Likewise Open 5.0 Installation And Administration Guide

IN THIS DOCUMENT

Abstract

Likewise Open joins Linux, Unix, and Mac OS X computers to Microsoft Active Directory so that you can centrally manage all your computers, authenticate users, and authorize access to resources. This guide describes how to install and administer Likewise Open, an open source version of Likewise Enterprise that includes the Likewise agent. The guide covers installing the agent, joining an Active Directory domain, logging on with Active Directory credentials, and troubleshooting the agent.

This guide is supplemented by the Likewise Open community mailing list, which you can join at http://www.likewisesoftware.com/community/ and use to discuss and troubleshoot Likewise Open with other users and developers.

Table of Contents

Likewise Open

Likewise Open

Quick Start for Linux

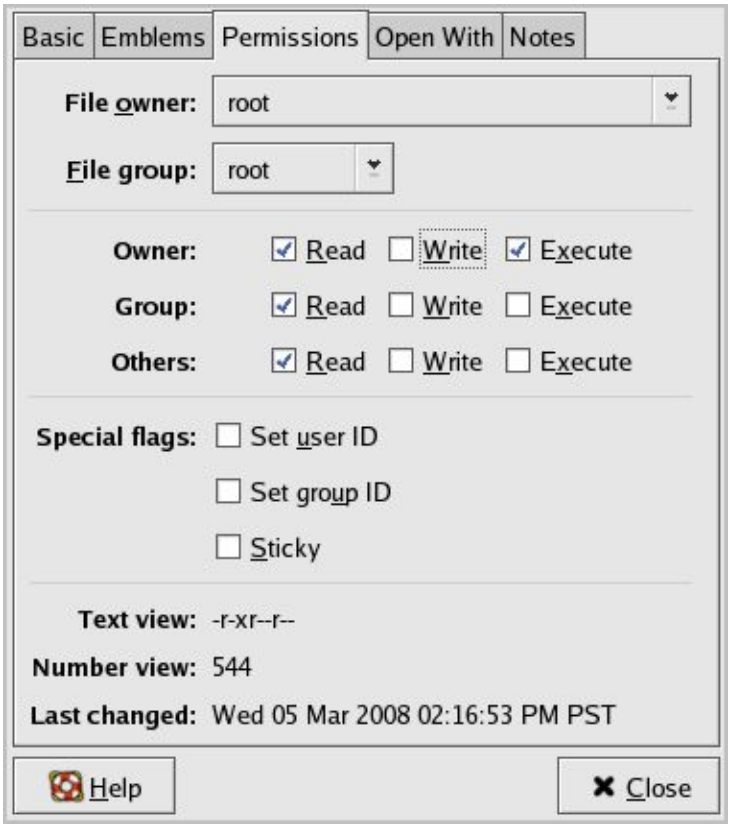
This chapter covers the basics of installing Likewise Open on a Linux computer, joining it to an Active Directory domain, and logging on with your Active Directory credentials. For more information, see the other chapters in this manual.

Install the Agent on Linux with the BitRock GUI

For most Linux platforms, you can install the Likewise Open agent or the Likewise Enterprise agent by using a BitRock installer — an executable whose file name ends with `installer`. Example: `LikewiseOpen-4.1.0.2921-linux-i386-rpm-installer`.

The following procedure assumes that you downloaded or copied the Likewise installer to the desktop of your Linux computer.

1. As root, on the desktop, right-click the installer, click **Properties**, click the **Permissions** tab, select **Execute** for **Owner**, and then click **Close**:



Tip: You can also make the installer executable from the command line with `chmod a+x`.

2. Double-click the installer to run it, and then follow the instructions in the installation wizard.

Join Linux to Active Directory with the Command Line

On Linux, the location of the domain join command-line utility is as follows:

```
/opt/likewise/bin/domainjoin-cli
```

Important: To run the command-line utility, you must use a **root** account. To join a computer to a domain, you must have the user name and password of an Active Directory account that has privileges to join computers to the domain and the full name of the domain that you want to join.

Before Joining a Domain

To join a domain, the computer's name server must be able to find the domain and the computer must be able to reach the domain controller. You can make sure the name server can find the domain by running this command:

```
nslookup domainName
```

You can verify that your computer can reach the domain controller by pinging it:

```
ping domainName
```

If either of these tests fails, see Check System Health Before Installing the Agent and Solve Domain-Join Problems.

Join a Linux Computer to Active Directory

- Execute the following command as root, replacing `domainName` with the FQDN of the domain that you want to join and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join domainName joinAccount
  ```

Example: `/opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator`

Log On with AD Credentials

After the Likewise agent has been installed and the Linux or Unix computer has been joined to a domain, you can log on interactively by using your Active Directory credentials. For example, you can log on by using the form `DOMAIN\userame`.

1. On a Linux computer, log out of the current session.
2. Log on the system console by using an Active Directory user account in the form of `DOMAIN\username`, where `DOMAIN` is the Active Directory short name.

Note: When you log on from the command line, you must use a slash to escape the slash character, making the logon form `DOMAIN\\username`.

Example with ssh: `ssh likewisedemo.com\\hoenstiv@localhost`

The Likewise Agent

Likewise Open is an agent that runs on Linux, Unix, and Mac OS X computers so that you can join them to Microsoft Active Directory and authenticate users with their Active Directory credentials.

This guide describes how to install Likewise Open, join computers running Linux, Unix, or Mac OS X to Microsoft Active Directory, and manage the Likewise Open Agent.

Likewise Open is free to download and use according to the terms of its license. To download Likewise Open or obtain the source code, go to http://www.likewisesoftware.com/products/likewise_open/.

The target audience for this document is network directory administrators who manage access to workstations, servers, and other network resources within Active Directory. The guide assumes that you know how to administer Active Directory as well as computers running Linux, Unix, and Mac OS X.

About the Likewise Agent

The Likewise agent integrates with the core operating system on Linux, Unix, and Mac OS X computers to implement the mapping for any application, such as the logon process (`/bin/login`), that uses the name service (NSS) or pluggable authentication module (PAM).

The agent acts as a Kerberos 5 client for authentication and as a LDAP client for authorization. In Likewise Enterprise, the agent also retrieves and enforces group policy objects to securely update local configurations, such as the sudo file.

The Likewise agent comprises the following daemons:

Daemon	Description
`/opt/likewise/sbin/lsassd`	The Likewise authentication daemon. It handles authentication, authorization, caching, and idmap lookups.
`/opt/likewise/sbin/netlogond`	Detects the optimal domain controller and global catalog

	and caches the data.
`/opt/likewise/sbin/npcmuxd`	Named pipe multiplexer.
`/opt/likewise/sbin/dcerpcd`	The DCE/RPC daemon. *DCE/RPC* stands for Distributed Computing Environment/Remote Procedure Calls. The daemon handles communication between Linux, Unix, Mac computers and Active Directory.
`/opt/likewise/sbin/gpagentd`	The group policy agent. Part of Likewise Enterprise, it runs as a background service to pull group policy objects from Active Directory and apply them to the computer.

The agent includes a number of libraries in `/opt/likewise/lib`.

The agent uses the following ports for outbound traffic. The agent is a client only; it does not listen on any ports.

Port	Protocol	Use
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos
123	UDP	NTP
137	UDP	NetBIOS Name Service
139	TCP	NetBIOS Session (SMB)
389	UDP/TCP	LDAP

445	TCP	SMB over TCP
464	UDP/TCP	Machine password changes (typically after 30 days)
3268	TCP	Global Catalog search

Caches

To maintain the current state and to improve performance, the Likewise agent caches information in four files, all of which are in `/var/lib/likewise/db`:

Cache File	Description
lsass-adcache.db	Cache managed by the Active Directory authentication provider.
lsass-local.db	Repository managed by the local authentication provider.
netlogon-cache.db	Domain controller affinity cache, managed by `netlogond`
pstore.db	Repository storing the join state and machine password

Time Synchronization

For the Likewise agent to communicate over Kerberos with the domain controller, the clock of the client must be within the domain controller's maximum clock skew, which is 300 seconds, or 5 minutes, by default. (For more information, see http://web.mit.edu/kerberos/krb5-1.4/krb5-1.4.2/doc/krb5-admin/Clock-Skew.html.)

The clock skew tolerance is a server-side setting. When a client communicates with a domain controller, it is the domain controller's Kerberos Key Distribution Center that determines the maximum clock skew. Changing the maximum clock skew in the client's `krb5.conf` file

does not affect the clock skew tolerance of the domain controller and will not unable a client outside the domain controller's tolerance to communicate with it.

The clock skew value that is set in the `/etc/likewise/krb5.conf` file of Linux, Unix, and Mac OS X computers is useful only when the computer is functioning as a server for other clients. In such cases, you can use a Likewise Enterprise group policy to change the maximum tolerance; for more information, see Set the Maximum Tolerance for Kerberos Clock Skew.

The domain controller uses the clock skew tolerance to prevent replay attacks by keeping track of every authentication request within the maximum clock skew. Authentication requests outside the maximum clock skew are discarded. When the server receives an authentication request within the clock skew, it checks the replay cache to make sure the request is not a replay attack. For more information, see the resources below.

Troubleshooting Kerberos

The following resources can help troubleshoot time synchronization and other Kerberos issues:

- Kerberos Authentication Tools and Settings: http://technet2.microsoft.com/windowsserver/en/library/b36b8071-3cc5-46fa-be13-280aa43f2fd21033.mspx
- Authentication Errors Caused by Unsynchronized Clocks: http://technet2.microsoft.com/windowsserver/en/library/6ee8470e-a0e8-40b2-a84f-dbec6bcbd8621033.mspx
- Kerberos Technical Supplement for Windows: http://msdn2.microsoft.com/en-us/library/aa480609.aspx
- The Kerberos Network Authentication Service (V5) RFC: http://www.ietf.org/rfc/rfc4120.txt
- Troubleshooting Kerberos Errors: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.mspx
- Kerberos and LDAP Troubleshooting Tips: http://www.microsoft.com/technet/solutionaccelerators/cits/interopmigration/unix/usecdirw/17wsdsu.mspx

Using a Network Time Protocol Server

If you set the system time on your computer with a Network Time Protocol (NTP) server, the time value of the NTP server and the time value of the domain controller could exceed the maximum skew. As a result, you will be unable to log on your computer.

If you use an NTP server with a cron job, there will be two processes trying to synchronize the computer's time -- causing a conflict that will change the computer's clock back and forth between the time of the two sources.

Likewise recommends that you configure your domain controller to get its time from the NTP server and configure the domain controller's clients to get their time from the domain controller.

Automatic Detection of Offline Domain Controller and Global Catalog

The Likewise authentication daemon -- `lsassd` -- manages site affinity for domain controllers and global catalogs and caches the information with `netlogond`. When a computer is joined to Active Directory, `netlogond` detects the optimum domain controller to use and caches the information. If the primary domain controller goes down, `lassd` automatically detects the failure and switches to another domain controller and another global catalog within a minute.

However, if another global catalog is unavailable within the forest, the Likewise agent will be unable to find the Unix and Linux information of users and groups. The Likewise agent must have access to the global catalog to function. Therefore, it is a recommended that each forest has redundant domain controllers and redundant global catalogs.

UID-GID Generation

In Likewise Open, UIDs and GIDs are generated by hashing the security identifier, or SID, from Active Directory. With Likewise Open, you do not need to make any changes to Active Directory. A user's UID and GID stay the same across host machines. Likewise caches credentials so users can logon when the computer is disconnected from the network or Active Directory is unavailable.

Upgrade to the Latest Agent

Before you upgrade to the latest version of the Likewise agent, it is recommended that you leave the domain, uninstall the domain join GUI, and uninstall the current agent.

Installing the Agent

You must install the Likewise agent on each Linux, Unix, or Mac OS X computer that you want to join to Active Directory. To obtain the installer or to view a list of supported platforms, see www.likewisesoftware.com.

The procedure for installing the Likewise Open agent or the Likewise Enterprise agent depends on the operating system of your target computer. Each procedure is documented in a separate section of this manual.

Operating System	Procedure by Title
Linux platforms running `glibc` 2.3 or later	Install the Agent on Linux with the BitRock GUI
Linux platforms running `glibc` 2.2 or earlier	Install the Agent on Linux with glibc 2.2 or Earlier
Unix: Sun Solaris, HP-UX, IBM AIX	Install the Agent on Unix with the Command Line
Mac OS X 10.4 or later	Install the Agent on a Mac Computer

You also have the option of installing the agent in unattended mode; see Install the Agent on Linux in Unattended or Text Mode and Install the Agent on a Mac in Unattended Mode.

Checking Your glibc Version

To determine the version of `glibc` on your Linux machine, run the following command:

```
rpm -q glibc
```

Requirements

This section lists the requirements to use Likewise. You must have at least the following components:

1. An Active Directory domain controller
2. One or more Unix, Linux, or Mac OS X computers

Administrator Privileges

- Root access or sudo permission on the Unix, Linux, and Mac OS X computers that you want to join to the domain.
- Active Directory credentials that allow you to add computers to an Active Directory domain -- for example, membership in the Domain Administrators security group or the Enterprise Administrators security group.

Active Directory Requirements

- Windows 2003 SP1 or R2 Standard and Enterprise
- Windows 2000 SP4 Server

Unix and Linux Requirements for the Agent

- An operating system that Likewise supports, such as versions of Mac OS X, Red Hat, SUSE Linux, Fedora, CentOS, Debian, Solaris, AIX, HP-UX, and Ubuntu. For a complete list of supported platforms, see the list of supported platforms at www.likewisesoftware.com.

Overview of the Installation Process

The installation and deployment process typically proceeds in the following order:

1. Make sure your computers meet the installation requirements and then download the Likewise software package from www.LikewiseSoftware.com.
2. Check the system health of your Linux, Unix, and Mac computers as well as Active Directory before installation.
3. Install the Likewise agent on each Unix, Linux, or Mac OS X computer that you want to join to the Active Directory domain.
4. Join Unix and Linux computers to the Active Directory domain.
5. Troubleshoot any deployment issues and optimize the deployment for your unique mixed network.

Checking System Health Before Installation

The following table lists items each item to check, describes the item, and suggests corrective action.

Item to Check	Corrective Action
Type of operating system	Install the agent on a computer that is running a supported operating system.
Processor type	Install the agent on a computer with a supported processor.
Disk usage	Increase the amount of disk space available to `/opt` or `/usr`.
Contents of `/etc/*release` (for AIX, to determine the `oslevel`)	Install the agent on a computer that is running a supported operating system and version.
Network interface and its status	Configure the computer so that it has network access and can communicate with the domain controller.
Contents of the IP routing table	If the computer does not use a single default gateway, you must define a route to a single default gateway. For example, you can run the `route -n` to view the IP routing table and set a static route. For more information, see the man pages for your system. On Solaris, you may need to create or edit `/etc/defaultrouter`. On Linux, you can set the default gateway by running the network utility for your distribution.
Connectivity to the default gateway	Configure the computer and the network so that the computer can connect to the default gateway.
Contents of `nsswitch.conf` (or, for AIX, `netsvc.conf`)	The `nsswitch.conf` file must contain the following line: `hosts: files dns` Computers running Solaris, in particular, may not contain this line in `nsswitch.conf`.
FQDN	Make sure the computer's FQDN is correct in `/etc/hosts`. You can determine the fully qualified domain name of a computer running Linux, Unix, or Mac OS X by executing the following command:

Item to Check	Corrective Action

	`ping -c 1 `hostname``
	
	On HP-UX:
	`ping `hostname` -n 1`
	
	On Solaris:
	`FQDN=`/usr/lib/mail/sh/check-hostname|cut -d" " -f7`;echo $FQDN`
	
	This command prompts the computer to look up the primary host entry for its hostname. In most cases, it looks for its hostname in `/etc/hosts`, returning the first FQDN name on the same line. So, for the hostname `qaserver`, here's an example of a correct entry in `/etc/hosts`:
	
	`10.100.10.10 qaserver.corpqa.likewise.com qaserver`
	
	If, however, the entry in `/etc/hosts` incorrectly lists the hostname (or anything else) before the FQDN, the computer's FQDN becomes, using the malformed example below, `qaserver`:
	
	`10.100.10.10 qaserver qaserver.corpqa.likewise.com`
	
	If the host entry cannot be found in `/etc/hosts`, the computer looks for the results in DNS instead. This means that the computer must have a correct A record in DNS. If the DNS information is wrong and you cannot correct it, add an entry to `/etc/hosts`.

IP address of local NIC	Either update DNS or change the local IP address so that the IP address of the local network card matches the IP address returned by DNS for the computer.
Contents of `resolv.conf`	Compare against the results of the items checked next.
DNS query results for system (hostname and IP)	Either update DNS or change the local IP address so that the IP address of the local network card matches the IP address returned by DNS for the computer.
DNS name resolution and connectivity to specified domain	Correct `resolv.conf` so that the `nameserver` points to a DNS server that can resolve the Active Directory domain name -- typically

Item to Check	Corrective Action
controller	the domain controller running DNS.
SRV records from DNS	Correct `resolv.conf` so that the `nameserver` points to a DNS server that can resolve the SRV records.
Location and version information for sudo, openssl, bash, rpm, and ssh	Likewise requires the following utilities: ssh and openssl. The other utilities are optional but may be useful.
Selected firewall settings (Kerberos, NetBIOS, and LDAP)	Reconfigure the firewall to allow the computer to access the domain controller.
DHCP	Set the computer to a static IP address or configure DHCP so that it does not update such files as `/etc/resolv.conf` and `/etc/hosts`.
ISA type	Use the installer for your ISA type.
Read-only filespaces	Make sure that `/usr` or `/opt` are writable.
AIX TL levels	Not all TL levels are supported. For AIX, check with Likewise support to make sure that Likewise is compatible with the TL level you are using.

Download Likewise Open

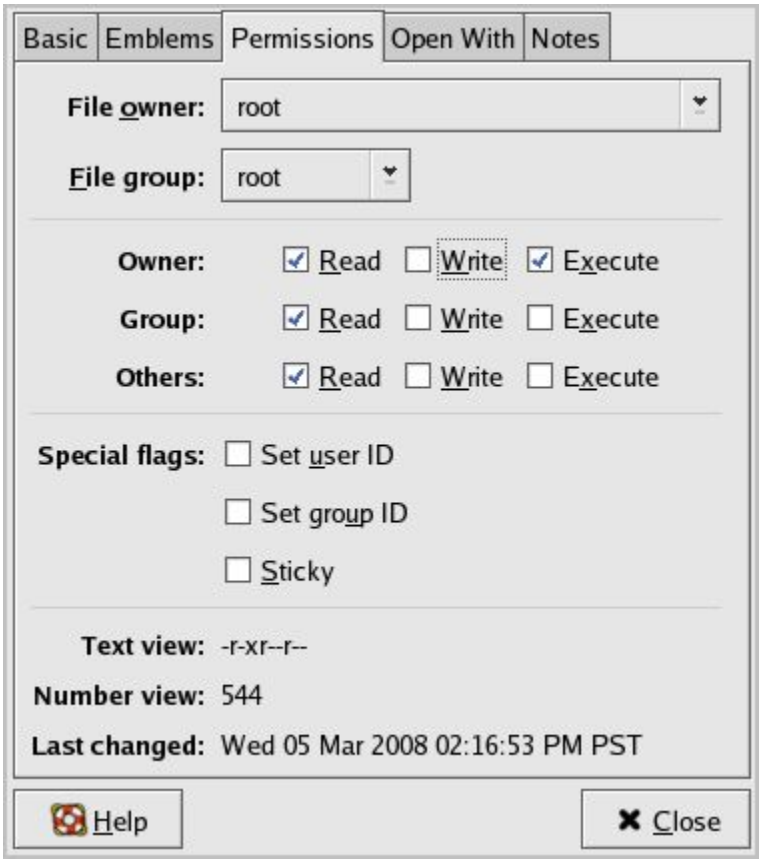
You can freely download the Likewise Open installation package at http://www.likewisesoftware.com/products/likewise_open/.

Install the Agent on Linux with the BitRock GUI

For most Linux platforms, you can install the Likewise Open agent or the Likewise Enterprise agent by using a BitRock installer — an executable whose file name ends with `installer`. Example: `LikewiseOpen-4.1.0.2921-linux-i386-rpm-installer`.

The following procedure assumes that you downloaded or copied the Likewise installer to the desktop of your Linux computer.

3. As root, on the desktop, right-click the installer, click **Properties**, click the **Permissions** tab, select **Execute** for **Owner**, and then click **Close**:



   Tip: You can also make the installer executable from the command line with `chmod a+x`.

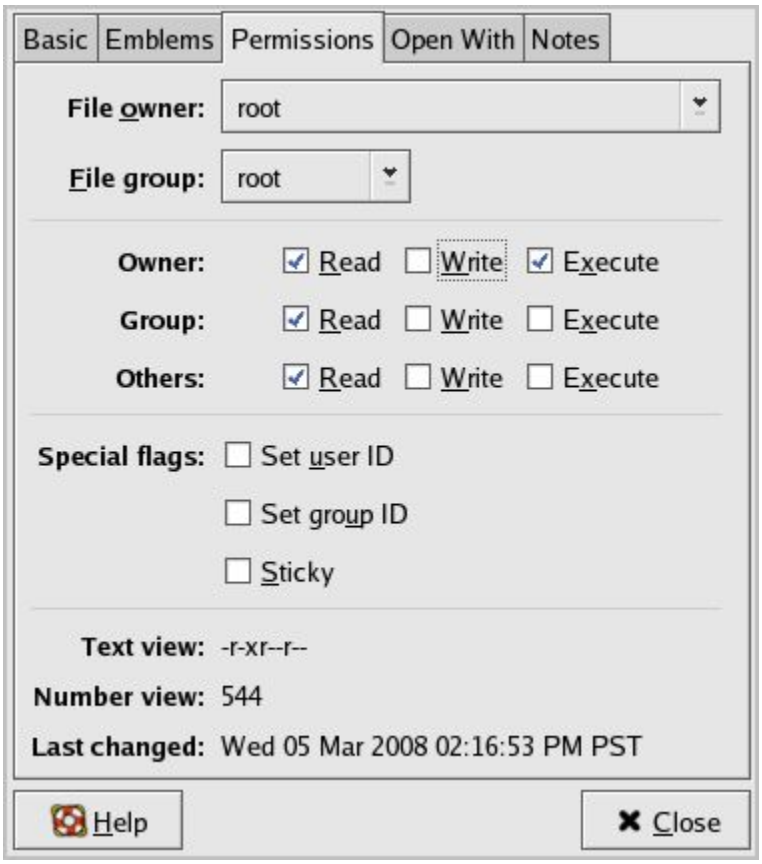
4. Double-click the installer to run it, and then follow the instructions in the installation wizard.

Install the Domain Join GUI

You can install the optional graphical user interface version of the Likewise domain join tool on a Linux computer after you have installed the Likewise agent. The domain join tool can be installed on Linux platforms that are running GTK+ version 2.6 or later.

Note: You do not need to install the domain join GUI to join a domain; for more information, see Join Active Directory with the Command Line.

1. Obtain the BitRock installer for the domain join tool for your platform from Likewise Software at http://www.LikewiseSoftware.com.
2. Copy the installer to the desktop of the target Linux computer.
3. As root, on the desktop, right-click the icon for the installer, click **Properties**, and then click the **Permissions** tab.
4. Change the owner's permissions to **Read** and **Execute**, and then click **Close**:



5. On the desktop, double-click the icon of the installer to run it, and then follow the instructions in the installation wizard.

Install the Agent on Linux with glibc 2.2 or Earlier

Linux platforms running `glibc` 2.2 or earlier require you to use the `oldlibc` installer -- a shell script that includes `oldlibc` in its name; example: `LikewiseIdentityServiceOpen-5.0.0.3494-linux-oldlibc-i386-rpm.sh`.

To check the version of `glibc` on your Linux computer, execute the following query:

```
rpm -q glibc
```

The following platforms are running `glibc` 2.2 or earlier and thus require the `oldlibc` installer:

- Red Hat Enterprise Linux AS 2.1
- Red Hat Enterprise Linux ES 2.1
- Red Hat Enterprise Linux WS 2.1
- Red Hat Linux 7.2
- Red Hat Linux 7.3
- Red Hat Linux 8
- Red Hat Linux 9
- SUSE 8.2

Install the Agent on glibc 2.2 or Earlier

Perform the following procedure with the root account.

1. Download or copy the `oldlibc` installer to the Linux computer's desktop.

   Important: If you FTP the file to the desktop of the target Linux computer, you must select binary, or BIN, for the transfer. Most FTP clients default to AUTO or ASCII, but the installer includes some binary code that will become corrupted in AUTO or ASCII mode.

2. Change directories to the desktop.

3. As root, change the mode of the installer to executable:

   ```
   chmod a+x LikewiseIdentityServiceOpen-5.0.0.3494-linux-oldlibc-i386-rpm.sh
   ```

   Tip: To view information about the installer or to view a list of command-line options, run the following command:

```
./LikewiseIdentityServiceOpen-5.0.0.3494-linux-
oldlibc-i386-rpm.sh --help
```

4. As root, run the installer:

```
./LikewiseIdentityServiceOpen-5.0.0.3494-linux-
oldlibc-i386-rpm.sh
```

5. Follow the instructions in the installer.

Install the Agent on Linux in Unattended or Text Mode

When you use the BitRock installer, command-line tools can help deploy the Likewise agent to multiple computers or install the agent remotely.

You can use the command-line tools to automatically install the agent, join the computer to a domain, and obtain credentials. For example, you can automate the installation of the agent by using the installation command in unattended mode:

```
 LikewiseEnterprise-4.1.0.2513-linux-x86_64-rpm-
installer --mode unattended
```

For Unix and Linux hosts, you can run the installer from the shell prompt with no special treatment. The installer detects that it is running in character mode and displays a character mode user interface, or you can force it into character mode with the option `--mode text`:

```
 LikewiseEnterprise-4.1.0.2513-linux-x86_64-rpm-
installer --mode text
```

Install the Agent on Unix with the Command Line

You can install the Likewise Open agent or the Likewise Enterprise agent on Sun Solaris, HP-UX, and IBM AIX by using a BitRock installer — an executable whose file name ends with `installer`. Example: `LikewiseIdentityServiceEnterprise-5.0.0.3499-solaris-sparc-pkg-installer`.

The examples shown are for Solaris Sparc systems. For other Unix platforms, simply substitute the appropriate installer. The installer's name

includes the product name, version and build numbers, operating system, computer type, and platform type.

Perform the following procedure with the root account.

1. Download or copy the installer to the Unix computer's desktop.
2. Change directories to the desktop.
3. As root, change the mode of the installer to executable:

   ```
   chmod a+x LikewiseIdentityServiceEnterprise-5.0.0.3499-solaris-sparc-pkg-installer
   ```

   Tip: To view a list of command-line options, run the following command:

   ```
   ./LikewiseIdentityServiceEnterprise-5.0.0.3499-solaris-sparc-pkg-installer --help
   ```

4. As root, run the installer:

   ```
   ./LikewiseIdentityServiceEnterprise-5.0.0.3499-solaris-sparc-pkg-installer
   ```

5. Follow the instructions in the installer.

Install the Agent on a Mac Computer

To install the Likewise agent on a computer running Mac OS X, you must have administrative privileges on the Mac. Likewise supports Mac OS X 10.4 or later.

1. Obtain the Likewise agent installation package for your Mac from Likewise Software and place it on your desktop.

   Important: On an Intel-based Mac, install the **i386** version of the `.dmg` package. On a Mac that does not have an Intel chip, install the **powerpc** version of the `.dmg` package.

2. Log on the Mac with a local account.
3. On the **Apple** menu , click **System Preferences**.

4. Under **Internet & Network**, click **Sharing**, and then select the **Remote Login** check box. Turning on Remote Login lets you access the Mac with SSH after you install Likewise.

5. On the Mac computer, go to the Desktop and double-click the Likewise `.dmg` file.

6. In the Finder window that appears, double-click the Likewise `.mpkg` file.

7. Follow the instructions in the installation wizard.

   When the wizard finishes installing the package, you are ready to join the Mac to an Active Directory domain.

Install the Agent on a Mac in Unattended Mode

The Likewise command-line tools can remotely deploy the shell version of the Likewise agent to multiple Mac OS X computers, and you can automate the installation of the agent by using the installation command in unattended mode.

The commands in this procedure require administrative privileges.

Important: For Intel-based Macs, use the **i386** version of the `.dmg` installer; for example: `LikewiseEnterprise-4.1.0.2779-i386.dmg`. For Macs that do not have Intel chips, use the **powerpc** version of the `.dmg` installer; for example: `LikewiseEnterprise-4.1.0.2779-powerpc.dmg`

The procedure below assumes you are installing the agent on an i386 Mac; if you are installing on a powerpc, replace the i386 installer with the powerpc installer.

1. Use SSH to connect to the target Mac OS X computer and then use SCP to copy the `.dmg` installation file to the desktop of the Mac or to a location that can be accessed remotely. The rest of this procedure assumes that you copied the installation file to the desktop.

2. On the target Mac, open Terminal and then use the `hdiutil mount` command to mount the `.dmg` file under `Volumes`:

   ```
   /usr/bin/hdiutil mount Desktop/LikewiseEnterprise-4.1.0.2779-i386.dmg
   ```

3. Execute the following command to open the `.mpkg` volume:

   ```
   /usr/bin/open Volumes/LikewiseEnterprise-
   4.1.0.2779-i386
   ```

4. Execute the following command to install the agent:

   ```
   sudo installer -pkg /Volumes/LikewiseEnterprise-
   4.1.0.2779-i386/LikewiseEnterprise-4.1.0.2779-
   i386.mpkg -target LocalSystem
   ```

   Note: For more information about the `installer` command, in Terminal execute the following command:

   ```
   man installer
   ```

5. To join the domain, execute the following command in the Terminal, replacing `domainName` with the FQDN of the domain that you want to join and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

   ```
   sudo /opt/likewise/bin/domainjoin-cli join
   domainName joinAccount
   ```

   Example: `sudo /opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator`

   Terminal prompts you for two passwords: The first is for a user account on the Mac that has admin privileges; the second is for the user account in Active Directory that you specified in the join command.

   Note: You can also add the password for joining the domain to the command, but Likewise recommends against this approach because another user could view and intercept the full command that you are running, including the password:

   ```
   sudo /opt/likewise/bin/domainjoin-cli join
   domainName joinAccount joinPassword
   ```

   Example: `sudo /opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator YourPasswordHere`

Joining Active Directory

When Likewise joins a computer to a domain, it uses the hostname of the computer to create the name of the computer object in Active Directory. From the hostname, the Likewise Domain Join Tool attempts to derive a fully qualified domain name.

By default, the domain join tool creates the Linux and Unix machine accounts in the default Computers container within Active Directory.

You can, however, choose to create machine accounts in Active Directory before you join your Unix, Linux, and Mac OS X computers to the domain. When you join a computer to a domain by running the Domain Join Tool, Likewise associates the Unix or Linux host with the pre-existing machine account. If no match is found, Likewise creates a machine account.

The location of the domain join command-line utility -- `domainjoin-cli` -- is as follows:

```
/opt/likewise/bin/domainjoin-cli
```

For Linux computers, there is an optional graphical user interface version of the Likewise Domain Join Tool. It can be installed on Linux platforms that are running GTK+ version 2.6 or later. For more information, see Install the Domain Join GUI and Join a Linux Computer to Active Directory with the GUI.

Configure nsswitch.conf

Before you attempt to join an Active Directory domain, make sure the `/etc/nsswitch.conf` file contains the following line:

```
hosts: files dns
```

Computers running Solaris, in particular, may not contain this line in `nsswitch.conf` until you add it.

For information, see the man page for `nsswitch.conf`.

Configure resolv.conf

Before you attempt to join an Active Directory domain, make sure that `/etc/resolv.conf` on your Linux, Unix, or Mac client includes a DNS server that can resolve Srv records for your domain.

For information, see the man page for `resolv.conf`.

Removing a Computer from a Domain

You can remove a computer from the domain either by removing the computer's account from Active Directory Users and Computers or by running the Domain Join Tool on the Unix, Linux, or Mac OS X computer that you want to remove; see Leave a Domain.

Join Active Directory with the Command Line

When you join a domain by using the command-line utility, Likewise uses the hostname of the computer to derive a fully qualified domain name (FQDN) and then automatically sets the computer's FQDN in the `/etc/hosts` file. You can also join a domain without changing the `/etc/hosts` file; see Join Active Directory Without Changing /etc/hosts.

On Linux, Unix, and Mac OS X computers, the location of the domain join command-line utility is as follows:

```
/opt/likewise/bin/domainjoin-cli
```

Important: To run the command-line utility, you must use a **root** account. To join a computer to a domain, you must have the user name and password of an Active Directory account that has privileges to join computers to the domain and the full name of the domain that you want to join.

Before Joining a Domain

To join a domain, the computer's name server must be able to find the domain and the computer must be able to reach the domain controller. You can make sure the name server can find the domain by running this command:

`nslookup` *`domainName`*

You can verify that your computer can reach the domain controller by pinging it:

`ping` *`domainName`*

If either of these tests fails, see Check System Health Before Installing the Agent and Solve Domain-Join Problems.

Join a Linux or Unix Computer to Active Directory

- Execute the following command as root, replacing `domainName` with the FQDN of the domain that you want to join and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join domainName joinAccount
  ```

  Example: `/opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator`

Join a Mac Computer to Active Directory

- Using `sudo`, execute the following command in the Terminal, replacing `domainName` with the FQDN of the domain that you want to join and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

  ```
  sudo /opt/likewise/bin/domainjoin-cli join domainName joinAccount
  ```

  Example: `sudo /opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator`

  The terminal prompts you for two passwords: The first is for a user account on the Mac that has administrative privileges; the second is for the user account in Active Directory that you specified in the join command.

Join a Linux or Unix Computer to an Organizational Unit

- Execute the following command as root, replacing `organizationalUnitName` with the path and name of the organizational unit that you want to join, `domainName` with the FQDN of the domain, and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

  ```
  /opt/likewise/bin/domainjoin-cli join --ou organizationalUnitName domainName joinAccount
  ```

  Example: `/opt/likewise/bin/domainjoin-cli join --ou Engineering likewisedemo.com Administrator`

Options and Basic Commands

The following tables list the options and commands of the command-line interface for joining a domain.

Options

The `domainjoin-cli` command-line interface includes the following options:

Option	Description	Example
`--help`	Displays the command-line options and commands.	`domainjoin-cli --help`
`--help-internal`	Displays a list of the internal debugging commands.	`domainjoin-cli --help-internal`

`--log {.| path}`	Generates a log file or prints the log to the console.	`domainjoin-cli --log /var/log/domainjoin.log join likewisedemo.com Administrator`
		
		`domainjoin-cli --log . join likewisedemo.com Administrator`

Basic Commands

The domain join command-line interface includes the following basic commands:

Command	Description	Example
`query`	Displays the hostname, current domain, and distinguished name, which	`domainjoin-cli query`

	includes the OU to which the computer belongs. If the computer is not joined to a domain, it displays only the hostname.	
`setname` *`computerName`*	Renames the computer and modifies the `/etc/hosts` file with the name that you specify.	`domainjoin-cli setname RHEL44ID`
`fixfqdn`	Fixes a computer's fully qualified domain name.	`domainjoin-cli fixfqdn`
`join [--ou` *`organizationalUnit`*`]` *`domainName userName`*	Joins the computer to the domain that you specify by using the account that you specify. You can use the `--ou` option to join the computer to an OU	`domainjoin-cli join --ou Engineering likewisedemo.com Administrator`

	within the domain by specifying the path to the OU and the OU's name. When you use this option, you must use an account that has membership in the Domain Administrators security group. The path to the OU is top down.	

`leave [userName]`	Removes the computer from the Active Directory domain.
	
	If the `userName` is provided, the computer account is disabled in Active Directory.
		`domainjoin-cli leave`
		
		`domainjoin-cli leave smithy@likewisedemo.com`

Advanced Commands

The command-line interface includes advanced commands that you can use to preview the stages of joining or leaving a domain, find out which configurations are required for your system, view information about a module that will be changed, and enable or disable a module. The advanced commands provide a potent tool for troubleshooting issues while configuring a Linux or Unix computer to interoperate with Active Directory.

Preview the Stages of the Domain Join for Your Computer

To preview the domain, DNS name, and configuration stages that will be used to join a computer to a domain, execute the following command at the command line:

`domainjoin-cli join --preview` *`domainName`*

Example: `domainjoin-cli join --preview likewisedemo.com`

Here's an example of the results, which can vary by computer:

```
[root@rhel4d bin]# domainjoin-cli join --preview likewisedemo.com
Joining to AD Domain:   likewisedemo.com
With Computer DNS Name: rhel4d.likewisedemo.com
The following stages are currently configured to be run during
the domain join:
join            - join computer to AD
krb5            - configure krb5.conf
nsswitch        - enable/disable Likewise nsswitch module
start           - start daemons
pam             - configure pam.d/pam.conf
ssh             - configure ssh and sshd
```

Check Required Configurations

To see a full listing of the modules that apply to your operating system, including those module that will not be run, execute either the following join or leave command:

`domainjoin-cli join --advanced --preview` *`domainName`*
`domainjoin-cli leave --advanced --preview` *`domainName`*

Example: `domainjoin-cli join --advanced --preview likewisedemo.com`

The result varies by computer:

```
[root@rhel4d bin]# domainjoin-cli join --advanced --preview
likewisedemo.com
Joining to AD Domain:   likewisedemo.com
With Computer DNS Name: rhel4d.likewisedemo.com
```

```
    [F] stop           - stop daemons
    [F] hostname       - set computer hostname
    [F] firewall       - open ports to DC
    [F] keytab         - initialize kerberos keytab
[X] [N] join           - join computer to AD
[X] [N] krb5           - configure krb5.conf
[X] [N] nsswitch       - enable/disable Likewise nsswitch module
[X] [N] start          - start daemons
    [F] gdm            - fix gdm presession script for spaces in
usernames
[X] [N] pam            - configure pam.d/pam.conf
[X] [S] ssh            - configure ssh and sshd


Key to flags
[F]ully configured        - the system is already configured for
this step
[S]ufficiently configured - the system meets the minimum
configuration
                            requirements for this step
[N]ecessary               - this step must be run or manually
performed.
[X]                       - this step is enabled and will make
changes
[ ]                       - this step is disabled and will not
make changes
```

View Details about a Module

The Likewise domain join tool includes the following modules -- the components and services that the tool must configure before it can join a computer to a domain:

Module	Description
join	Joins the computer to Active Directory
leave	Deletes the machine account in Active Directory
dsplugin	Enables the Likewise directory services plugin
stop	Stops daemons so that the system can be configured
start	Starts daemons after configuration
firewall	Opens ports to the Domain Controller

hostname	sets the computer hostname
krb5	Configures `krb5.conf`
pam-mode	Switches authentication from LAM to PAM
nsswitch	Enables or disables Likewise nsswitch module
pam	Configures pam.d and pam.conf
lam-auth	Configures LAM for Active Directory authentication
ssh	Configures ssh and sshd
bash	Fixes the bash prompt for backslashes in usernames
gdm	Fixes gdm presession script for spaces in usernames

As the previous section illustrated, you can see the modules that must be configured on your computer by executing the following command:

`domainjoin-cli join --advanced --preview` *`domainName`*

You can further bore down into the details of the changes that a module will make by using either the following join or leave command:

`domainjoin-cli join --details` *`module domainName joinAccount`*
`domainjoin-cli leave --details` *`module domainName joinAccount`*

Example: `domainjoin-cli join --details nsswitch likewisedemo.com Administrator`

The result varies depending on your system's configuration:

```
[root@rhel4d bin]# domainjoin-cli join --details nsswitch
likewisedemo.com Administrator
[X] [N] nsswitch       - enable/disable Likewise nsswitch module
Key to flags
[F]ully configured        - the system is already configured for
this step
```

```
[S]ufficiently configured - the system meets the minimum
configuration
                            requirements for this step
[N]ecessary               - this step must be run or manually
performed.
[X]                       - this step is enabled and will make
changes
[ ]                       - this step is disabled and will not
make changes
Details for 'enable/disable Likewise nsswitch module':
The following steps are required and can be performed
automatically:
    * Edit nsswitch apparmor profile to allow libraries in the
/opt/likewise/lib
        and /opt/likewise/lib64 directories
    * List lwidentity module in /usr/lib/security/methods.cfg
(AIX only)
    * Add lwidentity to passwd and group/groups line
/etc/nsswitch.conf or
        /etc/netsvc.conf
If any changes are performed, then the following services must be
restarted:
    * GDM
    * XDM
    * Cron
    * Dbus
    * Nscd
```

Turn On or Turn Off Domain Join Modules

You can explicitly enable or disable a module when you join or leave a domain. Disabling a module can be useful in cases where a module has been manually configured or in cases where you must ensure that certain system files will not be modified.

Note: If you disable a necessary module and you have not manually configured it, the domain join utility will not join your computer to the domain.

To disable a module, execute either the following join or leave command:

`domainjoin-cli join --disable` *`module domainName accountName`*
`domainjoin-cli leave --disable` *`module domainName accountName`*

Example: `domainjoin-cli join --disable pam likewisedemo.com Administrator`

To enable a module, execute the following command at the command line:

```
domainjoin-cli join --enable module domainName
accountName
```

Example: `domainjoin-cli join --enable pam likewisedemo.com Administrator`

Join Active Directory Without Changing /etc/hosts

When you join a computer to a domain by using the Likewise Domain Join Tool, Likewise uses the hostname of the computer to derive a fully qualified domain name (FQDN) and then automatically sets the computer's FQDN in the `/etc/hosts` file.

To join a Linux computer to the domain without changing the `/etc/hosts` file, execute the following command at the shell prompt as **root**, replacing `domainName` with the FQDN of the domain that you want to join and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

```
 /opt/likewise/bin/domainjoin-cli join --disable
hostname  domainName joinAccount
```

Example: `/opt/likewise/bin/domainjoin-cli join --disable hostname likewisedemo.com Administrator`

If the Computer Fails to Join the Domain

Make sure the computer's FQDN is correct in `/etc/hosts`.

You can determine the fully qualified domain name of a computer running Linux, Unix, or Mac OS X by executing the following command:

```
ping -c 1 `hostname`
```

When you execute this command, the computer looks up the primary host entry for its hostname. In most cases, this means that it looks for its hostname in `/etc/hosts`, returning the first FQDN name on the same line. So, for the hostname `qaserver`, here's an example of a correct entry in `/etc/hosts`:

```
10.100.10.10 qaserver.corpqa.likewise.com qaserver
```

If, however, the entry in `/etc/hosts` incorrectly lists the hostname (or anything else) before the FQDN, the computer's FQDN becomes, using the malformed example below, `qaserver`:

```
10.100.10.10 qaserver qaserver.corpqa.likewise.com
```

If the host entry cannot be found in `/etc/hosts`, the computer looks for the results in DNS instead. This means that the computer must have a correct A record in DNS. If the DNS information is wrong and you cannot correct it, add an entry to `/etc/hosts`.

Join a Linux Computer to Active Directory with the GUI

After you install the Likewise agent, you can install the Likewise Domain Join Tool, a graphical user interface for joining a domain. The domain join tool is not included when you install the agent; you must install the utility separately. For more information, see Install the Domain Join Utility.

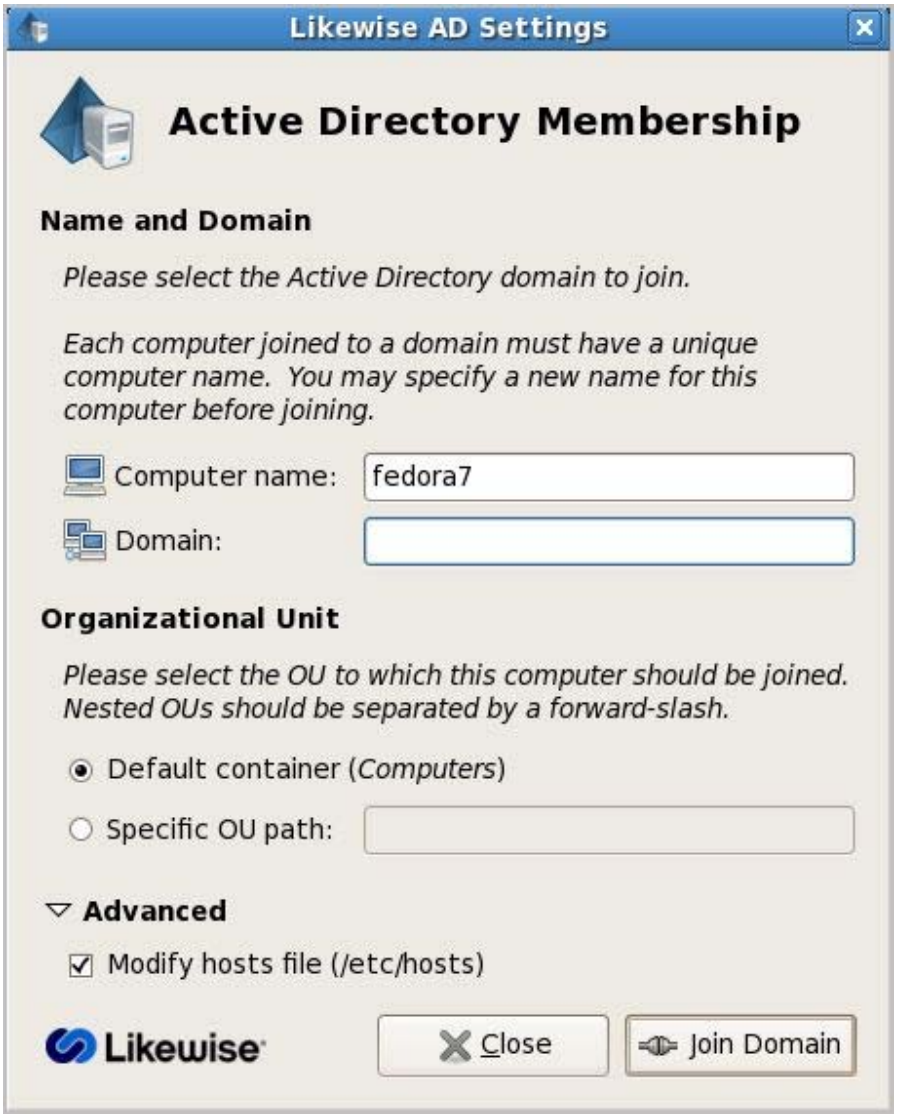
Important: To join a computer to a domain, you must have the user name and password of a user who has privileges to join computers to a domain and the full name of the domain that you want to join.

1. From the desktop with **root** privileges, double-click the Likewise Domain Join Tool, or at the shell prompt of a Linux computer, type the following command:

   ```
   /opt/likewise/bin/domainjoin-gui
   ```

2. On the Likewise AD Settings panel, in the **Domain** box, enter the Fully Qualified Domain Name (FQDN) of the Active Directory domain.

   Note: The domain join tool automatically sets the computer's FQDN by modifying the `/etc/hosts` file. For example, If your computer's name is `qaserver` and the domain is `corpqa.likewise.com`, the domain join tool adds the following entry to the `/etc/hosts` file: `qaserver.corpqa.likewise.com`. To manually set the computer's FQDN, see Join Active Directory Without Changing /etc/hosts.



4. Under **Organizational Unit**, you can join the computer to an OU in the domain by selecting **OU Path** and then typing a path in the **OU Path** box. The OU path is from the top of the Active Directory domain down to the OU that you want.

   Or, to join the computer to the Computers container, select **Default to container (Computers)**.

5. Click **Join Domain**.

6. Enter the user name and password of an Active Directory user with the right to join a machine to the Active Directory domain, and then

click **OK**.

Note: If you do not use an Active Directory Domain Administrator account, you might not have sufficient privileges to change an existing machine object in Active Directory.

Use Likewise with a Single OU

If you have only write privileges for an organizational unit in Active Directory, you can still use Likewise. You should enable an organizational unit (OU) for Likewise only when you want to manage your Linux, Unix, and Mac OS X computers within a single OU and you do not have Domain Administrator or Enterprise Administrator privileges, but you have been given rights to create objects in an OU. You can use the write privileges that you have been given for an OU to join Linux and Unix computers to that OU.

There are additional limitations to this approach:

- You must join the computer to a specific OU, and you must know the path to that OU.
- You cannot use Likewise in schema mode unless you have Enterprise Administrator privileges, which are required to upgrade the schema.

Join a Linux Computer to an Organizational Unit

To join a computer to a domain, you must have the user name and password of an account that has privileges to join computers to the domain and the full name of the domain that you want to join. The OU path is from the top OU down to the OU that you want.

Execute the following command, replacing `organizationalUnitName` with the path and name of the organizational unit that you want to join, `domainName` with the FQDN of the domain, and `joinAccount` with the user name of an account that has privileges to join computers to the domain:

```
/opt/likewise/bin/domainjoin-cli join --ou
organizationalUnitName domainName joinAccount
```

Example: `/opt/likewise/bin/domainjoin-cli join --ou Engineering likewisedemo.com Administrator`

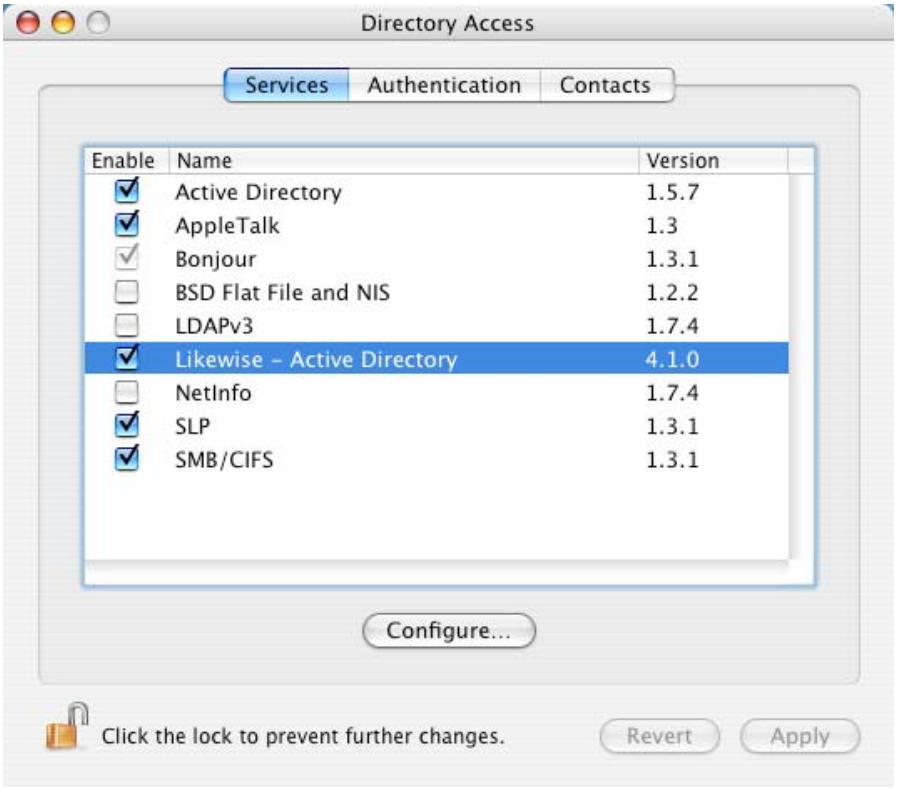
Join a Mac Computer to Active Directory with the GUI

To join a computer running Mac OS X 10.4 or later to an Active Directory domain, you must have administrative privileges on the Mac and privileges on the Active Directory domain that allow you to join a computer.

1. In Finder, click **Applications**. In the list of applications, double-click **Utilities**, and then double-click **Directory Access** in OS X 10.4 or **Directory Utility** in OS X 10.5.

2. On the **Services** tab, click the lock and enter an administrator name and password to unlock it.

3. In the list click **Likewise - Active Directory**, make sure the **Enable** check box for **Likewise - Active Directory** is selected, and then click **Configure** in OS X 10.4 or double-click **Likewise – Active Directory** in OS X 10.5.



4. Enter a name and password of a local machine account with administrative privileges.

5. On the menu bar at the top of the screen, click the **Likewise Domain Join** menu, and then click **Join or Leave Domain**.

6. In the **Computer name** box, type the local hostname of the Mac without the `.local` extension. Because of a limitation with Active Directory, the local hostname cannot be more than 15 characters. Also: `localhost` is not a valid name.

   Tip: To find the local hostname of a Mac, on the **Apple** menu , click **System Preferences**, and then click **Sharing**. Under the **Computer Name** box, click **Edit**. Your Mac's local hostname is displayed.

7. In the **Domain to join** box, type the fully qualified domain name of the Active Directory domain that you want to join.

8. Under **Organizational Unit**, you can join the computer to an OU in the domain by selecting **OU Path** and then typing a path in the **OU Path** box.

   Note: To join the computer to an OU, you must be a member of the Domain Administrator security group.

   Or, to join the computer to the Computers container, select **Default to "Computers" container**.

9. Click **Join**.

10. After you are joined to the domain, you can set the display login window preference on the Mac: On the **Apple** menu , click **System Preferences**, and then under **System**, click **Accounts**.

11. Click the lock and enter an administrator name and password to unlock it.

12. Click **Login Options**, and then under **Display login window as**, select **Name and password.**

Logging On with AD Credentials

After the Likewise agent has been installed and the Linux or Unix computer has been joined to a domain, you can log on interactively by using your Active Directory credentials. For example, you can log on by using the form `DOMAIN\username`.

3. On a Linux computer, log out of the current session.

4. Log on the system console by using an Active Directory user account in the form of `DOMAIN\username`, where `DOMAIN` is the Active Directory short name.

Note: When you log on from the command line, you must use a slash to escape the slash character, making the logon form `DOMAIN\\username`.

Example with ssh: `ssh likewisedemo.com\\hoenstiv@localhost`

Logon Options

Likewise provides the following logon options:

- Full domain credentials -- example: `likewisedemo.com\hoenstiv`
- Single domain user name -- example: `likewisedemo\hoenstiv`
- Alias -- example: `stiv`

  (For Likewise Enterprise, see Set a User Alias and Set a Group Alias. For Likewise Open, see Create a Local Name Mapping File to Set an Alias.)

- Cached credentials
- To use UPN names, you must raise your Active Directory forest functional level to Windows Server 2003, but note that raising the forest functional level to Windows Server 2003 will exclude Windows 2000 domain controllers from the domain. For more information, see About Schema Mode and Non-Schema Mode.

Important: When you log on from the command line, you must use a slash to escape the slash character, making the logon form `DOMAIN\\username`.

Solve Logon Problems

To troubleshoot problems logging on a Linux computer with Active Directory credentials after you joined the computer to a domain, perform the following series of diagnostic tests sequentially with a root account. The tests can also be used to troubleshoot logon problems on a Unix or Mac OS X computer; however, the syntax of the commands on Unix and Mac might be slightly different.

Make Sure You Are Joined to the Domain

Execute the following command:

```
/opt/likewise/bin/domainjoin-cli query
```

If you are not joined, see Join Active Directory with the Command Line.

Check Whether You Are Using a Valid Logon Form

When troubleshooting a logon problem, use your full domain credentials: `DOMAIN\username`. Example: `likewisedemo.com\hoenstiv`.

When logging on from the command line, you must escape the slash character with a slash character, making the logon form `DOMAIN\\username`. Example: `likewisedemo.com\\hoenstiv`.

To view a list of logon options, see About Logging On.

Clear the Cache

You might need to clear the cache to ensure that client computer recognizes the user's ID. See Clear the Authentication Cache.

Check the Status of the Likewise Authentication Daemon

Check the status of the authentication daemon on a Unix or Linux computer running the Likewise Agent by executing the following command at the shell prompt as the root user:

```
/sbin/service lsassd status
```

If	Do This
The result looks like this: `likewise-winbindd is stopped`	Restart the daemon.
The result looks like this:	Proceed to the next test.

`likewise-winbindd (pid 2572 2392 2384) is running...`	

Check Communication between the Likewise Daemon and AD

Verify that the Likewise daemon can exchange data with AD by executing this command:

`/opt/likewise/bin/lw-get-dc-name` *`FullDomainName`*

Example: `/opt/likewise/bin/lw-get-dc-name likewisedemo.com`

If	Do This
The result does not show the name and IP address of your domain controller	1. Make sure the domain controller is online and operational. 2. Check network connectivity between the client and the domain controller. 3. Join the domain again. 4. View log files.
The result shows the correct domain controller name and IP address	Proceed to the next test.

Verify that Likewise Can Find a User in AD

Verify that the Likewise agent can find your user by executing the following command, substituting the name of a valid AD domain and user for *`ADuserName`*:

`/opt/likewise/bin/lw-find-user-by-name` *`domainName`*`\\`*`ADuserName`*

Example: `/opt/likewise/bin/lw-find-user-by-name likewisedemo\\hab`

If	Do This
The command fails to find the user	1. Check whether the computer is joined to the domain by executing the following command as root: `domainjoin-cli query` Displays the hostname, current domain, and distinguished name, which includes the OU to which the computer belongs. Make sure the OU is correct. If the computer is not joined to a domain, it displays only the hostname. 2. Check Active Directory to make sure the user has an account. If you are using Likewise Enterprise, also ensure that the user is associated with the correct cell. 3. Check whether the same user is in the `/etc/passwd` file. If necessary, migrate the user.
The user is found	Proceed to the next test.

Switch User to Check PAM

Verify that a user's password can be validated through PAM by using the switch user service. Either switch from a non-root user to a domain user

or from root to a domain user. If you switch from root to a domain user, run the command below twice so that you are prompted for the domain user's password:

```
su DOMAIN\\username
```

Example: `su likewisedemo\\hoenstiv`

If	Do This

The switch user command fails to validate the user	Generate a PAM debug log.
	
	Also, check the following log files for error messages:
	
	`/var/log/messages`
	
	`/var/log/secure`

Test SSH

Check whether you can log on with SSH by executing the following command:

```
ssh DOMAIN\\username@localhost
```

```
ssh likewisedemo.com\\hoenstiv@localhost
```

Troubleshooting Domain Join Problems

Top 10 Reasons Domain Join Fails

Here are the top 10 reasons that an attempt to join a domain fails:

1. Root was not used to run the domain-join command (or to run the domain-join graphical user interface).
2. The user name or password of the account used to join the domain is incorrect.
3. The name of the domain is mistyped.
4. The name of the OU is mistyped.
5. The local hostname is invalid.
6. The domain controller is unreachable from the client because of a firewall or because the NTP service is not running on the domain controller. (See Make Sure Outbound Ports Are Open and Diagnose NTP on Port 123.)
7. The client is running RHEL 2.1 and has an old version of SSH.
8. On SUSE, GDM (dbus) must be restarted. This daemon cannot be automatically restarted if the user logged on with the graphical user interface.
9. On HP-UX and Solaris, `dtlogin` must be restarted. This daemon cannot be automatically restarted if the user logged on with the HP-UX or Solaris graphical user interface. To restart `dtlogin`, run the following command:

   ```
   /sbin/init.d/dtlogin.rc start
   ```

10. SELinux is turned on -- which is especially likely on Fedora and some versions of Red Hat. SELinux must be turned off before the computer can be joined to the domain.

    To turn off SELinux, edit the following file, which is the primary configuration file for enabling and disabling SELinux:

    ```
    /etc/sysconfig/selinux
    ```

For instructions on how to edit the file to disable SELinux, see the SELinux man page.

For more information, see Solve Domain-Join Problems.

Generate a Domain-Join Log

To help troubleshoot problems with joining a domain, you can use the command-line utility's `log` option with the `join` command. The `log` option captures information about the attempt to join the domain on the screen or in a file.

- To display the information in the terminal, execute the following command; the dot after `--log` specifies that the information is shown in the console:

  ```
  domainjoin-cli --log . join domainName userName
  ```

- To save the information in a log file, execute the following command:

  ```
  domainjoin-cli --log path join domainName userName
  ```

  Example:

  ```
  domainjoin-cli --log /var/log/domainjoin.log join
  likewisedemo.com Administrator
  ```

Solve Domain-Join Problems

To troubleshoot problems with joining a Linux computer to a domain, perform the following series of diagnostic tests sequentially on the Linux computer with a root account. The tests can also be used to troubleshoot domain-join problems on a Unix or Mac OS X computer; however, the syntax of the commands on Unix and Mac might be slightly different.

The procedures in this topic assume that you have already checked whether the problem falls under the Top 10 Reasons Domain Join Fails. It is also recommended that you generate a domain-join log.

Verify that the Name Server Can Find the Domain

Run the following command as root:

```
nslookup ADrootDomain.com
```

Make Sure the Client Can Reach the Domain Controller

You can verify that your computer can reach the domain controller by pinging it:

```
ping domainName
```

Verify that Outbound Ports Are Open

Run the following command as root:

```
domainjoin-cli join --details firewall
likewisedemo.com
```

The results of the command show whether you must open any ports.

For a list of ports that must be open on the client, see Make Sure Outbound Ports Are Open.

Check DNS Connectivity

The computer might be using the wrong DNS server or none at all. Make sure the nameserver entry in `/etc/resolv.conf` contains the IP address of a DNS server that can resolve the name of the domain you are trying to join. This is likely to be the IP address of one of your domain controllers.

Make Sure nsswitch.conf Is Configured to Check DNS for Host Names

The `/etc/nsswitch.conf` file must contains the following line. (On AIX, the file is `/etc/netsvc.conf`.)

```
hosts: files dns
```

Computers running Solaris, in particular, may not contain this line in `nsswitch.conf` until you add it.

Ensure that DNS Queries Are Not Using the Wrong Network Interface Card

If the computer is multi-homed, the DNS queries might be going out the wrong network interface card. Temporarily disable all the NICs except for the card on the same subnet as your domain controller or DNS server and then test DNS lookups to the AD domain. If this works, re-enable all the NICs and edit the local or network routing tables so that the AD domain controllers are accessible from the host.

Determine Whether the DNS Server Is Configured to Return SRV Records

Your DNS server must be set to return SRV records so the domain controller can be located. It is common for non-Windows (bind) DNS servers to not be configured to return SRV records.

Diagnose by executing the following command:

```
nslookup -q=srv _ldap._tcp.ADdomainToJoin.com
```

Make Sure that the Global Catalog Is Accessible

The global catalog for Active Directory must be accessible. A global catalog in a different zone might not show up in DNS. Diagnose by executing the following command:

```
nslookup -q=srv _ldap._tcp.gc._msdcs.ADrootDomain.com
```

From the list of IP addresses in the results, choose one or more addresses and test whether they are accessible on Port 3268 by using telnet.

```
telnet 192.168.100.20 3268
```

```
Trying 192.168.100.20...
Connected to sales-dc.likewisedemo.com (192.168.100.20).
Escape character is '^]'.
```

Press the **Enter** key to close the connection:

```
Connection closed by foreign host.
```

Verify that the Client Can Connect to the Domain on Port 123

The following test checks whether the client can connect to the domain controller on Port 123 and whether the Network Time Protocol (NTP) service is running on the domain controller. For the client to join the domain, NTP -- the Windows time service -- must be running on the domain controller.

On a Linux computer, run the following command as root:

`ntpdate -d -u` *`DC_hostname`*

Example: `ntpdate -d -u sales-dc`

For more information, see Diagnose NTP on Port 123.

In addition, check the logs on the domain controller for errors from source `w32tm`, the Windows time service.

Files Modified During a Domain Join

When Likewise joins a computer to a domain, it modifies some system files. The files that are modified depend on the platform, the distribution, and the system's configuration. The following files might be modified.

Note: Not all of these files are present on all computers.

- /etc/nsswitch.conf
- /etc/pam.conf or /etc/pam.d/*
- /etc/ssh/{ssh_config,sshd_config} (or wherever sshd configuration is located)
- /etc/hosts (To join a domain without modifying /etc/hosts, see Join Active Directory Without Changing /etc/hosts.)
- /etc/apparmor.d/abstractions/nameservice
- /etc/X11/gdm/PreSession/Default
- /etc/vmware/firewall/services.xml
- /usr/lib/security/methods.cfg
- /etc/security/user

- /etc/security/login.cfg
- /etc/netsvc.conf
- /etc/krb5.conf
- /etc/krb5/krb5.conf
- /etc/rc.config.d/netconf
- /etc/nodename
- /etc/{hostname,HOSTNAME,hostname.*}
- /etc/sysconfig/network/config
- /etc/sysconfig/network/dhcp
- /etc/sysconfig/network/ifcfg-*
- /etc/sysconfig/network-scripts/ifcfg-*

Managing Joined Computers

Set the Home Directory and Shell for Domain Users

When you install Likewise only on a Linux, Unix, or Mac computer and not on Active Directory, you cannot associate a Likewise cell with an organizational unit, and thus you have no way to define a home directory or shell in Active Directory for users who log on the computer with their domain credentials.

To set the home directory and shell for a Linux, Unix, or Mac computer that is using Likewise Open or Likewise Enterprise without cell, edit the following configuration file:

```
/etc/likewise/lsassd.conf
```

Modify the following lines to set the shell and home directory that you want:

```
login-shell-template =
homedir-template =
```

Examples:

```
login-shell-template = /bin/bash
homedir-template = /home/local/%D/%U
```

When you set the default home directory, you must use the default user name variable (`%U`). You may specify the default domain name by using the domain name variable (`%D`) but, unlike the user name variable, it is not required.

All the users who log on the computer by using their Active Directory domain credentials will have the shell and home directory that you set.

Note: `/bin/bash` might not be available on all systems.

Important: On Solaris, you cannot create a local home directory in `/home`, because `/home` is used by autofs, Sun's automatic mounting service. The standard on Solaris is to create local home directories in `/export/home`.

If you set the shell and home directory both in Active Directory and in `lsassd.conf`, the settings in Active Directory take precedence.

Change the Replacement Character for Spaces

When you install the Likewise agent on a Linux, Unix, or Mac computer but do not install Likewise Enterprise on Active Directory, you cannot configure local Likewise settings with group policies. Instead, you must edit the local Likewise configuration file.

To replace the spaces in Active Directory user and group names with a character that you choose, edit the following file:

```
/etc/likewise/lsassd.conf
```

In the file, modify the following line to set the replacement character that you want:

```
separator-character =
```

Example:

```
separator-character = ,
```

The default replacement character is set to `^`. So, by default, the Active Directory group `DOMAIN\Domain Users` appears as `DOMAIN\domain^users` on target Linux and Unix computers.

The following characters cannot be used as the separator:

- whitespace
- alphanumeric characters
- @
- /
- \
- #

Note: The Likewise authentication daemon renders all names of Active Directory users and groups lowercase.

Rename a Joined Computer

To rename a computer that has been joined to Active Directory, you must first leave the domain. You can then rename the computer by using

the domain join command-line interface. After you rename the computer, you must rejoin it to the domain. Renaming a joined computer requires the user name and password of a user with privileges to join a computer to a domain.

Important: Do not change the name of a Linux, Unix, or Mac computer by using the `hostname` command because some distributions do not permanently apply the changes.

Rename a Computer by Using the Command-Line Tool

The following procedure removes a Unix or Linux computer from the domain, renames the computer, and then rejoins it to the domain.

1. With root privileges, at the shell prompt of a Unix computer, execute the following command:

   ```
   /opt/likewise/bin/domainjoin-cli leave
   ```

2. To rename the computer in `/etc/hosts`, execute the following command, replacing *`computerName`* with the new name of the computer:

   ```
   /opt/likewise/bin/domainjoin-cli setname computerName
   ```

   Example: `/opt/likewise/bin/domainjoin-cli setname RHEL44ID`

3. To rejoin the renamed computer to the domain, execute the following command at the shell prompt, replacing *DomainName* with the name of the domain that you want to join and *UserName* with the user name of a user who has privileges to join a domain:

   ```
   /opt/likewise/bin/domainjoin-cli join DomainName UserName
   ```

   Example: `/opt/likewise/bin/domainjoin-cli join likewisedemo.com Administrator`

   It may take a few moments before the computer is joined to the domain.

Rename a Computer by Using the Domain Join Tool

To execute the following procedure, the Likewise Domain Join Tool, a graphical user interface for joining a domain, must be installed on your computer. For more information, see Install the Likewise Domain Join Tool.

1. From the desktop with root privileges, double-click the Likewise Domain Join Tool, or at the shell prompt of a Linux computer, type the following command:

   ```
   /opt/likewise/bin/domainjoin-gui
   ```

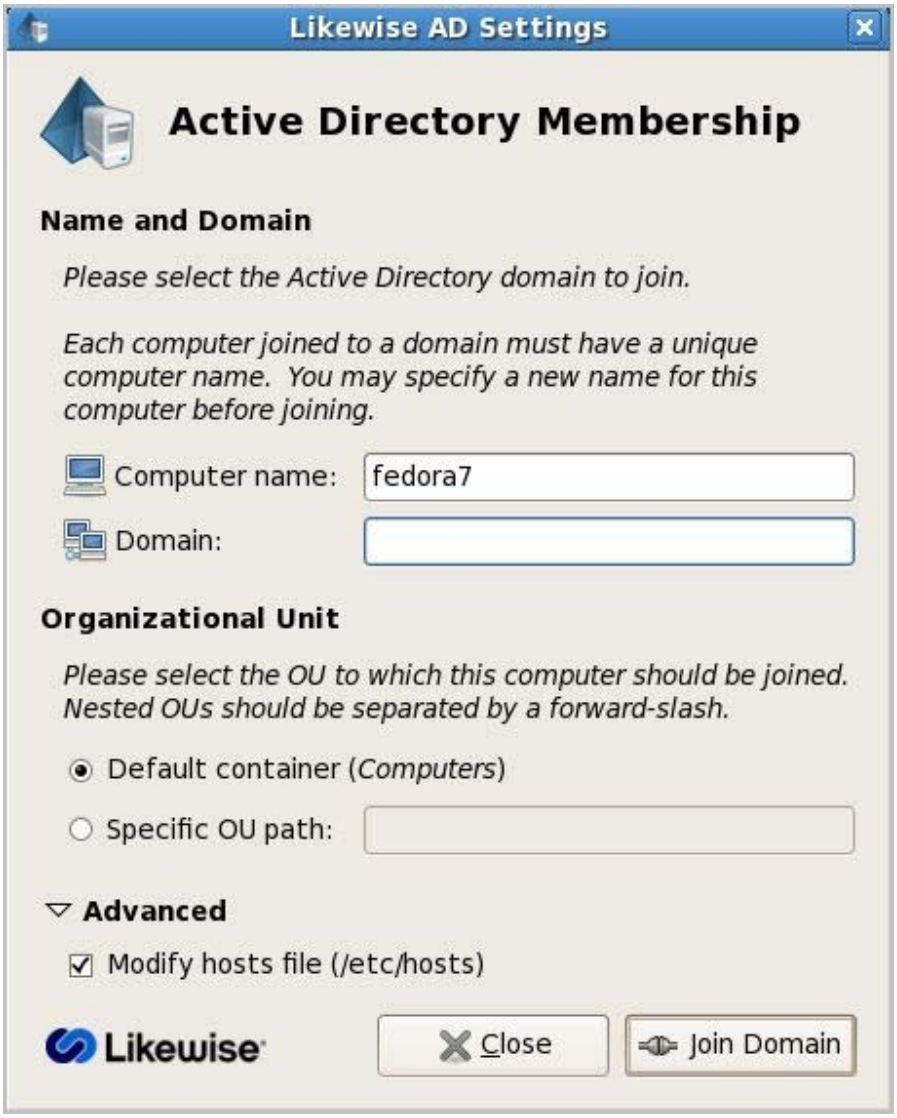
2. Click **Leave**, and then click **OK**.

3. Start the Domain Join Tool again by double-clicking the Likewise Domain Join Tool on the desktop, or by typing the following command at the shell prompt of a Linux computer:

   ```
   /opt/likewise/bin/domainjoin-gui
   ```

4. Click **Next**.

5. In the **Computer Name** box, rename the computer by typing a new name.



6. In the **Domain to join** box, enter the Fully Qualified Domain Name (FQDN) of the Active Directory domain.

7. Under **Organizational Unit**, you can join the computer to an OU in the domain by selecting **OU Path** and then typing a path in the **OU Path** box.

   Or, to join the computer to the Computers container, select **Default to "Computers" container**.

8. Click **Next**.

9. Enter the user name and password of an Active Directory user with authority to join a machine to the Active Directory domain, and then click **OK**.

The computer's name in `/etc/hosts` has been changed to the name that you specified and the computer has been joined to the Active Directory domain with the new name.

Troubleshooting the Agent

Check the Status of the Authentication Daemon

On Linux and Unix

You can check the status of the authentication daemon on a Unix or Linux computer running the Likewise agent by executing the following command at the shell prompt as the root user:

```
/sbin/service lsassd status
```

(On HP-UX, the command is `/sbin/init.d/lsassd status`.)

If the authentication daemon is running, the result should look like this:

```
lsassd (pid 25753) is running...
```

If the service is not running, execute the following command:

```
/sbin/service lsassd start
```

(On HP-UX, the command is `/sbin/init.d/lsassd start`.)

On Mac OS X

On a Mac OS X computer, you cannot use the `status` command, but you can monitor the daemon by using Activity Monitor:

1. In Finder, click **Applications**, click **Utilities**, and then click **Activity Monitor**.
2. In the list under **Process Name**, make sure `lsassd` appears. If the process does not appear in the list, you might need to start it.
3. To monitor the status of the process, in the list under **Process Name**, click the process, and then click **Inspect**.

Check the Version and Build Number

On Linux distributions that support RPM -- for example, Red Hat Enterprise Linux, Fedora, SUSE Linux Enterprise, OpenSUSE, and CentOS -- you can determine the version and build number of the agent (5.0.0.xxxx in the examples below) by executing the following command at the shell prompt:

```
rpm -qa | grep likewise
```

The result shows the build version after the version number:

```
likewise-sqlite-5.0.0-1.26353.3513
likewise-libxml2-5.0.0-1.26353.3513
likewise-netlogon-5.0.0-1.26353.3513
likewise-openldap-5.0.0-1.26353.3513
likewise-pstore-5.0.0-1.26353.3513
likewise-passwd-5.0.0-1.26353.3513
likewise-domainjoin-5.0.0-1.26353.3513
likewise-lsass-5.0.0-1.26353.3513
likewise-krb5-5.0.0-1.26353.3513
likewise-base-5.0.0-1.26353.3513
likewise-rpc-5.0.0-1.26353.3513
```

On Unix computers and Linux distributions that do not support RPM, the command to check the build number varies by platform:

Platform	Command
Debian and Ubuntu	`dpkg –S /opt/likewise/`
Solaris	`pkginfo | grep -i likewise`
AIX	`lslpp –l | grep likewise`
HP-UX	`swlist | grep -i likewise`

Clear the Authentication Cache

There are certain conditions under which you might need to clear the cache so that a user's ID is recognized on a target computer.

By default, the user's ID is cached for 900 seconds (15 minutes). If you change a user's UID for a Likewise cell, during the 900 seconds after you change the UID you must clear the cache on a target computer in the cell before the user can log on.

For example, if you set the Minimum UID-GID Value group policy to 99 for a OU with an associated Likewise cell that contains a user with a UID lower than 99, you must change the user's UID so that it is 99 or higher and then you must clear the cache before the user can log on during the 15-minute period after the change.

If you do not clear the cache after changing the UID, the computer will find the old UID until after the cache expires.

There are three Likewise group policies that can affect the cache time:

- The Winbind Cache Expiration Time, which stores UID-SID mappings, user/group enumeration lists, `getgrnam()` and `getpwnam()`, and so forth. Its default expiration time is 900 seconds (15 minutes).
- The ID Mapping Cache Expiration Time, which caches the mapping tables for SIDs, UIDs, and GIDs. Its default is 1 hour.
- The ID Mapping Negative Cache Expiration Time, which stores failed SID-UID-GID lookups to prevent an overload of resolution requests. Its default is 5 minutes.

Tip: While you are deploying and testing Likewise, set the cache expiration times of the Winbind Cache, the ID Mapping Cache, and the ID Mapping Negative Cache to a short period of time, such as 1 minute.

Clear the Cache on a Linux Computer

1. Stop the Likewise authentication daemon by executing the following command as root:

   ```
   /sbin/service lsassd stop
   ```

2. Clear the AD-provider cache and the local-provider cache by removing the following two files:

   ```
   rm -f /var/lib/likewise/db/adcache.db
   rm -f /var/lib/likewise/db/lwi_lsass.db
   ```

   Important: Do not delete the other `.db` files in the `/var/lib/likewise/db` directory.

3. Start the Likewise authentication daemon:

   ```
   /sbin/service lsassd start
   ```

Clear the Cache on a Mac

1. In Terminal, stop the Likewise authentication daemon by executing the following command as sudo:

   ```
   sudo launchctl stop com.likewisesoftware.lsassd
   ```

2. Clear the AD-provider cache and the local-provider cache by removing the following two files:

   ```
   sudo rm -f /var/lib/likewise/db/adcache.db
   sudo rm -f /var/lib/likewise/db/lwi_lsass.db
   ```

   Important: Do not delete the other `.db` files in the `/var/lib/likewise/db` directory.

3. Restart the Likewise authentication daemon:

   ```
   sudo launchctl start com.likewisesoftware.lsassd
   ```

Determine a Computer's FQDN

You can determine the fully qualified domain name of a computer running Linux, Unix, or Mac OS X by executing the following command at the shell prompt:

```
ping -c 1 `hostname`
```

On HP-UX

The command is different on HP-UX:

```
ping `hostname` -n 1
```

On Solaris

On Sun Solaris, you can find the FQDN by executing the following command, but note that the computer's configuration can affect the results:

```
FQDN=`/usr/lib/mail/sh/check-hostname|cut -d" " -
f7`;echo $FQDN
```

Diagnose NTP on Port 123

When you use the Likewise domain join utility to join a Linux or Unix client to a domain, the utility might be unable to contact the domain controller on Port 123 with UDP. The Likewise agent requires that Port 123 be open on the client so that it can receive NTP data from the domain controller. In addition, the time service must be running on the domain controller.

You can diagnose NTP connectivity by executing the following command as root at the shell prompt of your Linux machine:

`ntpdate -d -u DC_hostname`

Example: `ntpdate -d -u sales-dc`

If all is well, the result should look like this:

```
[root@rhel44id ~]# ntpdate -d -u sales-dc
 2 May 14:19:20 ntpdate[20232]: ntpdate 4.2.0a@1.1190-r Thu Apr
20 11:28:37 EDT 2006 (1)
Looking for host sales-dc and service ntp
host found : sales-dc.likewisedemo.com
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
receive(192.168.100.20)
transmit(192.168.100.20)
server 192.168.100.20, port 123
stratum 1, precision -6, leap 00, trust 000
refid [LOCL], delay 0.04173, dispersion 0.00182
transmitted 4, in filter 4
reference time:    cbc5d3b8.b7439581  Fri, May  2 2008
10:54:00.715
originate timestamp: cbc603d8.df333333  Fri, May  2 2008
14:19:20.871
transmit timestamp:  cbc603d8.dda43782  Fri, May  2 2008
14:19:20.865
filter delay:  0.04207  0.04173  0.04335  0.04178
         0.00000  0.00000  0.00000  0.00000
filter offset: 0.009522 0.008734 0.007347 0.005818
         0.000000 0.000000 0.000000 0.000000
delay 0.04173, dispersion 0.00182
offset 0.008734
 2 May 14:19:20 ntpdate[20232]: adjust time server 192.168.100.20
offset 0.008734 sec
```

Output When There Is No NTP Service

If the domain controller is not running NTP on Port 123, the command returns a response such as `no server suitable for synchronization found`, as in the following output:

```
 5 May 16:00:41 ntpdate[8557]: ntpdate 4.2.0a@1.1190-r Thu Apr 20
11:28:37 EDT 2006 (1)
Looking for host RHEL44ID and service ntp
host found : rhel44id.likewisedemo.com
transmit(127.0.0.1)
transmit(127.0.0.1)
transmit(127.0.0.1)
```

```
transmit(127.0.0.1)
transmit(127.0.0.1)
127.0.0.1: Server dropped: no data
server 127.0.0.1, port 123
stratum 0, precision 0, leap 00, trust 000
refid [127.0.0.1], delay 0.00000, dispersion 64.00000
transmitted 4, in filter 4
reference time:    00000000.00000000  Wed, Feb  6 2036
22:28:16.000
originate timestamp: 00000000.00000000  Wed, Feb  6 2036
22:28:16.000
transmit timestamp:  cbca101c.914a2b9d  Mon, May  5 2008
16:00:44.567
filter delay:  0.00000  0.00000  0.00000  0.00000
         0.00000  0.00000  0.00000  0.00000
filter offset: 0.000000 0.000000 0.000000 0.000000
         0.000000 0.000000 0.000000 0.000000
delay 0.00000, dispersion 64.00000
offset 0.000000
 5 May 16:00:45 ntpdate[8557]: no server suitable for
synchronization found
```

Find a User or a Group

On a Unix or Linux computer that is joined to the Active Directory domain, you can check a domain user's or group's information by either name or ID. These commands can verify that the client can locate the user or group in Active Directory.

Find a User by Name

Execute the following command, replacing *domain**username* with the full domain user name or the single domain user name of the user that you want to check:

/opt/likewise/bin/lw-find-user-by-name *domain**username*

Example: `/opt/likewise/bin/lw-find-user-by-name likewisedemo\\hoenstiv`

You can optionally specify the level of detail of information that is returned. Example:

```
/opt/likewise/bin/lw-find-user-by-name --level 2
likewisedemo\\hab

User info (Level-2):
====================
Name:                       LIKEWISEDEMO\hab
UPN:                        hab@likewisedemo.com
Uid:                        593495196
Gid:                        593494529
Gecos:                      Jurgen Habermas
```

```
Shell:                       /bin/sh
Home dir:                    /home/LIKEWISEDEMO/hab
LMHash length:               0
NTHash length:               0
Local User:                  NO
Account disabled:            FALSE
Account Expired:             FALSE
Account Locked:              FALSE
Password never expires:      TRUE
Password Expired:            FALSE
Prompt for password change: YES
```

For more information, execute the following command:

```
/opt/likewise/bin/lw-find-user-by-name --help
```

Find a User by UID

To find a user by UID, execute the following command, replacing *UID* with the user's ID:

```
/opt/likewise/bin/lw-find-user-by-id UID
```

Example:

```
/opt/likewise/bin/lw-find-user-by-id 593495196
```

Find a Group by Name

/opt/likewise/bin/lw-find-group-by-name *domain\\username*

Example:

```
/opt/likewise/bin/lw-find-group-by-name
likewisedemo.com\\dnsadmins
```

Find the Likewise Daemons on a Mac

To locate the Likewise processes on a Mac OS X computer, execute the following command in Terminal:

```
sudo launchctl list | grep likewise
```

There are typically four Likewise daemons running on a Mac:

```
com.likewisesoftware.npcmuxd
com.likewisesoftware.netlogond
com.likewisesoftware.dcerpcd
```

```
com.likewisesoftware.lsassd
```

With the Likewise Enterprise agent, the group policy daemon is also running.

Fix the Shell and Home Directory Paths

Symptom: A `local` directory is in the home directory path and the home directory path does not match the path specified in Active Directory or in `/etc/password`.

Example: `/home/local/DOMAIN/USER` instead of `/home/DOMAIN/USER`

The shell might also be different from what is set in Active Directory -- for example, `/bin/ksh` instead of `/bin/bash`.

Problem: The computer is not in a Likewise cell in Active Directory.

Solution: Make sure the computer is in a Likewise cell. For more information, see Associate a Cell with an OU or a Domain, or create a default cell.

A default cell handles mapping for computers that are not in an OU with an associated cell. The default cell can contain the mapping information for all your Linux and Unix computers. For instance, a Linux or Unix computer can be a member of an OU that does not have a cell associated with it. In such a case, the home directory and shell settings are obtained from the nearest parent cell, or the default cell. If there is no parent cell and no default cell, the computer will not receive its shell and home directory paths from Active Directory.

Generate a Domain-Join Log

To help troubleshoot problems with joining a domain, you can use the command-line utility's `log` option with the `join` command. The `log` option captures information about the attempt to join the domain on the screen or in a file.

- To display the information in the terminal, execute the following command; the dot after `--log` specifies that the information is shown in the console:

```
domainjoin-cli --log . join domainName userName
```

- To save the information in a log file, execute the following command:

  ```
  domainjoin-cli --log path join domainName userName
  ```

  Example:

  ```
  domainjoin-cli --log /var/log/domainjoin.log join
  likewisedemo.com Administrator
  ```

Generate a Network Trace

Execute the following command in a separate session to dump network traffic as the root user and interrupt the trace with CTRL-C:

```
tcpdump -s 0 -i eth0 -w trace.pcap
```

The result should look something like this:

```
tcpdump: listening on eth0
28 packets received by filter
0 packets dropped by kernel
```

Generate a PAM Debug Log

You can generate a debug log for PAM on a Unix or Linux computer running the Likewise Agent. *PAM* stands for pluggable authentication modules.

The location of the configuration and log files in the following procedure can vary by platform.

1. Log on as root user.
2. Edit `/etc/security/pam_lwidentity.conf` so that the following lines are set to `yes` and are not commented out with either a number sign or a semicolon:

   ```
   debug = yes
   debug_state = yes
   ```

   The data is sent to syslog.

3. Edit `/etc/syslog.conf` to add the following line:

   ```
   *.*                                /var/log/all.log
   ```

   Important: You must use a ***TAB*** to delimit `*.*` from `/var/log/all.log`.

4. Restart syslog by executing the following command at the shell prompt:

   ```
   service syslog restart
   ```

5. At the command line, execute the following command and note the time stamp:

   ```
   date
   ```

6. Perform a login test for both a local account and an Active Directory account.

7. At the command line, execute the following command again and note the new time:

   ```
   date
   ```

8. Comment out the changes that you made to `/etc/security/pam_lwidentity.conf` and `/etc/syslog.conf` in the steps above.

9. Remove all activity from `all.log` that is not between the time stamps that you noted.

Generate an Authentication Agent Debug Log

By editing `/etc/likewise/lsassd.conf`, you can specify the level of logging for the Likewise authentication daemon's interaction with PAM. The following log levels are available: `error`, `warning`, `info`, `verbose`. The default is `error`.

The log messages are processed by syslog. Although the path and file name of the log varies by platform, they typically appear in a subdirectory of `/var/log`.

1. Log in as root user.

2. Modify `/etc/likewise/lsassd.conf` to include the following line:

   ```
   log-level = verbose
   ```

3. Restart the Likewise authentication daemon by executing the following command from the command line (On HP-UX, the path to the command is `/sbin/init.d`):

   ```
   /sbin/service lsassd restart
   ```

   On a Mac:

   ```
   sudo launchctl stop com.likewisesoftware.lsassd
   sudo launchctl start com.likewisesoftware.lsassd
   ```

4. After you finish troubleshooting, set the `log-level` back to `error` and restart the daemon again.

   Important: Leaving the log level at `info` or `verbose` might result in disk space issues over time.

Increase Max Username Length on AIX

By default, AIX is not configured to support long user and group names, which might present a conflict when you try to log on with a long Active Directory username. To increase the max username length on AIX 5.3, use the following syntax:

```
# chdev -l sys0 -a max_logname=MaxUserNameLength+1
```

Example:

```
# chdev -l sys0 -a max_logname=255
```

This command allocates 254 characters for the user and 1 for the terminating null.

The safest value that you can set `max_logname` to is `255`.

You must reboot for the changes to take effect:

```
# shutdown –Fr
```

Note: AIX 5.2 does not support increasing the maximum user name length.

Make Sure Outbound Ports Are Open

If you are using local firewall settings, such as `iptables`, on a computer running the Likewise agent, make sure the following ports are open for outbound traffic.

Note: The Likewise agent is a client only; it does not listen on any ports.

Port	Protocol	Use
53	UDP/TCP	DNS
88	UDP/TCP	Kerberos 5
123	UDP	NTP
137	UDP	NetBIOS Name Service
139	TCP	NetBIOS Session (SMB)
389	UDP/TCP	LDAP
445	TCP	SMB over TCP
464	UDP/TCP	Machine password changes (typically after 30 days)
3268	TCP	Global Catalog search

Resolve an AD Alias Conflict with a Local Account

When you use Likewise to set an Active Directory alias for a user, the user can have a file-ownership conflict under the following conditions if the user logs on with the AD account:

- The AD alias is the same alias as the original local account name.
- The home directory assigned to the user in Active Directory is the same as the local user's home directory.
- The owner UID-GID of the AD account is different from that of the local account.

To avoid such conflicts, by default Likewise includes the short AD domain name in each user's home directory. If the conflict nevertheless occurs, there are two options to resolve it:

1. Make sure that the UID assigned to the user's AD alias is the same as that of the user's local account. See Specify a User's ID and Unix or Linux Settings.
2. Log on as root and use the `chown` command to recursively change the ownership of the local account's resources to the AD user alias.

Change Ownership

Log on the computer as root and execute the following commands:

```
cd <users home directory root>

chown –R <AD user UID>:<AD primary group ID> *.*
```

Or: `chown –R <short domain name>\\<account name>:<short domain name>\\<AD group name> *.*`

Restart the Authentication Daemon

On Linux and Unix

You can restart the authentication daemon by executing the following command at the shell prompt:

```
/sbin/service lsassd restart
```

To stop the daemon, enter the following command:

```
/sbin/service lsassd stop
```

To start the daemon, enter the following command:

```
/sbin/service lsassd start
```

Note: On Unix systems, the location of the daemon may vary.

On HP-UX

Restart: `/sbin/init.d/lsassd restart`
Stop: `/sbin/init.d/lsassd stop`
Start: `/sbin/init.d/lsassd start`

On Mac OS X

On a Mac, use the following `stop` and `start` commands (you cannot use the `restart` command on a Mac):

```
sudo launchctl stop com.likewisesoftware.lsassd

sudo launchctl start com.likewisesoftware.lsassd
```

View Kerberos Tickets

On a target Linux or Unix computer, you can see a list of Kerberos tickets by executing the following command:

```
 /opt/likewise/bin/klist
```

The command lists the location of the credentials cache, the expiration time of each ticket, and the flags that apply to the tickets. For more information, see the man page for `klist`.

Because Likewise includes its own Kerberos 5 libraries (in `/opt/likewise/lib`), you must use the Likewise `klist` command by either changing directories to `/opt/likewise/bin` or including the path in the command.

Example:

```
-sh-3.00$ /opt/likewise/bin/klist
Ticket cache: FILE:/tmp/krb5cc_593495191
Default principal: hoenstiv@LIKEWISEDEMO.COM
Valid starting     Expires            Service principal
07/22/08 16:07:23  07/23/08 02:06:39
 krbtgt/LIKEWISEDEMO.COM@LIKEWISEDEMO.COM
        renew until 07/23/08 04:07:23
07/22/08 16:06:39  07/23/08 02:06:39
 host/rhel4d.LIKEWISEDEMO.COM@
        renew until 07/23/08 04:07:23
07/22/08 16:06:39  07/23/08 02:06:39
 host/rhel4d.LIKEWISEDEMO.COM@LIKEWISEDEMO.COM
        renew until 07/23/08 04:07:23
07/22/08 16:06:40  07/23/08 02:06:39  RHEL4D$@LIKEWISEDEMO.COM
        renew until 07/23/08 04:07:23
-sh-3.00$
```

Note: To address Kerberos issues, see Troubleshooting Kerberos Errors at http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/tkerberr.mspx.

Leaving a Domain And Uninstalling the Agent

Leave a Domain

Likewise reverses the Likewise-specific settings that were made to the computer's configuration when it was joined to the domain. Likewise also reverses any changes that you manually made to `/etc/likewise/lsassd.conf`. Before you leave a domain, you can execute the following command to view the changes that will be made:

`domainjoin-cli leave --advanced --preview` *`domainName`*

Example:

```
[root@rhel4d likewise]# domainjoin-cli leave --advanced --preview
likewisedemo.com
Leaving AD Domain:   LIKEWISEDEMO.COM
[X] [S] ssh            - configure ssh and sshd
[X] [N] pam            - configure pam.d/pam.conf
[X] [N] nsswitch       - enable/disable Likewise nsswitch module
[X] [N] stop           - stop daemons
[X] [N] leave          - disable machine account
[X] [N] krb5           - configure krb5.conf
    [F] keytab         - initialize kerberos keytab
Key to flags
[F]ully configured        - the system is already configured for
this step
[S]ufficiently configured - the system meets the minimum
configuration
                            requirements for this step
[N]ecessary               - this step must be run or manually
performed.
[X]                       - this step is enabled and will make
changes
[ ]                       - this step is disabled and will not
make changes
```

For information on advanced commands for leaving a domain, see Join Active Directory with the Command Line.

The Computer Account in Active Directory

When you leave a domain, the computer's account in Active Directory is not disabled and not deleted. If, however, you include the user name as part of the `leave` command, the computer's account is disabled but not deleted. You can include the user name as part of the `leave` command as follows; you will be prompted for the password of the user account:

`domainjoin-cli leave` *`userName`*

Example: `domainjoin-cli leave brsmith`

Remove a Linux or Unix Computer from a Domain

- On the Linux or Unix computer that you want to remove from the Active Directory domain, use a root account to run the following command:

```
/opt/likewise/bin/domainjoin-cli leave
```

Remove a Mac from a Domain

To leave a domain on a Mac OS X computer, you must have administrative privileges on the Mac.

1. In Finder, click **Applications**.
2. In the list of applications, double-click **Utilities**, and then double-click **Directory Access**.
3. On the **Services** tab, click the lock  and enter an administrator name and password to unlock it.
4. In the list, click **Likewise**, and then click **Configure**.
5. Enter a name and password of a local machine account with administrative privileges.
6. On the menu bar at the top of the screen, click the **Likewise Domain Join Tool** menu, and then click **Join or Leave Domain**.
7. Click **Leave**.

Remove a Mac with the Command Line

Execute the following command with an account that allows you to use sudo:

```
sudo /opt/likewise/bin/domainjoin-cli leave
```

Uninstall the Domain Join GUI

On a Linux computer, you can uninstall the domain join GUI from the command line by running the following command as root:

```
/opt/likewise/setup/djgtk/uninstall
```

Uninstall the Agent on a Linux or Unix Computer

Uninstall BitRock Installations on Linux or Unix

On a Linux or Unix computer, you can uninstall the Likewise agent from the command line if you originally installed the agent with the BitRock installer.

Important: Before uninstalling the agent, you should leave the domain and uninstall the domain-join GUI. Then execute the `uninstall` command from a directory other than `likewise` so that the uninstall program can delete the `likewise` directory and all its subdirectories. For example, execute the command from the root directory.

- To uninstall the agent on a Linux computer running Likewise Enterprise, run the following command as root:

  ```
  /opt/likewise/setup/lwise/uninstall
  ```

- To uninstall the agent on a Linux computer running Likewise Open, run the following command as root:

  ```
  /opt/likewise/setup/lwiso/uninstall
  ```

Uninstall Likewise with the Shell Script on Linux or Unix

If you installed the agent on a Linux or Unix computer by using the shell script, you can uninstall the Likewise agent from the command line by using the installer shell script with the `uninstall` option. For example, on HP-UX, change directories to the location of Likewise Enterprise and then run the following command as root:

```
./LikewiseEnterprise-5.0.0.1883-hpux-depot-hppa20.sh
uninstall
```

Or, if the software has been unpacked, run the following command as root:

```
./LikewiseEnterprise-5.0.0.1883-hpux-depot-
hppa20/install.sh uninstall
```

Uninstall the Agent on a Mac

On a Mac computer, you must uninstall the Likewise agent by using the Terminal. Before uninstalling the agent, you should leave the domain.

1. Log on the Mac by using a local account with privileges that allow you to use `sudo`.

2. Open a Terminal window: In Finder, on the **Go** menu, click **Utilities**, and then double-click **Terminal**.

3. At the Terminal shell prompt, execute the following command:

   ```
   sudo /opt/likewise/bin/macuninstall.sh
   ```

Platform Support

Likewise Open and Likewise Enterprise run on a broad range of platforms. Likewise is constantly adding new vendors and distributions to the following list. To get the latest list of supported platforms, go to http://www.likewisesoftware.com/products/likewise_enterprise/supported_platforms.php.

Vendor	Distribution	Supported	
		32-bit	64-bit
	AIX 5L 5.2	-	✓
	AIX 5L 5.3	-	✓
	OS X v10.3 PPC	✓	✓
	OS X v10.4 PPC	✓	✓
	OS X Server v10.4 PPC	✓	✓
	OS X v10.4 x86	✓	✓
	Asianux Server 3	✓	✓
	CentOS 4.0	✓	✓
	CentOS 4.1	✓	✓
	CentOS 4.2	✓	✓
	CentOS 4.3	✓	✓
	CentOS 4.4	✓	✓
	CentOS 5.0	✓	✓
	Debian Linux 3.1	✓	✓

Vendor	Distribution	Supported 32-bit	Supported 64-bit
fedora	Fedora Core 3	✓	-
	Fedora Core 4	✓	✓
	Fedora Core 5	✓	✓
	Fedora Core 6	✓	✓
	Fedora Core 7	✓	✓
hp	HP-UX 11.11 PA-RISC - Trusted Mode	-	✓
	HP-UX 11.11 PA-RISC - Untrusted Mode	-	✓
	HP-UX 11.23 Itanium - Trusted Mode	-	✓
	HP-UX 11.23 Itanium - Untrusted Mode	-	✓
ORACLE	Oracle Enterprise Linux 4	✓	✓
	Oracle Enterprise Linux 5	✓	✓
redhat	Red Hat Enterprise Linux AS 2.1	✓	-
	Red Hat Enterprise Linux ES 2.1	✓	-
	Red Hat Enterprise Linux WS 2.1	✓	-
	Red Hat Enterprise Linux AS 3.0	✓	✓
	Red Hat Enterprise Linux ES 3.0	✓	✓
	Red Hat Enterprise Linux WS 3.0	✓	✓
	Red Hat Enterprise Linux AS 4.0	✓	✓
	Red Hat Enterprise Linux ES 4.0	✓	✓
	Red Hat Enterprise Linux WS 4.0	✓	✓

Vendor	Distribution	Supported	
		32-bit	64-bit
Sun	Red Hat Enterprise Linux 5.0	✓	✓
	Red Hat Enterprise Linux 5.0 Desktop	✓	✓
	Red Hat Enterprise Linux 5.0 Advanced Platform	✓	✓
	Red Hat Linux 7.2	✓	-
	Red Hat Linux 7.3	✓	-
	Red Hat Linux 8	✓	-
	Red Hat Linux 9	✓	-
	Solaris 8 (SPARC)	✓	✓
	Solaris 8 x86	✓	✓
	Solaris 9 (SPARC)	✓	✓
	Solaris 9 x86	✓	✓
	Solaris 10 (SPARC)	-	✓
	Solaris 10 x86	-	✓
	Open Solaris	-	✓
SuSE	SuSE Linux Desktop 8.2	✓	-
	SuSE Linux Desktop 9.0	✓	-
	SuSE Linux Desktop 9.1	✓	✓
	SuSE Linux Desktop 9.2	✓	✓
	SuSE Linux Desktop 9.3	✓	✓

Vendor	Distribution	Supported 32-bit	Supported 64-bit
ubuntu	SuSE Linux Enterprise Desktop 10.0	✔	✔
	OpenSuSE Linux 10.0	✔	✔
	OpenSuSE Linux 10.1	✔	✔
	OpenSuSE Linux 10.2	✔	✔
	SuSE Linux Enterprise Server 9.0	✔	✔
	SuSE Linux Enterprise Server 10.0	✔	✔
	Ubuntu Desktop 6.06	✔	✔
	Ubuntu Desktop 6.10	✔	✔
	Ubuntu Server 6.06	✔	✔
	Ubuntu Server 6.10	✔	✔
	Ubuntu Desktop 7.04	✔	✔
	Ubuntu Desktop 7.10	✔	✔
	Ubuntu Server 8.04	✔	✔
	Ubuntu Desktop 8.04	✔	✔
vmware	VMWare ESX Server 2.5	✔	-
	VMWare ESX Server 3.0.1	✔	-

About Likewise Enterprise

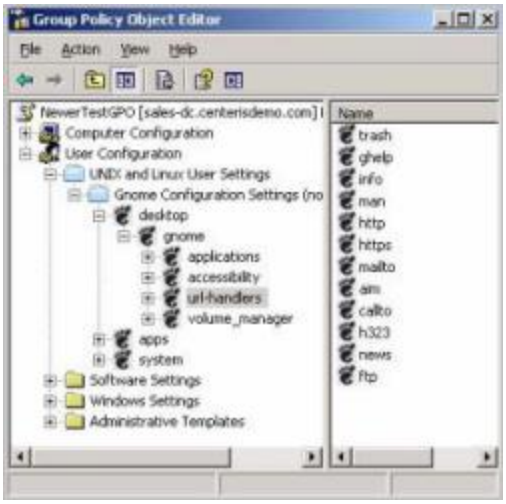
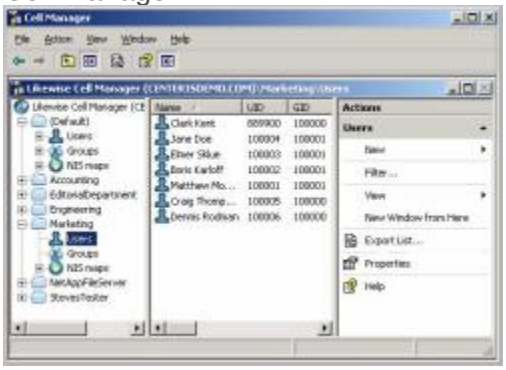
Likewise Enterprise joins Linux, Unix, and Mac OS X computers to Microsoft Active Directory to centrally manage all your computers, authenticate users, control access to resources, apply group policies, and audit your systems. To upgrade to Likewise Enterprise, see http://www.likewisesoftware.com/ or send an email to sales@likewisesoftware.com.

By joining non-Windows computers to Active Directory – a secure, scalable, stable, and proven identity management system – Likewise Enterprise 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, migrate NIS users while retaining their ID mappings, and centrally administer Linux, Unix, and Mac computers with group policies. The Likewise group policies are simple to manage because they are integrated into the Microsoft Group Policy Object Editor. Likewise includes reporting tools that can help improve regulatory compliance. The result: lower operating costs, better security, enhanced compliance.

Software Components

Likewise Enterprise comprises several software components, each of which provides part of the functionality necessary to manage Linux and Unix computers in Active Directory.

Component	Function
Agent 	• Joins a Linux or Unix computer to Active Directory with the domain join command-line interface or GUI. • Communicates with an Active Directory Domain Controller to authenticate and authorize users and groups by using the Likewise authentication daemon. • Pulls and refreshes group policies by using the Likewise group policy daemon.

Component	Function
Management Console 	• Runs on a Windows administrative workstation that connects to an Active Directory Domain Controller to help manage Linux, Unix, and Mac OS X computers within Active Directory. • Migrates users, checks status, finds and removes orphaned objects, and generates reports.
MMC Snap-Ins for ADUC and GPOE 	• Extends Active Directory Users and Computers to include Unix and Linux users. • Extends the Group Policy Object Editor and the Group Policy Management Console to include Linux, Unix, and Mac OS X group policies as well as a way to target them at specific platforms.
Cell Manager 	• An MMC snap-in to manage cells associated with Active Directory Organizational Units.

Get Technical Support

For technical support, please visit the Likewise Open community Web page at http://www.likewisesoftware.com/community/. You can use the page to join the Likewise Open mailing list to discuss Likewise Open with other users and developers.

You can also obtain paid support from Likewise Software by visiting http://www.likewisesoftware.com/support/ or writing to sales@likewisesoftware.com.

ABOUT LIKEWISE SOFTWARE

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.

Likewise® Open

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.

Likewise Open is an open source, community project sponsored by Likewise Software to provide fast and easy integration into networks using Microsoft Active Directory. For licensing information, see www.likewisesoftware.com.

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

Likewise Open