectControl reports also allow administrators and auditors to instantly see who has access to corporate resources.
- **More manageable.** The resulting solution is easier to configure and maintain. Administrators have full centralized control over user and group access rights with the Centrify Administrator's Console. Management costs can be reduced as less time is required to maintain Samba.
- **Enterprise ready.** By providing pre-packaged, tested Samba binaries and enterprise-class support, Centrify turns Samba into a solution that any enterprise can feel comfortable deploying.

For the latest product information on DirectControl and the Centrify Suite, check out our web site:

<http://www.centrify.com/products>

See the Centrify-enabled Samba web page for the latest information on using this solution:

<http://www.centrify.com/samba>

## 6 How to Contact Centrifly

### **North America** (And All Locations Outside EMEA)

Centrifly Corporation  
785 N. Mary Ave., Suite 200  
Sunnyvale, CA 94085  
United States

Sales: +1 (408) 542-7500

Enquiries: [info@centrifly.com](mailto:info@centrifly.com)  
Web site: [www.centrifly.com](http://www.centrifly.com)

### **Europe, Middle East, Africa** (EMEA)

Centrifly EMEA  
1210 Parkview, Office 202  
Arlington Business Park  
Theale, Reading  
Berkshire, RG7 4TY  
United Kingdom

Sales: +44 (0) 118 965 7755