

## Likewise Security Benefits

---

**AUTHOR:**

Manny Vellon  
*Chief Technology Officer*  
Likewise Software

**Abstract**

This document describes how Likewise improves the security of Linux and UNIX computers by allowing computers to authenticate and authorize users through Microsoft Active Directory.

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.

© 2007 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>User Authentication and Authorization in Linux and Unix Systems</b> .5	
Local Password Files .....	5
Synchronization.....	6
NIS and NIS+ .....	7
LDAP-Based Directory Services.....	7
<b>Security Benefits of Likewise</b> .....	<b>9</b>
Password and Account Policies.....	9
Enforce Security Settings on UNIX and Linux.....	11
Mac OS X Security Policies.....	12
Application Support .....	13
Compliance Reporting.....	14
<b>Summary</b> .....	<b>15</b>
<b>For More Information</b> .....	<b>16</b>

## Introduction

Likewise allows Linux and UNIX computers to authenticate and authorize users through Microsoft Active Directory™. This provides many benefits:

- A single username and password for users, regardless of whether they are using Microsoft Windows™ or non-Windows systems
- Greatly simplified user account management. System administrators can provision users, maintain passwords and deprovision users using a single identity management system
- Improved security. Likewise extends numerous Active Directory account policies to Linux and UNIX systems. Administrators can configure minimum password lengths, password complexity requirements, password expiration policies and other settings that are applied to both Windows and non-Windows systems
- Granular authorization supporting separation of duties. Likewise extends Active Directory Group Policy features to Linux and UNIX and provides policy settings to control the provisioning of standardized SUDOer configuration files

Likewise will lower costs, improve security and help you demonstrate compliance with regulatory requirements.

This document explores the security aspects of Likewise — *how* Likewise improves the security of your Linux/UNIX systems.

## User Authentication and Authorization in Linux and Unix Systems

Linux and UNIX provide a variety of different mechanisms for *authentication* (assuring that users are who they say they are) and *authorization* (assuring that users are authorized to perform operations). Most distributions of these operating systems support systems such as *PAM* and *nsswitch* that allow the use of local files, networked information services (*NIS*) and LDAP directory services.

Likewise is an LDAP-based solution. Before describing its benefits, let's first consider the weaknesses of the alternatives.

### Local Password Files

Given the flexible infrastructure of these operating systems, it is surprising to find that a large number of Linux/UNIX systems employ only the most rudimentary authentication and authorization mechanism: local password files. In this mechanism, each Linux/UNIX computer maintains user accounts in a local file (usually, in `/etc/passwd`). A second file (usually, `/etc/group`) maintains additional information used to determine group membership.

The weakness of this solution is evident. If you have 100 computers, you need to maintain 200 files. If a new user is added to your organization and that user needs access to all 100 machines, you have to add him/her to 100 `passwd` files and (perhaps) to 100 group files. If that user changes his/her password, the password change has to be performed on all 100 machines. It is not surprising then that one or more of the following results in organizations that use only local password files:

- Administrators employ scripts or other automated techniques to try to keep password files properly synchronized
- Administrators give up maintaining synchronized password files and leave it up to users to maintain their passwords on all of the systems to which they have access

- Administrators give up maintaining password files altogether and just have everyone log on with a service account. Too often, this service account is root!

When users have different accounts and different passwords on different systems, they end up writing down their passwords, as they are incapable of remembering all of them.

Having everyone log in as root has obvious drawbacks:

- Pretty soon, everyone knows the root password
- Whenever you change the root password, you have to inform everyone of its new value
- When something goes wrong, it's impossible to figure out who was at fault because all you know is that "root" did it.

### **Synchronization**

Systems that rely on local password files for authentication and authorization are well advised to employ some type of mechanism to keep all of their systems synchronized. This can be done with "low-tech" tools such as scp or rsync or can be done with expensive directory synchronization programs. Note, however, that synchronization itself can introduce security problems:

- The synchronization process may need a stored password in order to be able to connect to the systems that it needs to update
- The synchronization process may need to store passwords instead of password hashes (especially if different systems use different hashing techniques) and the password store may be subject to attack
- Systems that are temporarily offline (for example, servers under repair or laptop computers) might be "missed" by the synchronization process and remain vulnerable to compromised passwords.

### **NIS and NIS+**

A step up from using local password files, NIS (and, more recently, NIS+) provides a way of sharing a password file. Rather than having separate password files on Linux and UNIX computers, NIS allows you to maintain a single password file on a NIS server and to set up other computers as NIS clients that retrieve the data from this NIS server. The benefit of this approach is that you only need to maintain a single password file as the NIS clients will access this file over the network when they need account information.

Although Likewise offers many benefits over NIS, it should suffice to note that NIS is not considered a secure authentication mechanism. NIS uses encryption techniques (for example, DES hashes) that are considered inadequate by modern standards. Additionally, because NIS clients have access to the shared password file, a rogue NIS client can try to use brute force techniques to crack the encrypted password hashes stored in the file. Companies running NIS typically do not pass regulatory compliance audits.

NIS+ addresses some of the security weaknesses of NIS, but has seen very little adoption. Early versions of NIS+ were plagued with problems and not available on a variety of platforms. NIS+ servers are difficult to configure and manage and even Sun, the inventors of the protocol, are recommending LDAP-based solutions as preferable to NIS+.

### **LDAP-Based Directory Services**

Directory services are, essentially, special databases designed for the efficient access of directory information. Directory services are frequently combined with communication protocols (for example, Kerberos) to serve as authentication and authorization systems. Additionally, they provide functionality that makes them the preferred solution for this purpose:

- Automatic replication to multiple servers – this provides redundancy, performance and high-availability
- Extensible schemas to allow flexibility in how/what data they store

- Standardized protocols (LDAP v3 and Kerberos 5) that permit use from a variety of operating systems

In spite of these standard features, not all LDAP-based solutions are created equal! Most vendor-specific LDAP directories don't work well with Windows, leading to additional complexity in managing multiple identity stores and directories.

## Security Benefits of Likewise

Likewise allows Linux and UNIX computers to authenticate users with Microsoft Active Directory (AD). From the discussion above it should be clear that the use of a centralized authentication database yields some immediate benefits:

- Users have to remember only one username and password. This significantly reduces security breaches due to passwords written on Post-It™ Notes
- AD uses well-designed communication protocols (Kerberos and authenticated LDAP queries) that resist most network attacks (replay attacks, man-in-the-middle attacks, etc.)
- AD is designed with security in mind and makes it much more difficult to employ system attacks (by malicious external or internal sources) to crack passwords and defeat security mechanisms

### Password and Account Policies

Likewise provides group policies for account security features and passwords that you can apply to Linux, Unix, and Mac OS X computers within Active Directory. Likewise allows you to join Linux, UNIX, and Mac OS X computers to Active Directory and to place these computers in organizational units that have group policy objects (GPOs) applied to them.

GPOs are collections of settings that apply to all computers that are direct or indirect members of the organizational units to which they are applied. GPOs can be applied at multiple levels in the AD hierarchy to specify different settings to computers that require different security configurations.

Here are some of the password and account policies that Likewise provides:

- **Log on using Kerberos authentication:** This policy grants Linux and Unix computers access to a Windows NT domain using the Kerberos authentication protocol.
- **Acquire Kerberos tickets on logon:** Users obtain a Kerberos ticket when they log on the Windows NT domain using the Kerberos protocol.
- **Create a .k5login file in a user's home directory:** This policy creates a .k5login file in the home directory of a user account on Linux and Unix computers that log on the Windows NT domain using the Kerberos authentication protocol. The .k5login file contains the user's Kerberos principal, which uniquely identifies the user within the Kerberos authentication protocol. Kerberos can use the .k5login file to check whether a principal is allowed to log on as a user. A .k5login file is useful when your computers and your users are in different Kerberos realms or different Active Directory domains, which can occur when you use Active Directory trusts.
- **Refresh Kerberos tickets:** The Kerberos authentication protocol grants tickets to prove the identity of users in a secure way. By automatically refreshing tickets, you can maintain a user's domain access.
- **Allow cached logons:** This policy allows Unix and Linux computers to use cached credentials when they cannot connect to the network or the domain controller for authentication.
- **Allow logon rights:** Users and groups who have logon rights can log on the target computers either locally or remotely. You can also use this policy to enforce logon rules for local users and groups.
- **Lock the screen with the screensaver:** This policy can help prevent unauthorized access to idle machines. This policy applies to computers running a version of Linux or Unix that includes Gnome desktop 2.12 or later.

- Set the machine account password expiration time: This policy sets the machine account password's expiration time, which specifies when machine account passwords are reset in Active Directory.
- Linux password policies: Likewise includes policies to set the maximum and minimum number of days that a password can be used before it must be changed, to set the minimum number of characters for a user account password, and to enforce complexity requirements, such as containing a digit or a non-alphabetic character.

### **Enforce Security Settings on UNIX and Linux**

Likewise adds settings to control Linux- and UNIX-specific security features. Here are some of the group policies that Likewise provides to control Unix and Linux security features:

- Specification of a SUDO configuration file. A SUDO configuration file can be used to identify which users can access different sets of supervisor-only programs and scripts. SUDO configuration settings can refer to AD account groups. This facilitates the use of AD as a means for specifying different administrative roles and more granular control of restricted user access
- Specification of startup scripts. Likewise lets you specify script files that should be run whenever a computer is started. These scripts can be used to perform arbitrary security configuration operations
- Specification of standard CRON jobs. CRON jobs can be used to perform periodic security audits and other operations
- SELinux: A Security-Enhanced Linux group policy helps secure target computers running Red Hat Enterprise Linux by implementing mandatory access control to provide fine-grained control over the users and processes that are allowed to access a system or execute commands on it. SELinux can secure processes from each other. For example, if you have a public

web server that is also acting as a DNS server, SELinux can isolate the two processes so that a vulnerability in the web server process does not expose access to the DNS server.

- **AppArmor:** An AppArmor group policy helps secure target computers that are running SUSE Linux Enterprise. AppArmor is a Linux Security Module implementation of name-based access controls. To help protect your operating system and applications from threats, AppArmor uses security policies, called *profiles*, that define the system resources and privileges that an application can use.
- **Display a message of the day:** This policy sets a message of the day in the `/etc/motd` file. The message of the day, which appears after a user logs in but before the logon script executes, can give users information about a computer. For example, the message can remind users of security policies.
- **Display a message with the login prompt:** This policy sets a message in the `/etc/issue` file. The message, which appears before the login prompt, can display information about security policies.
- **SysLog:** This policy can help manage, troubleshoot, and audit your systems. You can log different facilities, such as cron, daemon, and auth, and you can use priority levels and filters to collect messages.
- **Set permissions with a file creation mask:** Likewise can set permissions for the files in the home directory that is created when a user logs on Linux and Unix computers. All the files in the home directory are preset with the ownership settings of the file creation mask, or `umask`.

### Mac OS X Security Policies

Likewise also includes group policies to apply Mac-specific security settings to computers running Mac OS X 10.4 or later.

- **Block UDP traffic on a Mac:** This policy sets the built-in Mac OS X firewall to block User Datagram Protocol traffic, which can help improve security.
- **Disable automatic user login:** This policy disables automatic login so that a user is required to log on every time the computer is turned on or restarted.
- **Log firewall activity:** To help monitor and audit Mac computers for security issues, this policy turns on firewall logging, which keeps a log of such events as blocked attempts, blocked sources, and blocked destinations.
- **Secure system preferences:** This policy locks system preferences on Mac OS X computers so that only administrators with the password can change the preferences.
- **Use firewall stealth mode:** This policy sets the built-in Mac OS X firewall to operate in stealth mode. Stealth mode cloaks the target computer behind its firewall. Stealth mode can help protect the target computer's security.
- **Use secure virtual memory:** This policy configures target computers running Mac OS X to store application data in secure virtual memory. In case the computer's hard drive is accessed without authorization, this policy sets the Mac to encrypt the data that it stores in virtual memory.

### Application Support

Likewise allows any Kerberos-enabled (“Kerberized”) application to support single sign-on (SSO) and user authorization through Active Directory. Likewise automatically configures sshd and Samba to support SSO. Likewise Software provides knowledge-base articles, software components and consulting help to configure other applications to support SSO, as well. SSO provides not only user convenience but also security benefits:

- Users do not have to remember different passwords for OS and application access. This results in fewer problems due to theft of written passwords
- Reduced costs due to fewer password resets
- Using AD for user authorization inside applications provides a consistent mechanism (group membership) for specifying different operational roles in order to restrict user access

### **Compliance Reporting**

Likewise can generate various reports that help you demonstrate which users can access what machines and what capabilities (group memberships) they have on those machines. These reports simplify the demonstration of your compliance with various standards. Likewise can also export report information to other products for further analysis.

- Likewise reports help you understand and demonstrate user access restrictions and compliance with regulatory requirements
- Likewise can generate HTML, XML, and CSV (comma-separated value) files to be processed by other reporting tools

## Summary

Likewise allows you to use your existing Microsoft Active Directory infrastructure to manage user accounts for both Windows and non-Windows systems. Likewise will help you lower administrative costs and demonstrate regulatory compliance while simultaneously improving the security of your network. Its security features provide:

- Strong cryptographic protocols
- Password and account policies extended to Linux and UNIX computers
- Group policy settings to control SUDO and other Linux- and UNIX-specific security systems
- Support for Kerberized applications
- Reporting tools to demonstrate regulatory compliance

Although some of these features are provided by other LDAP-based authentication and authorization solutions, only Likewise provides all of these features in a package that is easy to install and administer.

## For More Information

For more information on Likewise or to download a free 30-day trial version, visit the Web site at <http://www.likewisoftware.com>.

For general questions, call (800) 378-1330 or e-mail [info@likewisoftware.com](mailto:info@likewisoftware.com).

For technical questions or support for the 30-day free trial, e-mail [support@likewisoftware.com](mailto:support@likewisoftware.com).

### ABOUT LIKEWISE

Likewise® Software solutions improve management and interoperability of Windows, Linux, and UNIX systems with easy to use software for Linux administration and cross-platform identity management.

Likewise provides familiar Windows-based tools for system administrators to seamlessly integrate Linux and UNIX systems with Microsoft Active Directory. This enables companies running mixed networks to utilize existing Windows skills and resources, maximize the value of their Active Directory investment, strengthen the security of their network and lower the total cost of ownership of Linux servers.

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.