



### IMPLEMENT SINGLE SIGN-ON FOR APPLICATIONS, SERVICES

- Use Active Directory credentials for single sign-on.
- One user, one ID
- Securely authenticate application users with Kerberos.
- Consistently implement security settings across the enterprise.
- Use Likewise to automatically configure Kerberos on Linux and Unix computers.
- Generating a keytab file.
- Use Likewise for SSO with SSH.
- Use Likewise for SSO with Apache Tomcat.

# Using Likewise for Single Sign-On With Kerberos and Active Directory

## Overview

Likewise Enterprise lets you join Linux and Unix computers running the applications and services to Microsoft Active Directory, yielding a range of benefits for users, system administrators, and managers.

Users get single sign-on: They log on once to a workstation that is authenticated through Active Directory and automatically receive Kerberos-based single sign-on for other computers and applications, including the application server. System administrators rest easy with the knowledge that users accessing your intranet through HTTP are securely authenticated with Kerberos 5 and authorized for access to the resources on your application server. Managers see their operational costs drop as their Linux and Unix computers are centrally managed within Active Directory. Security managers find help in their quest for regulatory compliance.

This document outlines how to configure applications to provide single sign-on authentication through Kerberos with Likewise and Active Directory.

## 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.

#### Introduction

When you log on a Linux, Unix, or Mac OS X computer by using your Active Directory domain credentials, Likewise initializes and maintains a Kerberos ticket granting ticket (TGT). With a TGT, you can log on other computers joined to Active Directory or applications provisioned with a Service Principal Name and be automatically authenticated with Kerberos and authorized for access through Active Directory. In a process transparent to the user, the underlying Generic Security Services (GSS) system requests a Kerberos service ticket for the Kerberos-enabled application or server. The result: single sign-on.

To gain access to the other computer, you can use various protocols and applications:

- SSH
- rlogin
- rsh
- Telnet
- FTP
- Firefox (for browsing of intranet sites)
- LDAP queries against Active Directory
- HTTP with an Apache HTTP Server

#### How Likewise Makes SSO Happen

Since Microsoft Windows 2000, Active Directory's primary authentication protocol has been Kerberos. When a user logs on a Windows computer that is joined to a domain, the operating system uses the Kerberos protocol to establish a key and to request a ticket for the user. Active Directory serves as the Kerberos key distribution center, or KDC.

Likewise configures Linux and Unix computers to interact with Active Directory in a similar way. When a user logs on a Linux and Unix computer joined to a domain, Likewise requests a ticket for the user. The ticket can then be used to implement SSO with other applications.

Likewise fosters the use of the highly secure Kerberos 5 protocol by automating its configuration and use on Linux and Unix computers. To ensure that the Kerberos authentication infrastructure is properly configured, Likewise does the following:

- Ensures that DNS is properly configured to resolve names associated with Active Directory (AD).
- Provides tools to join Linux, Unix, and Mac OS X computers to AD.
- Performs secure, dynamic DNS updates to ensure that Linux and Unix computer names can be resolved with AD-integrated DNS servers.
- Configures Kerberos. In an environment with multiple KDCs, Likewise makes sure that Kerberos selects the appropriate server.
- Configures SSHD to support SSO through Kerberos (by using GSSAPI).
- Creates a keytab for the computer in the following way: When you join a Linux or Unix computer to AD, Likewise creates a machine account for the computer. Likewise then automatically creates a keytab for the SPN and places it in the standard system location (typically `/etc/krb5.keytab`).
- Provides a tool, `lwinet`, to generate additional keytab entries for other applications or services.
- Creates a keytab for the user during logon. On most systems, the user keytab is placed in the `/tmp` directory and named `krb5cc_UID`, where `UID` is the numeric user ID assigned by the system.

### How to Implement SSO with Likewise

When you install Likewise on a Linux, Unix, or Mac OS X computer and join it to Active Directory, Likewise prepares it for single sign-on by creating a keytab for the computer. However, when you use Likewise to implement SSO with other applications or services, such as SAP or Oracle, you will likely have to configure the application to use Kerberos authentication and you will likely have to provision each application user for external Kerberos authentication. At the very least, however, you will

have to provision your application with a Service Principal Name in Active Directory.

**Note:** Configuring an application such as SAP or Oracle for SSO with Kerberos is beyond the scope of the Likewise documentation; for more information, see the manual for your application.

### Example of Configuration Steps for Apache Tomcat

The following process outlines the steps for setting up an application or service -- here, Apache Tomcat -- to use Likewise for single sign-on.

1. Create a service account for Tomcat in Active Directory.
2. Associate a Service Principal Name, or SPN, with the service account in Active Directory.
3. Create a keytab for the SPN.
4. Place the keytab in the appropriate location on the Linux or Unix computer.
5. Add the Likewise Java authentication module (a valve class) to Tomcat.
6. Configure the authentication module to get its Kerberos key from the generated keytab.
7. Configure the authentication module to determine Java roles by examining Active Directory group membership.
8. Configure an application to restrict access to Active Directory authenticated users in certain roles.
9. Test Tomcat SSO by accessing restricted web sites from a Windows client running Microsoft Internet Explorer or Mozilla Firefox. Repeat this step on Linux and Unix using Firefox.

### Example of Configuration Steps for OpenSSH

Although Likewise automatically configures OpenSSH to support SSO through Kerberos, it is worthwhile to review how Likewise does so. Because you might need to configure other applications for SSO,

understanding the process will make it easier to apply the technique to other applications.

**Note:** Not all versions of OpenSSH support Kerberos. Versions older than 4.2p1 might not work or might work improperly.

### The SSH Service Principal Name

The first thing that needs to be considered is the Kerberos service principal name (SPN) that is used by `ssh` and `sshd`. The SPN is a string that identifies the service for which an authentication ticket is to be generated. In the case of SSH, the SPN has the form:

```
host/<server name>@<REALMNAME>
```

For example, when a user uses `ssh` to connect to a computer named `fizzie.mycorp.com`, the `ssh` program will request a service ticket for the SPN:

```
host/fizzie.mycorp.com@MYCORP.COM
```

**Note:** The Kerberos realm is the computer's domain name using uppercase letters.

### System Keytab Generation

In order for Microsoft Active Directory to generate a Kerberos ticket for this SPN, a service account must exist for it. Additionally, a keytab must be created for the service account and placed on the `sshd` server. Likewise completely automates this operation. When a Linux or Unix computer is joined to AD, a machine account is created for the computer. If the computer is called `fizzie`, a machine account called `fizzie$` is created in AD. Likewise then automatically creates a keytab for the SPN and places it in the standard system location (typically, `/etc/krb5.keytab`). Likewise includes a tool, `lwinet`, that can be used to generate additional keytab entries for other services.

### User Keytab Generation

When the user runs the `ssh` program and OpenSSH determines that it will use Kerberos authentication, it will need to access a keytab for the user so that it can obtain a service ticket for the service/computer to which it is trying to connect. This keytab must be created using the user's account

name and password. Manually, this can be performed by using the Linux/UNIX kinit utility. Likewise, however, does it automatically when the user logs into the computer. On most systems, the user keytab is placed in the `/tmp` directory and named `krb5cc_UID` where `UID` is the numeric user ID assigned by the system.

### Configuring OpenSSH

OpenSSH must be configured at both the client and server computer. On the client, the `ssh_config` file (typically, in `/etc/ssh/ssh_config`) must be modified. On the server, `sshd_config` (typically, in `/etc/ssh/sshd_config`) must be modified.

In the server, the following lines must be present in `sshd_config`:

```
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

On the client, these lines must be present in `ssh_config`:

```
GSSAPIAuthentication yes
GSSAPIDelegateCredentials yes
```

Likewise adds these lines to the appropriate files if they are not already present.

### Testing SSO

With OpenSSH properly configured, demonstrating SSO support is simple. Log on a Linux or Unix machine running Likewise by using Active Directory credentials and then use `ssh` to connect to another machine that's also running Likewise. OpenSSH should establish a connection without prompting for a username or password.

### 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.