



## Access Control for Linux, Unix And Mac OS X Computers

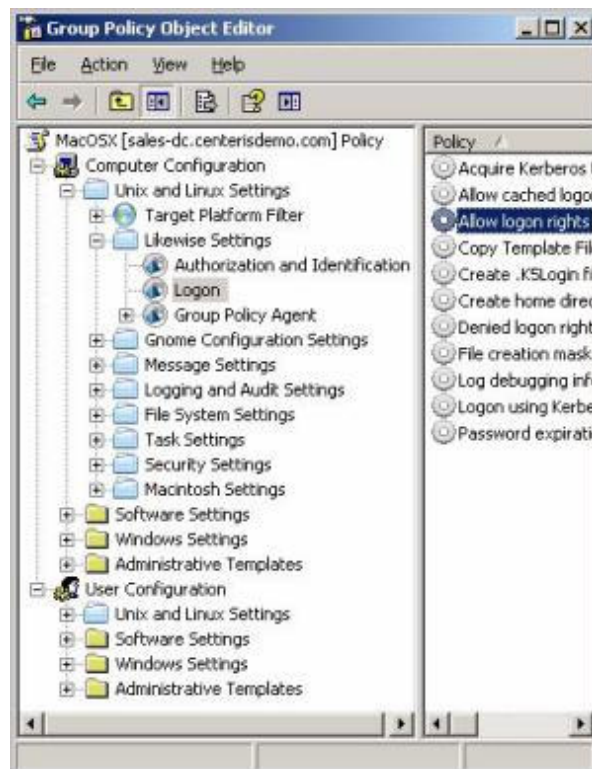
### USE LIKewise ENTERPRISE TO CONTROL ACCESS TO LINUX, UNIX, AND MAC

- Centrally manage Unix, Linux, and Mac user accounts
- Control who is allowed to log on different computers
- Control what actions users are allowed to perform on different computers

### Overview

Effective access control is fundamental to all enterprise IT organizations. It is essential that only authorized users have access to systems that contain sensitive information. The ability to demonstrate effective access control is imperative during IT security audits.

Likewise Enterprise provides several mechanisms that can be used to implement access control for Linux, Unix, and Mac OS X computers. This paper explores these mechanisms and suggests when each is most appropriate.



### How Access Control Works with Unix, Linux, and Mac OS X

Fundamentally, access control is a matter of restricting who is allowed to log on a particular computer. In most versions of Unix and Linux, this process is managed by the Pluggable Authentication Module, or *PAM*. In Mac OS X, the *Open Directory* service provides this functionally.

PAM and Open Directory allow a computer to support different authentication mechanisms. For example, a computer might support a local authentication mechanism based on a local list of users and passwords (*/etc/passwd* in most Unix and Linux systems).

A computer can, at the same time, support another authentication mechanism based on a centralized directory. Likewise Enterprise provides such a mechanism and installs its mechanism into PAM and Open Directory.

The Likewise authentication mechanism, which is based on the Kerberos and LDAP security protocols, lets computers authenticate using data stored in a centralized Microsoft Active Directory™ (AD) server. Likewise Enterprise provides tools that let you specify information in AD to provide effective access control for Unix, Linux, and Mac OS X computers.

### How Likewise Enterprise Authenticates Users

When PAM or Open Directory calls the Likewise authentication mechanism, it supplies a username and password and asks Likewise whether these credentials represent a valid user. To answer that question, Likewise must determine several things:

1. Does the username/password represent a valid Active Directory user?
2. Is this user enabled for Unix, Linux, and Mac access?
3. Does the user pass any authentication restrictions defined through group policy?

The user is authenticated only if the answer to *all* of these questions is yes. Consequently, each of the steps offers an opportunity for access control; if any of the steps results in a answer of no, the Likewise authentication mechanism returns a status code to PAM or Open Directory indicating that it cannot authenticate the user. The following sections consider each of these questions separately and explore what mechanisms Likewise Enterprise provides that allow you to implement access control.

### Determining Whether a Username/Password Represents a Valid Active Directory User

Likewise implements this step by using the Kerberos security protocol. Kerberos provides a strong cryptographic mechanism that allows Likewise to communicate with Active Directory to verify that a username and password correspond to a valid user in AD.

This is the most fundamental form of access control that Likewise provides. It allows administrators to stop using local accounts on Unix, Linux, and Mac OS X computers and, instead, empowers them to manage all their user accounts centrally in AD. A user is allowed to log on only if he or she has a valid AD user account.

In addition to this existence check, AD provides settings at the user account level that can be used to further strengthen access controls. Using the Microsoft *Active Directory Users and Computers* (ADUC) console you can set various options:

- *Logon Hours* – the days of the week and times of day that a user is allowed to log on any machine
- *Log On To* list – the computers that a user logon can log on
- *Disable account* – disallow logons by a user

Although the *Log On To* list can be a very powerful, granular, way of specifying access control, other similar mechanisms described below might be easier to administer.

### **Determining Whether a User is Enabled for Unix, Linux, and Mac OS X Access**

To log on a Unix, Linux, Mac OS X computer running Likewise Enterprise, the user must have more than just a valid account in AD: The user must be explicitly *enabled* for such access and assigned a set “Unix” attributes (these apply to Linux and Mac OS X, as well):

- *UID* – a “Unix” user ID number
- *Primary GID* – a Unix ID number for the user’s primary group
- *Home directory* – a file system path to be used as the user’s home directory
- *Login shell* – the file system path of the system shell program to be used, by default, for the user
- *Login name* (optional) – an alternative alias that the user can use instead of his or her full AD user account name
- *GECOS* (optional) – a description string for the user

A further nuance in this step is that Likewise Enterprise allows an AD user to be assigned *multiple* sets of Unix attributes, allowing the user to employ

different attributes when logging on different computers. Likewise implements this feature by way of its *Cell* mechanism.

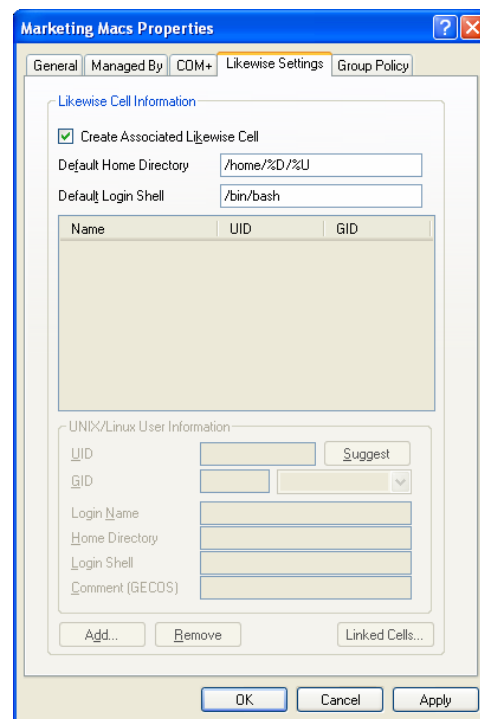
A Likewise Cell is...

- ...a collection of Unix, Linux, Mac OS X computers that share a single set of Unix attributes for a particular AD user
- ...a container of Unix attributes for AD users *enabled* to access the computers in the Cell
- ...associated with an Active Directory *Organizational Unit* (OU)

To better understand this, let us review how a Cell is created and administered.

First, using the Microsoft ADUC console, an AD organizational unit is created. The OU is typically given a name that reflects its function, for example, “OU=Accounting UNIX Servers” or “OU=Marketing Macs”.

Second, again in ADUC, the properties for the OU are displayed and the Likewise Settings tab is selected:



The Create Associated Likewise Cell checkbox is selected and OK or Apply is chosen.

Once the Cell is created, the Add button can be used to enable users and groups to be used in the Cell. Enabling an AD user or group in a Cell assigns Unix attributes to that user or group. The lower portion of the property page allows you to specify these attributes.

Finally, individual Unix, Linux and Mac OS X computers are joined to Active Directory in the newly created organizational unit.

Joining a computer to a particular OU creates an AD computer object in that OU. From the Likewise perspective, OU membership determines the Likewise Cell that is used to determine whether users are enabled to access the Unix/Linux/Mac OS X computers that belong to that Cell.

Note the algorithm used by Likewise to determine to which Cell a Unix, Linux or Mac OS X belongs: Likewise will look for the computer's associated computer object and will then look at its containing organizational unit to see if a Likewise Cell has been created there. If it has not, *Likewise will continue looking for Cells in parent OUs*. A computer belongs to the first Cell encountered when looking at the parentage of its associated computer object in AD.

With this understanding of Likewise Cells, it is easy to see how Cells can be used for access control. If a user is enabled in a Cell, he or she can logon to the Unix, Linux and Mac OS X machines that belong to that Cell. Judicious use of Cells can provide a convenient way of controlling access to different classes of Unix, Linux and Mac OS X computers.

There is a potential disadvantage to using Likewise Cells, however. Each Cell is a container of Unix attributes for users and groups. A Cell allows a user to have *different* attributes when accessing different computers. For example, the user *CORP\jane* might have a UID of 1000 when accessing the *Accounting UNIX Servers* Cell and a UID of 2134 when accessing the *Marketing Macs* Cell. What if you want *CORP\jane* to have the same attributes in both? Because each Cell is a container of attributes, it can become necessary to manage data in multiple Cells requiring duplicate work.

To minimize this need for redundant work, Likewise provides the concept of *Linked Cells*. A Cell can be linked to another Cell so that its Unix attributes are automatically considered to be part of the current Cell, too. Likewise will search for Unix attributes in the current Cell first and then in any linked Cells. Linked Cells can greatly reduce the need for duplicated data and administrative work.

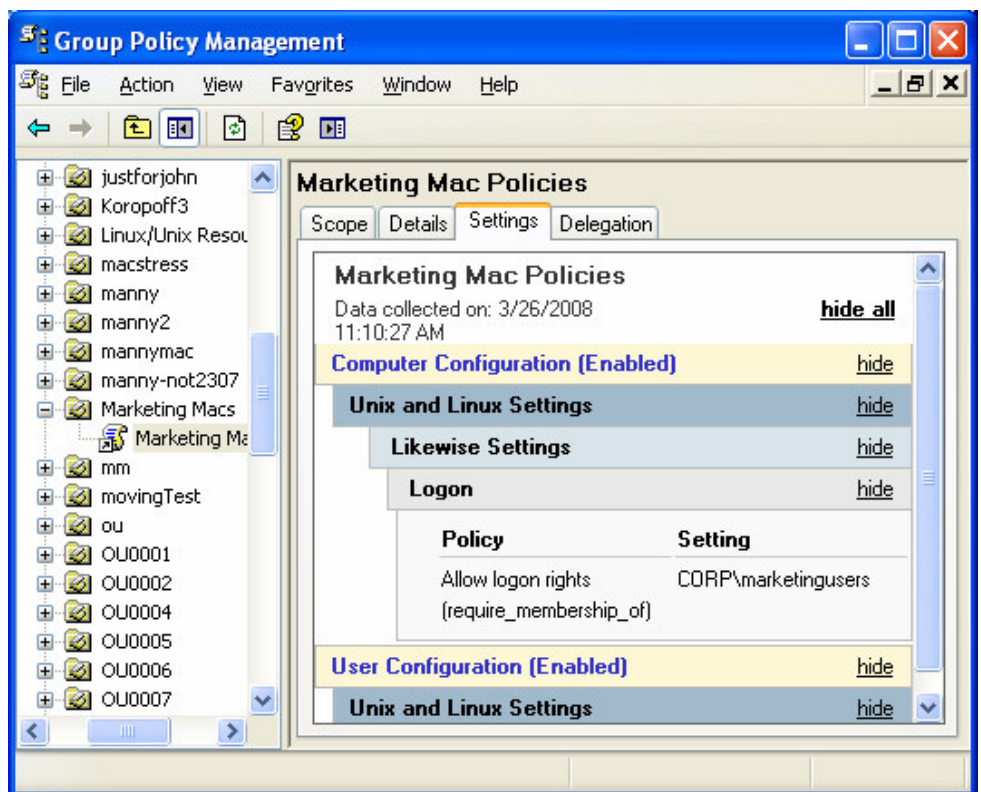
### **Determining Whether the User Passes Any Authentication Restrictions Defined Through Group Policy**

Likewise Enterprise extends the Active Directory Group Policy architecture to encompass Unix, Linux and Mac OS X computers. Likewise provides

user interface components for Microsoft Windows that allow administrators to create Group Policy settings specific to Unix, Linux and Mac OS X.

Currently, there is one particular setting that is of interest when implementing access controls: *Allow logon rights (require\_membership\_of)*. This setting allows you to require that a user be a member of a particular group in order to log on a computer affected by the Group Policy object. You can designate one or more groups when defining this Group Policy setting. *A user will be allowed to log on only if he or she is a member of at least one of the designated groups.*

The *Allow logon rights* setting is found in the *Computer Configuration/Unix and Linux Settings/Likewise Settings/Logon* section when editing a group policy object.



In this example, the policy setting requires users to be members of the *CORP/marketingusers* group.

Note that, although Likewise provides Group Policy support for this mechanism, it can also be used without Group Policy. Ultimately, the

Likewise Group Policy agent, when it detects that *Allow logon rights* has been defined, edits a configuration file to reflect the Group Policy settings. This file can be manually edited if you do not wish to use Group Policy or if you wish to specify logon rights on a machine-by-machine (instead of an OU) basis. The file typically exists in `/etc/security/pam_lwidentity.conf`. You can edit this file manually and set the `require_membership_of` keyword to the appropriate list of groups (comma separated). The file contains comments instructing you on how to do this.

### Authentication vs. Authorization

So far, our discussion of access control has focused exclusively on authentication. Once Likewise determines that a user is properly authenticated and has access to a particular computer, the user is allowed to login. Beyond login, Likewise Enterprise can also help you control what operations a user is *authorized* to perform.

By connecting Unix, Linux and Mac OS X systems to Active Directory, Likewise allows the efficient use of the *SUDO* utility to control access to privileged system commands and utilities.

SUDO allows non-privileged user accounts (users who are not *root* or members of the *root* group) to execute privileged commands and utilities. The user prefixes the privileged operation with `sudo`:

```
sudo umount /dev/hd0
```

The *sudo* utility first consults its configuration file (typically, in `/etc/sudoers`) and determines if the current user is allowed to perform the specified command. If so (and, perhaps, after another password prompt), the *sudo* program executes the command on behalf of the user.

Likewise Enterprise provides a Group Policy setting that facilitates the centralized configuration of SUDO. Additionally, with Likewise, the SUDO configuration file can refer to Active Directory users and groups when designating who can perform privileged commands. SUDO can be configured, for example, to allow members of the `CORP\MarketingAdmins` group to execute the *umount* utility. Administrators can then easily control what users are authorized to perform what operations based on their role by simply adding users to appropriate AD groups.

A full explanation of SUDO is beyond the scope of this paper. Another Likewise Technical Note, *How to Create and Test a SUDO Group Policy for Unix and Linux*, provides additional information on this topic.

### Design Guidelines

Likewise Enterprise provides multiple mechanisms for implementing access control. Which of these mechanisms should you use? Here are some guidelines:

- If all you need is centralized account management, then a single Cell will serve all your purposes. Create a single Likewise Cell and join all your systems to it. Enabling a user in that Cell will enable the user to log on any of the Unix, Linux or Mac OS X systems in the Cell. Use AD user account settings to control login days/times and granular access to individual systems.
- If you need to have different Unix attributes when logging on different machines (e.g. you're currently using multiple NIS servers and migrating to Likewise Enterprise), you should use a Cell-based approach. Create multiple organizational units and multiple Likewise Cells. Join Unix, Linux and Mac OS X systems to the appropriate OU/Cell. Enable users in the specific Cells to which they need access.
- If you do not need different multiple Unix attribute sets for users but still want to restrict who can logon to different groups of computers, define a single Likewise Cell but make use of *Allow logon rights* to restrict access based on Active Directory group membership, which can in effect give you role-based access control. Configure *Allow logon rights* through Group Policy or by modifying the *pam\_lwidentity.conf* file in your Unix, Linux, and Mac OS X systems.

These mechanisms are not completely exclusive of each other. For example, you can define multiple Cells and use them for access control but *also* use *Allow logon rights* Group Policy to further restrict access.

### Reporting and Auditing Considerations

Once you have set up your access controls, it is useful to be able to generate reports that illustrate what users can access which computers. If

you are undergoing a security audit you may be required to generate such reports.

To demonstrate Cell-based access control, you can use the Likewise Console to generate the necessary reports. In the *Reports* pane, select the *Forest Users and Groups* report and click on *Run Report*. The output will look similar to this:

**Report**

Print... Print Preview... Save As... Close

Cell Name: Mac

Computer Name	Computer DNS Name
BUILD1896	build1896.corp.centeris.com
macbookair	macbookair.corp.centeris.com
MIKEW-MACOSX	mikew-macosx.corp.centeris.com
nielmac4	nielmac4.corp.centeris.com
SYOUNG-OSX	syoung-osx.corp.centeris.com

Group Name	Full Group Name	GID	Group Description	Group Alias	Members
Domain Users	CORP\Domain Users	196608513			Barry Crist, Mike Wietholter, Steve Nielsen, Steve Young, Bill Skoda

User Name	Login Name	UID	Primary GID	Login Shell	Home Directory
Barry Crist	CORP\bcris	196609126	196608513	/bin/bash	/CORP/bcris
Bill Skoda	CORP\bskoda	196609900	196608513	/bin/bash	/CORP/bskoda
Mike Wietholter	CORP\mwietholter	196609957	196608513	/bin/bash	/CORP/mwietholter
Steve Nielsen	CORP\snelsen	196609970	196608513	/bin/bash	/CORP/snelsen
Steve Young	CORP\syoun	196609954	196608513	/bin/bash	/CORP/syoun

Likewise Enterprise will generate a report that, for each Cell, shows:

- The computers in the Cell
- The groups enabled in the Cell
- The users enabled in the Cell

To demonstrate access control based on *Allow logon rights*, use the Microsoft Group Policy Management Console to identify the applicable Group Policy objects and to generate reports that illustrate their settings (as shown earlier).

### Summary

Likewise Enterprise provides several mechanisms for implementing effective access controls. The choice of which to use depends on your particular needs. All of them can help you meet your reporting and auditing needs.

### ABOUT LIKewise

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

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