



IMPROVE SOX COMPLIANCE WITH CENTRALIZED ACCESS CONTROL AND AUTHENTICATION

- With Likewise Enterprise, you get one user, one ID — even in mixed networks.
- Integrate Linux, Unix, and Mac computers into Active Directory for role-based access control.
- Authenticate Linux, Unix, and Mac users with the highly secure Kerberos 5 protocol.
- Achieve separation of duties on Linux and Unix by using sudo group policies.
- Control access to sensitive resources.
- Enforce security settings across the enterprise.
- Monitor and audit security-related events such as denied sudo commands and failed logon attempts.

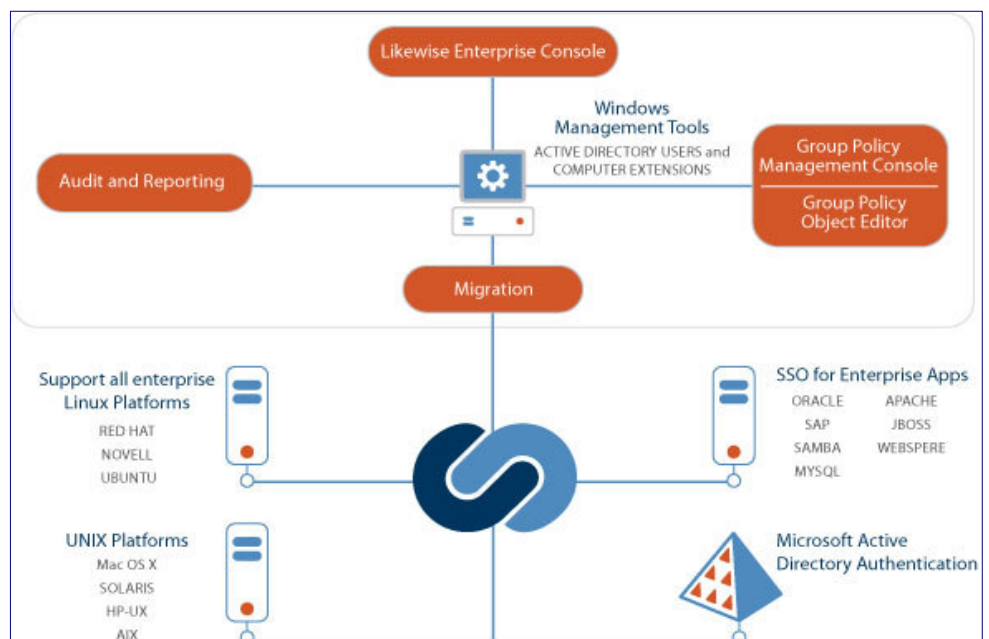
Using Likewise Enterprise to Boost Compliance with Sarbanes-Oxley

Abstract

Experts have been advising for some time that companies should change the way they approach Sarbanes-Oxley compliance, and after a few trips through the annual audit cycle, company leaders are coming to understand why. It no longer makes sense to treat SOX compliance as a recurring project that needs to be accomplished repeatedly at a particular point in time. A better approach is to integrate the principles of compliance into regular business processes so that compliance shows up 365 days a year — not just the day the auditor comes.

This paper begins by exploring why SOX compliance continues to be so difficult when it is treated as an annual project rather than a continuous process. Then the paper discusses how Likewise Enterprise can help your company make the shift to continuous compliance for identity and access management in a mixed network.

Likewise joins Linux, Unix, and Mac OS X computers to Active Directory, providing the basis to assign each user a unique ID for authentication, authorization, and monitoring. Likewise also includes group policies for non-Windows computers so that you can centrally manage their security settings in the same way as Windows computers.



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. The contents herein are subject to change without notice.

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

Introduction: The Compliance Scramble	4
Rapid Change Can Overwhelm Tight Controls	4
Building a Foundation for Compliance	5
The Common Denominator: Risk	6
The Principles of Compliance	7
Establishing Controls: Best Practices for SOX Compliance	7
Enforcing and Monitoring Controls	8
How Likewise Lays the Foundation For SOX IT Compliance Efforts	9
Feature Support for Internal Controls	11
Establishing Internal Controls with Likewise	11
Enforcing and Monitoring Controls	15
Likewise's Reporting Features.....	16
Summary	17
For More Information.....	19

Introduction: The Compliance Scramble

You've been through it more than once by now: The yearly time-consuming scramble to get all your IT systems into orderly compliance with the internal control requirements of Sarbanes-Oxley, or SOX. Access and identity management issues arise because your company uses not only Microsoft platforms but also Unix, Linux, and Mac to achieve best-of-breed IT infrastructure. You struggle to demonstrate internal controls in an environment where individuals can have multiple user names and passwords, and where user identities reside in more than one directory. Every time a user joins or leaves your company, you have to update each of these identity management systems separately — a time-consuming process that can leave security holes. The complexity of these identity management systems and their lack of central management increases the likelihood that something will go wrong. A user account with access to protected data, for example, might not get deprovisioned from one of the systems when the user leaves the company — which increases exposure to risk and might result in noncompliance. In addition, authorization mechanisms for your Unix, Linux, Mac, and Windows systems are completely separate, and your solutions for LDAP authentication seem to raise new questions all the time.

Even after you've made it through the compliance gauntlet — audits, deficiencies, remediation, workarounds — there is little satisfaction. The day after compliance is achieved, that's the day that non-compliance begins to creep back in — and soon thereafter the compliance scramble begins all over again.

Rapid Change Can Overwhelm Tight Controls

The push to achieve compliance continues to be time consuming and expensive every year. Why is that? Why don't systems put into compliance stay in compliance? Why does the project of demonstrating compliance never become routine and easily repeatable?

For one thing, enterprises are dealing with change at such a rapid rate that it is difficult to maintain effective controls. People are hired, lost, or transferred into new roles all the time. IT systems change through

acquisitions, expansions, upgrades, and migrations. Keeping tight control over who among the changing cast of users has access to what key information on which of the evolving systems is not an easy task. Identifying exactly who has access to what can be extremely difficult when that information resides in different systems, sometimes at great distances, and is managed in different ways on different operating systems. Without a consolidated central user directory controlling access for all systems, this year's SOX snapshot of access and authorization is bound to drift quickly out of focus.

It is also the case that the requirements for SOX compliance themselves represent something of a shifting goal. SOX does not specify IT requirements in any detail, but relies on more general principles that are subject to interpretation by auditors. Different auditors might ask different questions and require different information. Interpretations and expectations may also raise the bar higher for compliance year over year. In short, the controls and workarounds that were deemed adequate for compliance one year might be insufficient in a later year.

Building a Foundation for Compliance

So the key question becomes: How can you put in place internal controls that provide the *foundation* for compliance in the face of different auditors, shifting objectives, and various risks?

The answer of course depends on the kind of business you are, the matrix of risks and threats that you are likely to face, the requirements that you identify to mitigate risk, the control objectives that are likely to reduce risks, and finally the internal controls that you can put in place to achieve your objectives and reduce risk.

You can, however, generalize about the internal controls that, for any company, provide a strong foundation for Sarbanes-Oxley compliance.

This whitepaper outlines some general controls that you can develop to improve any IT compliance effort — and shows you how Likewise can quickly and easily implement a number of these controls to reduce risk and foster compliance in mixed networks.

The Common Denominator: Risk

Risk is the underlying factor that drives compliance efforts. In the context of SOX compliance, risk is the potential that a given threat, whether internal or external, will exploit the vulnerabilities of an asset or group of assets to cause loss or damage to the asset. The impact or severity of the risk is proportional to the business value of the potential loss and to the estimated frequency of the threat. To put it more directly — what could go wrong? Sensitive data could be lost or stolen. Your reputation could be damaged. You could lose money. Or maybe you just fail a compliance audit. Compliance remediation costs more than prevention.

The risks that you face give rise to requirements for mitigating risk. You might also have to meet industry-specific requirements as well as SOX's general requirements. (For example, companies that process credit card information must also meet the requirements of the [Payment Card Industry Data Security Standard](#).) Requirements in turn yield control objectives, and your objectives ultimately translate into internal controls — policies, practices, procedures,— that you put in place to mitigate risk and to help ensure SOX compliance:



The Principles of Compliance

The fundamental principles of compliance are straightforward:

1. Establish internal controls — the policies, procedures, and practices that reduce risk.
2. Enforce the internal controls, monitor their effectiveness, and be prepared to report on them and show them to auditors.

Establishing Controls: Best Practices for SOX Compliance

The following internal controls help ensure SOX compliance by putting in place fundamental policies and practices:

- One user, one identity. Each user has a unique identity, and that user's identity is authenticated by a secure protocol each time the user logs on a computer or accesses sensitive applications or resources.
- System-wide password enforcement. Every computer on the network requires a user to log on with a password.
- Secure authentication and two-factor authentication.
- Access control and authorization.
- Separation of duties.
- Timed computer lock downs after a short period without use.
- Log backups.
- One-way cross-forest trusts in Active Directory.
- System security and hardening to help prevent unauthorized access or external attacks.

Principles of Access Control

Access control and authorization breaks down into additional principles:

- Deny All That is Not Explicitly Permitted – Anything not explicitly allowed is denied.
- Least Privilege – Users and systems should only have minimum level of access necessary to perform their defined function. All unnecessary levels of access should be restricted unless explicitly needed.
- Defense-in-Depth – Overall security should not be reliant upon a single defense mechanism. If an outer security perimeter is penetrated, underlying layers should be available to resist the attack.
- Defense through Simplicity – A simple system is more easily secured than a complex system, as there is a reduced chance for error.
- Need-to-Know – Information will only be circulated to those parties that require it in order to perform their defined business function.
- Effective Authentication and Authorization – Firmly established identity and role-based authorization are essential to making informed access control decisions.

Enforcing and Monitoring Controls

The following methods of enforcing and monitoring controls can provide a solid foundation for dealing with annual audits:

- Extending the event filter in Active Directory to Linux, Unix, and Mac OS X computers.
- Centrally managing syslogs for Unix and Linux computers.
- Logging every sudoer command.
- Using cron scripts to alert you to changes in files or policies.

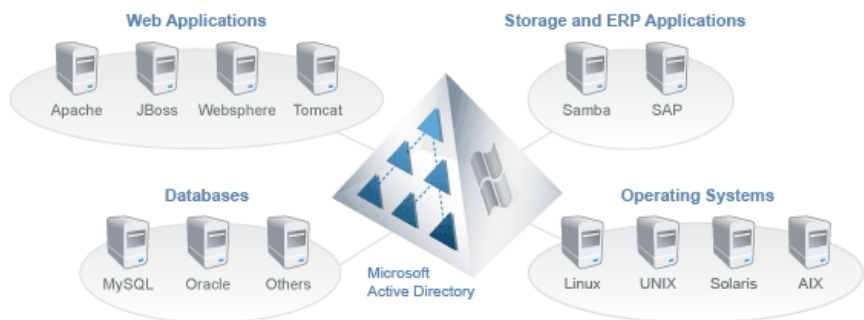
- Executing refreshes to undo unknown changes to, for example, sudo and automount files.
- Provisioning, deprovisioning, and managing changes when an employee joins the company, leaves the company, or changes roles.
- Reports that detail which users and groups have access to which systems.
- Auditing capabilities that show, for example, attempts to use sudo by unauthorized personnel, failed sudo attempts, failed logon attempts, and so forth.

Identifying the controls that are right for your company and integrating them into your regular business practices is the challenge. After discussing the challenges of achieving compliance when you have a mixed network, this section breaks down these high-level principles into everyday policies and practices that you can implement in a mixed network by using Likewise Enterprise.

How Likewise Lays the Foundation For SOX IT Compliance Efforts

Without a single, centralized identity management system in place, preparing for your yearly compliance audits will continue to be a grueling – and expensive – challenge.

Likewise helps overcome the challenges of complying with SOX by joining Linux, Unix, and Mac OS X computers to Microsoft Active Directory – a secure, scalable, stable, and proven Identity Management System.



Joining Linux, Unix, and Mac computers to Active Directory immediately yields a range of internal controls that are fundamental to any compliance effort:

- You can use a single, centralized identity management system that is secure, scalable, stable, and proven.
- You can provision each user with a single, unique ID that works on all your systems, and then use that ID to control access to resources, monitor sessions, and generate access reports.
- You can authenticate Linux, Unix, Mac, and Windows users with the highly secure Kerberos 5 protocol.
- You can implement role-based access controls that give users only the minimum access needed to do their jobs.
- You can apply group policies to Linux, Unix, and Mac computers to manage passwords policies, control root access, and manage logs.
- You can generate access reports that show which users and groups have access to which computers.
- You can audit event logs that show denied sudo attempts and failed logon attempts.

Feature Support for Internal Controls

This section details the support that Likewise provides for establishing, enforcing, and monitoring internal controls.

Establishing Internal Controls with Likewise

Likewise helps establish the following internal controls to provide the foundation for SOX compliance in a mixed network.

Internal Control	Likewise and AD Feature Support
A unique ID for each user.	Likewise empowers you to use Active Directory to assign a unique ID to each user, including not only Windows users, but also Linux, Mac, and Unix users. The unique ID can then be used on all computers joined to Active Directory.
System-wide password enforcement.	Using Likewise to join Linux, Unix, and Mac computers to Active Directory enables you to enforce passwords on all your systems.
Secure authentication.	Using Likewise with Active Directory makes the Kerberos 5 authentication protocol available to Unix, Linux, and Mac OS X as well as Windows computers. The highly secure and well-regarded Kerberos protocol encrypts the transmission and storage of passwords.
Two-factor authentication.	You can use Likewise with secure ID cards to extend Active Directory-based two-factor authentication to Unix, Linux, and Mac computers containing sensitive information or resources.
Separation of duties.	Likewise provides features that help separate duties: <ul style="list-style-type: none"> • Role-based authorization for Linux, Unix, and Mac computers.

Internal Control	Likewise and AD Feature Support
	<ul style="list-style-type: none"> • Sudo group policy.
Computer lock down.	Likewise includes group policies that lock down a Unix or Linux computer with a screensaver after a set period of inactivity. A user must re-enter a password to continue working.
Log rotation and backup.	Likewise includes a group policy to configure and customize your log-rotation daemon on Unix, Linux, and Mac OS X workstations and servers. For example, you can choose to use either a <code>logrotate</code> or <code>logrotate.d</code> file, specify the maximum size before rotation, compress old log files, and set an address for emailing log files and error messages. You can also enter commands to run before and after rotation.
One-way cross-forest trusts.	Likewise supports one-way cross-forest trusts.
System security and hardening.	Likewise includes group policies that help prevent external attacks, unauthorized access, and system changes: <ul style="list-style-type: none"> • An AppArmor group policy to help secure target computers that are running SUSE Linux Enterprise. AppArmor is a Linux Security Module implementation of name-based access controls. • A Security-Enhanced Linux group policy to help secure target computers running Red Hat Enterprise Linux. Security-Enhanced Linux, or SELinux, puts in place mandatory access control by using the Linux Security Modules, or

Internal Control	Likewise and AD Feature Support
	<p>LSM, in the Linux kernel. The security architecture, which is based on the principle of least privilege, provides fine-grained control over the users and processes that are allowed to access a system or execute commands on it.</p> <ul style="list-style-type: none"> • A group policy to log firewall activity on computers running Mac OS X. • A group policy to enable the built-in firewall on computers running Mac OS X. • A group policy to lock system preferences on target computers running Mac OS X so that only administrators with the password can change the preferences.
Password policies and logon security	<ul style="list-style-type: none"> • By using Likewise with Active Directory, you can enforce security settings for passwords on all the computers in your network, including password change intervals and minimum password length. • A Likewise group policy can require complex passwords, which must contain both numeric and alphabetic characters. • A Likewise group policy can enforce password history on computers that are joined to Active Directory. • With Active Directory, a group policy can specify the account lockout threshold — the

Internal Control	Likewise and AD Feature Support
	<p>number of invalid logon attempts before the account is locked.</p>
<p>Control access to resources.</p>	<p>Likewise ports the granular access control of Active Directory to Linux, Unix, and Mac OS X workstations and servers.</p> <p>Likewise and Active Directory empower you to control access to computer resources. Specifically, you can use Active Directory groups to control access to customer data only to those with a business need to know.</p> <p>User identifiers (UIDs) and group identifiers (GIDs) from NIS domains can be migrated to Active Directory and their mapping to Linux and Unix resources can be maintained through the use of Likewise <i>cells</i>. Cells provide a custom mapping of Active Directory users to UIDs and GIDs.</p>
<p>Role-based and need-to-know based access control</p>	<p>Likewise and Active Directory provide a mechanism for granular access control based on roles or need-to-know. You decide who needs to know: Only the users that you authorize get access to the systems that you specify, and all other users are denied.</p> <p>Likewise and Active Directory can restrict access in two ways: groups and sudo configuration files.</p> <p>In Active Directory, security groups are an efficient way to assign access to resources.</p> <p>A sudo configuration file can restrict access to commands on a computer to the users or groups that you specify.</p>

Enforcing and Monitoring Controls

The following methods of enforcing and monitoring controls can provide a solid foundation for dealing with annual audits in a mixed network:

Enforcement or Monitoring Mechanism	Likewise Feature Support
Provisioning, deprovisioning, and managing changes when an employee joins the company, leaves the company, or changes roles.	Likewise extends Active Directory's user provisioning and deprovisioning processes to Linux, Unix, and Mac computers.
Centralized and structured management of syslogs.	Likewise's syslog group policy can help you manage, troubleshoot, and audit your Unix and Linux systems from a central location: Active Directory. Likewise's syslog group policy includes a graphical user interface to configure and customize your syslog policies. You can log different facilities, such as cron, daemon, and auth, and you can use priority levels and filters to collect messages.
Event filtering.	Likewise extends the event filter in Active Directory to Linux, Unix, and Mac computers.
Logging sudo commands.	Likewise includes an event log subsystem that stores events on Unix, Linux, and Mac computers in a database. System administrators and security managers can use an event viewer to monitor and review events such as denied sudo commands.
Using cron scripts to alert you to changes in files or policies.	With Likewise's cron group policy, you can schedule commands, or cron jobs, that are executed at a set time on target Linux and Unix computers. You can use the policy to automatically run scripts that analyze files and policies for changes and alert you when they occur.

Enforcement or Monitoring Mechanism	Likewise Feature Support
Executing refreshes to undo unknown changes.	Likewise includes group policies for automount, syslog, cron jobs, script files, and sudo configuration files so that you can centrally manage and refresh these files on demand from a central location.
Auditing capabilities.	You can use Likewise's event log subsystem for compliance-related self-auditing and for preparing for an audit. The Likewise event log database, which can be accessed through an API, provides system administrators and security managers with an event viewer that shows, for example, denied sudo commands, failed logon attempts, and attempts to access resources for which a user is not authorized.

Likewise's Reporting Features

Likewise empowers you to create the following custom reports about Linux and Unix users, groups, computers, forests, and domains within Active Directory. These reports can aid your SOX compliance efforts by tracking and showing which users and groups have access to which systems.

Report	Description
Forest Users and Groups	Displays all Unix- and Linux-enabled users and groups in an Active Directory forest. This report can also display duplicate UIDs, GIDs, login names, and group aliases.
User Access	Shows the Unix and Linux machines that each Active Directory user can access.
Group Access	Lists the Unix and Linux machines

	that each AD group can access.
Group Membership	Shows the members of each Unix- and Linux-enabled Active Directory group.
Computer Access	Lists the users who can access each Unix and Linux computer.

You can choose the information that you want to include in a report by selecting from a variety of report columns. Depending on the type of report, you can select different columns for users, groups, computers, and cells. When you generate a User Access report, for example, you can select from such report columns as Login Name, Unix Login Name, User Status, UID, Primary GID, Login Shell, and Home Directory.

Each type of report includes filters and options. All the reports let you filter by domain. Depending on the type of report that you create, you can choose whether to show disabled users or disabled computers. For some reports you can limit the number of objects by specifying a maximum. For example, the Group Access report gives you a report option to set the maximum number of computers per group.

After you generate a report, you can view, save, preview, and print it.

Summary

To foster compliance with Sarbanes-Oxley, Likewise seamlessly integrates Linux, Unix, and Mac computers into Active Directory – a stable, secure, and scalable identity management system.

Likewise gives you the power not only to join non-Windows computers to Active Directory but also to migrate Linux and Unix users to Active Directory while maintaining their identities and permissions. Once you have joined non-Windows computers to Active Directory and migrated your Linux and Unix users, Likewise and Active Directory can help you comply with a number of practices that are fundamental to achieving SOX compliance:

- One user, one identity: Assign a single identity to each user and then use that ID to authenticate the user, authorize the user for access to resources based on his or her role, and monitor the user.
- Authenticate the encrypted passwords of users and groups with the highly secure Kerberos authentication protocol.
- Authorize and control access to resources.
- Apply group policies, such as for sudo configuration files and for password settings, to Linux, Unix, and Mac computers.

Together, Likewise and Active Directory provide a proven identity management system, ease management of your mixed network, improve security, and, most important, help you put in place practices that are fundamental to complying with Sarbanes-Oxley.

For More Information

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

For general questions, call (800) 378-1330 or e-mail info@likewise.com.

For technical questions or support for the 30-day free trial, e-mail support@likewise.com.

ABOUT LIKewise

Likewise Software is an open source company that provides authentication and auditing 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, auditing, 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.