



## IN THIS DOCUMENT

- Integrating Samba file sharing from Linux and Unix servers with Likewise Enterprise.
- Replacing the authentication backend and native Samba 3 idmapper with that provided by Likewise Enterprise.

# Samba 3 Integration Guide

## Abstract

This document describes how to integrate Samba file sharing from Linux and Unix servers with Likewise Enterprise, so that these shares provide controlled access for Windows clients that are authenticated by Active Directory. The guide also discusses the configuration of home directories and roaming profiles.

The Samba 3 integration guide is intended to provide the system administrator with deployment guidance when integrating Samba 3 with Likewise Enterprise to provide secure, interoperable enterprise solutions for Windows file and print sharing on Linux and UNIX operating systems. This guide provides a step-by-step instruction on replacing the authentication backend and native Samba 3 idmapper with that provided by Likewise Enterprise.

## About Likewise Enterprise

By joining Linux, Unix, and Mac computers to Active Directory – a secure, scalable, stable, and proven identity management system – Likewise gives you the power to manage all your users' identities in one place, use the highly secure Kerberos 5 protocol to authenticate users in the same way on all your systems, apply granular access controls to sensitive resources, and centrally administer Linux, Unix, Mac, and Windows computers with group policies. Likewise includes reporting and auditing capabilities that can help improve regulatory compliance. The result: lower operating costs, better security, enhanced compliance.

The information contained in this document represents the current view of Likewise Software on the issues discussed as of the date of publication. Because Likewise Software must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Likewise, and Likewise Software cannot guarantee the accuracy of any information presented after the date of publication.

These documents are for informational purposes only. LIKEWISE SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED.

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, by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Likewise Software.

Likewise 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 Likewise, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2008 Likewise Software. All rights reserved.

Likewise and the Likewise logo are either registered trademarks or trademarks of Likewise Software in the United States and/or other countries. All other trademarks are property of their respective owners.

Likewise Software  
15395 SE 30th Place, Suite #140  
Bellevue, WA 98007  
USA



## Table of Contents

<b>INTRODUCTION.....</b>	<b>4</b>
<b>Key Benefits of Combining Samba and Likewise Enterprise.....</b>	<b>4</b>
Consolidation of User Account Management .....	4
Simplified Installation and Configuration.....	4
Increased security.....	4
<b>SID-TO-UID MAPPING IN AD .....</b>	<b>5</b>
<b>SIMPLE FILE SHARING.....</b>	<b>5</b>
<b>Setup .....</b>	<b>5</b>
Assumptions.....	5
Verification .....	7
<b>SAMBA SUPPORT FOR AD INTEGRATION.....</b>	<b>8</b>
<b>How to I determine if your version of Samba supports Active Directory integration? .....</b>	<b>8</b>
<b>Samba Resources.....</b>	<b>8</b>
<b>TROUBLESHOOTING FAQ .....</b>	<b>8</b>

## Introduction

Samba is the one the most popular and widely available programs used to integrate UNIX servers with Windows clients. Although originally written to facilitate the sharing of files and printers, Samba can also be configured to allow the UNIX server to act as an NT4 equivalent Domain Controller, a master browser, a WINS server and more. Samba services beyond simple file sharing and authentication are beyond the scope of this document. For more information about Samba, visit the Samba project website at <http://www.samba.org>.

### Key Benefits of Combining Samba and Likewise Enterprise

#### Consolidation of User Account Management

Samba, by default, will maintain its own database of users and passwords. These credentials are in addition to those required by the UNIX server itself and by your Windows environment, and must be managed separately. Furthermore, Samba requires that a local UNIX user account be created in addition to the Samba user account.

Likewise Enterprise allows you to consolidate all of these identities to a single AD account simplifying management.

#### Simplified Installation and Configuration

Likewise Enterprise provides an easy-to-use installer and configuration tool. This tool simplifies the Samba manual process of Active Directory integration by through the process of:

- Configuring hostname and DNS, including Active Directory integrated Secure Dynamic DNS support
- Installation and configuration of enterprise authentication components to match multi-forest, multi-domain Active Directory expectations
- Performing a robust domain join

#### Increased security

Samba, by default, will authenticate users with credentials passed across the network in clear text. This means that anybody monitoring the network traffic would be able to retrieve that information without the knowledge of the user. This can happen several times through the day,



first when the user maps a drive to the share, as well as any time the user logs in to a system with a persistent mount, and even after long periods of inactivity. With your Samba servers integrated with Active Directory using Likewise Enterprise, however, all of your authentication traffic is encrypted.

The benefit of consolidated user account management also increases enterprise security by eliminating the locally maintained Samba database of user data on every Samba server.

## SID-to-UID Mapping in AD

Microsoft Windows distinguishes one user from another using a security ID (SID). The SID is not recognized by Unix-based systems, however, which use a simple number (the user ID, or UID) to each user in the environment. In order for a single security principle (user) to exist in both realms, it must be mapped to both of these types of identifiers.

The `idmapper` is the part of Samba that maps Active Directory SIDs to Unix UIDs and GIDs. The `idmap backend` refers to the name of the module used by `idmap` to store the name space information. Other parameters are available for `idmap` configuration of allowed UID and GID ranges, cache time, etc.

## Simple File Sharing

Likewise Enterprise contains a compatibility `idmap` plugin for Samba 3.0.0 - 3.0.24. This section describes integration of a vendor's version of Samba to integrate with the Likewise Enterprise Authentication Daemon (`lwiauthd`). Be aware that older versions of Samba may contain bugs that will alter the behavior from what is described below.

### Setup

#### Assumptions

Likewise Enterprise (LWE) has been installed on your Linux server, and the system has been joined to Active Directory. The vendor's version of Samba has been installed on the Linux system, and is functional.

1. Create a directory named 'idmap' under `/usr/lib/samba`, if necessary (`/usr/lib64/samba` for 64-bit servers). Create a symbolic link from `/usr/lib/samba/idmap/lwicompat_v2.so` to point to `/usr/centeris/lib/idmap/lwicompat_v2.so`. Repeat for



### lwicompat\_v4.

```
# cd /usr/lib/samba
# mkdir idmap
# cd idmap
# ln -s /usr/centeris/lib/idmap/lwicompat_v2.so
# ln -s /usr/centeris/lib/idmap/lwicompat_v4.so
```

### 2. Confirm the version of Samba that you have installed.

```
# smb -V
Version 3.0.26a-1478
```

### 3. Edit the Samba configuration file `/etc/samba/smb.conf` to set the following parameters to the listed values. If the parameters are not included in the `smb.conf` file, add a new line for them in the **[global]** section of the file. Be sure to use `lwicompat_v2` if your Samba version is 3.0.0 to 3.0.24, and `lwicompat_v4` for versions 3.0.25 and higher.

```
security = ads
workgroup = <enter workgroup from /etc/samba/lwiauthd.conf here>
realm = <enter realm from /etc/samba/lwiauthd.conf here>
# use lwicompat_v2 for Samba 3.0.0 to 3.0.24
# idmap backend = lwicompat_v2
# use lwicompat_v4 for Samba 3.0.25 and later
idmap backend = lwicompat_v4
idmap uid = 50-9999999999
idmap gid = 50-9999999999
```

### 4. Create a `userPrincipalName` value for the machine in its Active Directory account object using the command `lwinet`.

```
$/usr/centeris/bin/lwinet ads setmachineupn -U Administrator
Password: <enter admin password>
Added userPrincipalName value of host/PASCAL@EAST.AD.PLAINJOE.ORG
```

**Special note for Ubuntu and Debian only:** Ubuntu and Debian store `secrets.tdb` in `/var/lib/samba` so you will need to create a symlink back to `/etc/samba/secrets.tdb`.

```
$ mv /var/lib/samba/secrets.tdb /var/lib/samba/secrets.tdb.orig
$ ln -s /etc/samba/secrets.tdb /var/lib/samba/secrets.tdb
```

### Verification

In order to verify the configuration:

1. Start the Samba winbind daemon **winbindd** (e.g.: `/etc/init.d/winbind start`).
2. Use the **wbinfo** tool to verify various pieces of information. Start by ensuring that **winbindd** is honoring the machine trust account settings.

```
$ wbinfo -t
checking the trust secret via RPC calls succeeded
```

3. Next resolve a name to a SID and that SID to a uid or gid. This example resolves the user `EAST\testuser1001`:

```
$ wbinfo -n "EAST\testuser1001"
S-1-5-21-1862414975-1169984241-1344135624-1103 User (1)

$ wbinfo -S S-1-5-21-1862414975-1169984241-1344135624-1103
200000
```

This should match the information returned from `getent` which is sent through Likewise Authentication daemon.

```
$ getent passwd "EAST\testuser1001"
EAST\testuser1001:*:200000:200000::/home/EAST/testuser1001:/bin/bash
```

4. Next, start up Samba and try to access a share from **smbclient** or a Windows client. You can verify the connected user's Software using the **smbstatus** command.

```
$ smbstatus
Samba version 3.0.10-1.4E.11
PID Username Group Machine
-----
4486 EAST\testuser1001 EAST\domain^users drizzt (192.168.1.84)

Service pid machine Connected at
-----
public 4486 drizzt Wed Mar 14 16:26:31 2007
No locked files
```

## Samba Support for AD Integration

### How to I determine if your version of Samba supports Active Directory integration?

In order to determine whether your version of Samba supports Active Directory integration run, examine the build options for the WITH\_ADS option. You can execute the Samba daemon with the build options '-b' argument and search for the WITH\_ADS 'build' and 'with' option with grep, e.g.:

```
$ /usr/sbin/smbd -b | grep WITH_ADS  
  
WITH_ADS  
WITH_ADS
```

### Samba Resources

Samba documentation and resources can be found at the Samba website:  
<http://www.samba.org>.

## Troubleshooting FAQ

### Q. Samba 3.0.10 (FC3 and RHEL4) fails to allow a user to connect.

A. This and possibly other versions of Samba's winbindd have a bug that causes a connection to fail if the getgroups() call fails to resolve the first group SID in a user's list to a gid. The shows up as a NT\_STATUS\_NO\_SUCH\_USER error in the Samba log files. An alternative method of testing this is to run "wbinfo -r DOMAIN\User". This should return a list of gids (at least one). The workaround is to enable all the user's groups for Unix access in the cell or forest.

### Q. How do I use the non-sAMAccount Likewise Enterprise aliases (usernames) and Samba?

A. You must inform Samba of the alias by including a username map. Add "username map = /etc/samba/users.map" to the [global] section of /etc/samba/smb.conf. The create the /etc/samba/users.map file and add an entry for each aliases user in the form "!alias = DOMAIN\user".

To alias AD groups, use the form "!alias = @DOMAIN\group".

**Note:** The exclamation mark causes Samba to stop processing on the first matching alias. This prevents issues with multiple alias matches caused by the use of wildcards.

## ABOUT LIKewise

Likewise Software is an open source company that provides audit and authentication solutions designed to improve security, reduce operational costs and help demonstrate regulatory compliance in mixed network environments. Likewise Open allows large organizations to securely authenticate Linux, UNIX and Mac systems with a unified directory such as Microsoft Active Directory. Additionally, Likewise Enterprise includes world-class group policy, audit and reporting modules.

Likewise Software is a Bellevue, WA-based software company funded by leading venture capital firms Ignition Partners, Intel Capital, and Trinity Ventures. Likewise has experienced management and engineering teams in place and is led by senior executives from leading technology companies such as Microsoft, F5 Networks, EMC and Mercury.

