



## Group Policies for Mac OS X

### APPLY GROUP POLICIES TO MAC OS X COMPUTERS

- Centrally manage Mac configuration settings
- Automate enforcement of IT policies such as password length and complexity
- Simplify administrative tasks like shell scripts and cron jobs
- Consistently implement security settings across the enterprise
- View reports about group policies in the Group Policy Management Console.

### SUPPORTED MAC VERSIONS

Likewise Enterprise supports the 32-bit and 64-bit versions of the following Mac operating systems:

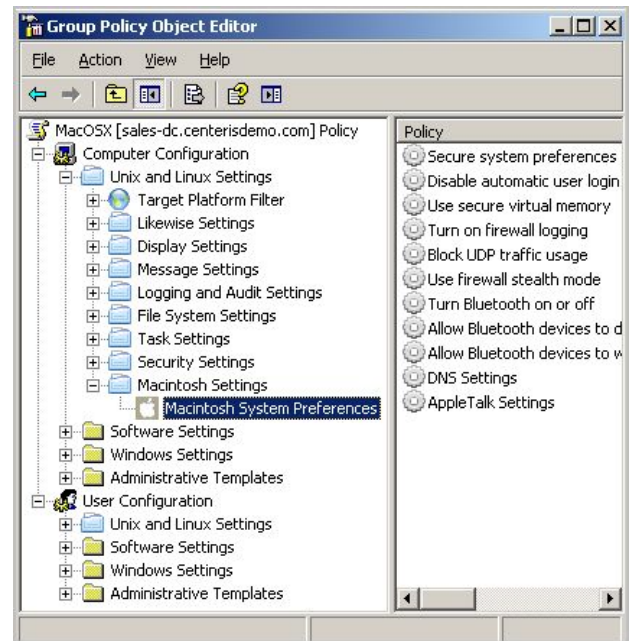
- OS X v10.4 PowerPC
- OS X Server v10.4 PowerPC
- OS X v10.4 x86
- OS X v10.3 PowerPC

### Overview

Microsoft Active Directory lets you define settings for servers and workstations. Local policy settings can be applied to all machines, and for those that are part of a domain, you can apply group policies across a given site, domain, or range of organizational units.

Likewise provides a Group Policy Agent that extends policy-based management to Mac OS X computers so that you

can centrally administer all your Mac computers. The Likewise policies are simple to manage because they are integrated into the Microsoft Group Policy Object Editor and the Microsoft Group Policy Management Console.



### How Group Policy Works with Mac OS X

Likewise group policies work like Windows group policies. After Likewise joins a Mac OS X computer to Active Directory, the Likewise Group Policy Agent runs in the background on the Mac. The agent determines the group policy objects that are applied to a system.

Likewise has implemented a set of client-side extensions for Unix computers, including computers running Mac OS X. This document lists the Likewise group policies that can be applied to Mac computers.

### Likewise Mac OS X Policies

Likewise adds support for configuring Mac system settings with group policies. You can use the following policies to manage and protect Mac OS X computers. The policies in the following table apply only to computers running Mac OS X.

Group Policy	Description
<b>Allow Bluetooth Devices to Find the Computer</b>	This group policy makes target Mac OS X computers discoverable by Bluetooth devices.
<b>Allow Bluetooth Devices to Wake the Computer</b>	This group policy sets the system preferences to allow Bluetooth devices to wake target Mac OS X computers. The policy allows a user who has a Bluetooth keyboard or mouse to press a key or click the mouse to wake a sleeping computer.
<b>Block UDP Traffic</b>	This policy sets the built-in firewall on target computers running Mac OS X to block UDP traffic. Blocking User Datagram Protocol traffic can help secure target computers.
<b>Disable Automatic User Login</b>	This policy disables automatic login on target computers running Mac OS X. The policy requires a user to log on every time the computer is turned on or restarted.
<b>Log Firewall Activity</b>	This policy logs firewall activity on target computers running Mac OS X Tiger or later. To help you monitor and audit Mac computers for security issues, the policy turns on firewall logging, which keeps a log of such events as blocked attempts, blocked sources, and blocked destinations.
<b>Secure System Preferences</b>	This policy locks system preferences on target computers running Mac OS X so that only administrators with the password can change the preferences.
<b>Turn Bluetooth On or Off</b>	This policy turns on or turns off Bluetooth power on target Mac OS X computers. When Bluetooth power is turned off, other Bluetooth devices, such as wireless keyboards and mobile phones, cannot connect to the computer.

Group Policy	Description
<b>Use Firewall Stealth Mode</b>	This policy sets the built-in firewall on target computers running Mac OS X to operate in stealth mode.  Stealth mode cloaks the target computer behind its firewall: Uninvited traffic gets no response, and other computers that send traffic to the target computer get no information about it. Stealth mode can help protect the target computer's security.
<b>Use Secure Virtual Memory</b>	This policy configures target computers running Mac OS X to store application data in secure virtual memory. In case the computer's hard drive is accessed without authorization, the policy sets the target Mac to encrypt the data that it stores in virtual memory.
<b>Make AppleTalk Active</b>	This policy makes AppleTalk active on target Mac OS X computers. You can also use this policy to make AppleTalk inactive.
<b>Set DNS Servers and Search Domains</b>	This policy specifies the DNS servers and search domains on target Mac OS X computers. The search domains are automatically appended to names that are typed in Internet applications.

### Authentication and Identification Policies

Group Policy	Description
<b>Refresh Kerberos Tickets Automatically</b>	This policy automatically refreshes Kerberos tickets on target Mac OS X computers. By automatically refreshing tickets, you can maintain a user's domain access. When this policy is enabled, the Likewise winbind daemon, <code>lwiauthd</code> , automatically refreshes Kerberos tickets that are retrieved using the <code>pam_winbind</code> module.
<b>Allow Offline Logon Support</b>	This policy allows target computers running Mac OS X to log onto domain accounts when the network or domain controller is unavailable by caching logon credentials and account info in <code>lwiauthd</code> .

Group Policy	Description
<b>ID Mapping Cache Expiration Time</b>	This policy sets the expiration time for the ID mapping cache on target Mac OS X computers. After a user or group is mapped to its security identifier (SID) in Active Directory, the Likewise winbind daemon, <code>lwiauthd</code> , caches the entry for the time that you specify. You can use this policy to improve the performance of your system if, for example, you are making a lot of changes to your ID mapping.
<b>ID Mapping Negative Cache Expiration Time</b>	This policy specifies how long the Likewise winbind daemon, <code>lwiauthd</code> , caches the unmapped state for an unsuccessful security identifier (SID) mapping for an Active Directory user or group to prevent repeated lookup requests that might degrade the performance of your system. You can use this policy on computers running Mac OS X.
<b>Winbind Cache Expiration Time</b>	This policy specifies how long the Likewise winbind daemon, <code>lwiauthd</code> , caches information about a user's home directory, logon shell, and the mapping between the user or group and the security identifier (SID) on target Mac OS X computers. Winbind features that are using offline cached credentials reattempt to log onto the Active Directory domain controller at the interval that you set. When online, <code>lwiauthd</code> also caches the information for the specified time. You can use this policy to improve the performance of your system by increasing the expiration time of the cache.
<b>Machine Account Password Expiration Time</b>	This policy sets the machine account password's expiration time on target Mac OS X computers. The expiration time specifies when machine account passwords are reset in Active Directory.
<b>Depth of Nested Group Expansion</b>	This policy sets the level of nested group expansion on target Mac OS X computers. The level of nested group expansion specifies how deep the Likewise winbind daemon, <code>lwiauthd</code> , traverses the tree when it expands nested groups into a membership list. You can specify how many levels you want <code>lwiauthd</code> to process when it expands nested groups into a membership list. For example, if you set the depth of group expansion to 0, group expansion is in effect disabled. If you set the depth of group expansion to 7 -- a typical setting -- <code>lwiauthd</code> processes nested groups as deep as 7 levels.

Group Policy	Description
<b>Replacement Characters for Names with Spaces</b>	<p>This policy replaces spaces in Active Directory user and group names with a character that you choose. For example, when you set the replacement character to ^, the group DOMAIN\Domain Users in Active Directory appears as DOMAIN\domain^users on target Mac OS X computers.</p>
<b>Allow Access to Samba Server Null-Password Accounts</b>	<p>This policy allows clients to gain access to Samba server accounts with null passwords. The policy modifies the following file on target Samba servers: /etc/samba/smb.conf. Enabling this policy can pose significant security risks.</p>
<b>Digitally Sign Client Communications</b>	<p>This policy enables, disables, or requires SMB signing when a client communicates with a server. The policy can help prevent session-hijacking attacks.</p> <p>To use SMB signing, you must either offer it or require it on both the SMB client and the SMB server. If SMB signing is offered on a server, clients that are also enabled for SMB signing use the packet signing protocol during all subsequent sessions. If SMB signing is required on a server, a client cannot establish a session unless it is at least enabled for SMB signing.</p>
<b>Digitally Sign Server Communications</b>	<p>This policy controls whether a server offers or requires SMB signing. The policy modifies the following file on target Mac OS X servers: /etc/samba/smb.conf.</p> <p>To help prevent message attacks, the Server Message Block (SMB) protocol supports mutual authentication by placing a digital signature into each Server Message Block. The digital signature is then verified by both the client and the server.</p>
<b>Send Encrypted Passwords to Third-Party SMB Servers</b>	<p>This policy requires a client to send encrypted passwords to a third-party SMB server when the server does not accept plain text passwords.</p> <p>Defining and then disabling this group policy requires the client to send an encrypted password to the SMB server. Defining and enabling this group policy allows the client to send a plain text password to the SMB server -- the default setting.</p>

Group Policy	Description
<b>Set the Maximum Tolerance for Kerberos Clock Skew</b>	This policy sets the maximum amount of time that the clock of the Kerberos Distribution Center (KDC) can deviate from the clock of target hosts. For security, a host rejects responses from any KDC whose clock is not within the maximum clock skew, as set in the host's <code>krb5.conf</code> file. The default clock skew is 300 seconds, or 5 minutes. This policy changes the clock skew value in the <code>krb5.conf</code> file of target Mac OS X hosts.
<b>Set the Samba Hostname Resolver Cache Timeout</b>	This policy sets Samba's hostname cache resolver timeout on target Mac OS X servers. The policy specifies the number of minutes before entries in Samba's hostname resolver cache expire. If you define the policy and set the timeout to 0, caching is disabled.
<b>Set the Samba Server LDAP Connection Timeout</b>	This policy sets the time, in seconds, that a Samba server is to wait to connect to an LDAP server before the connection fails.
<b>Turn Off Client LANMAN Authentication</b>	This policy can disable LANMAN authentication by an SMB client. LANMAN is an obsolete Windows authentication protocol that was replaced by NTLM. By default, LANMAN authentication is enabled, which might pose a security threat because of LANMAN's weak encryption.
<b>Turn On Client NTLMv2 Authentication</b>	This policy enables client NTLMv2 authentication. NTLM is a Microsoft challenge-response authentication protocol that is used with the SMB protocol. NTLMv2 is cryptographically stronger than NTLMv1. Without setting this group policy, the default is to not use NTLMv2.
<b>Minimum UID-GID Value</b>	This policy specifies the minimum UID-GID value for target Mac OS X computers. The lowest minimum value that you can set is 50; the highest minimum is 9999.

## Logon Policies

Group Policy	Description
<b>Acquire Kerberos Tickets on Logon</b>	This policy acquires Kerberos tickets when a computer running Mac logs onto the domain and, if <code>FILE</code> appears as the setting's string value field, stores the ticket in memory — that is, in a Kerberos 5 credential cache. To authenticate with Kerberos 5 but not store at ticket in memory, leave the string value field empty.
<b>Log on Using Kerberos Authentication</b>	This policy grants target Mac OS X computers access to a Windows NT domain using the Kerberos authentication protocol. When the policy is enabled, users log onto the Windows NT domain using Kerberos. When disabled, NT LAN Manager (NTLM) is used instead. NTLM is also used if Kerberos is unavailable from the domain controller.
<b>Create a .k5login File in a User's Home Directory</b>	This policy creates a .k5login file in the home directory of a user account on target Mac OS X computers that log onto the Windows NT domain using the Kerberos authentication protocol. The .k5login file contains the user's Kerberos principal. Kerberos can use the .k5login file to check whether a principal is allowed to log on as a user. A .k5login file is useful when your computers and your users are in different Kerberos realms or different Active Directory domains, which can occur when you use Active Directory trusts.
<b>Allow Cached Logons</b>	This policy allows computers running Mac OS X to use cached credentials when they cannot connect to the network or the domain controller for authentication. If you enable this policy, you also must enable the Allow offline logon support group policy in the Authorization and Identification folder.
<b>Allow Logon Rights</b>	This policy specifies the Active Directory users and groups allowed to log on target computers running Mac OS X. The setting can contain a comma-separated list of short domain names with Active Directory account names and group names, local account names and local user groups, and SIDs in string format.

Group Policy	Description
<b>Show a Denied Logon Rights Message</b>	This group policy displays a message when an Active Directory user cannot log on a target computer because the user is not in the list of the users or groups defined in the <a href="#">Allow Logon Rights</a> ( <code>require_membership_of</code> ) group policy. When you set the policy, you specify the message that is displayed for the <code>not_a_member_error</code> . This policy is for computers running Mac OS X.
<b>Create a Home Directory for a User Account at Logon</b>	This policy automatically creates a home directory for a user account on target Mac OS X computers. When the user logs on the computer, the home directory is created if it does not exist. The location of the home directory is specified in the Likewise settings of the user account.
<b>Copy Template Files When Creating a Home Directory</b>	This policy adds the contents of <code>skel</code> to the home directory created for a user account on target computers running Mac OS X. Using the <code>skel</code> directory ensures that all users begin with the same settings.
<b>File Creation Mask for the Contents of the Home Directory</b>	This policy sets permissions for the files in the home directory that is created when a user logs on target Mac OS X computers. All the files in the home directory are preset with the ownership settings of the file creation mask, or <code>umask</code> . You can use this policy to enter a <code>umask</code> value to set the permission level. For example, if you specify an octal permission set of <code>0022</code> , the file permissions are set as follows: Owner Read/Write, Others Read Only.
<b>Log Debugging Information</b>	This policy logs debugging information for the Likewise <code>winbind</code> daemon, <code>lwiauthd</code> , on target computers running Mac OS X.

### Message Policies

Group Policy	Description
<b>Login Prompt (/etc/issue)</b>	This policy places a message in the <code>/etc/issue</code> file on target computers running Mac OS X. The message, which appears before the login prompt, can display information that identifies the system. In the message text, you can use escape codes that <code>getty</code> recognizes.
<b>Message of the Day (/etc/motd)</b>	This policy sets a message of the day in the <code>/etc/motd</code> file on target computers running Mac OS X. The message of the day, which appears after a user logs in but before the logon script executes, can give users information about a computer. The policy replaces the <code>motd</code> file on the target computer.

### Logging and Audit Policies

Group Policy	Description
<b>SysLog</b>	This policy creates a syslog for target computers running Mac OS X to help you manage, troubleshoot, and audit your systems. You can log several facilities, such as <code>cron</code> , <code>daemon</code> , and <code>auth</code> , and you can use priority levels and filters to specify the messages that you want to collect.
<b>Rotate Logs</b>	To help you manage, troubleshoot, and archive your system's log files, this group policy configures and customizes your log-rotation daemon. For example, you can choose to use either a <code>logrotate</code> or <code>logrotate.d</code> file, specify the maximum size before rotation, compress old log files, and set an address for emailing log files and error messages. You can also enter commands to run before and after rotation.

## File System Policies

Group Policy	Description
<b>Files, Directories, and Links</b>	This policy creates directories, files, and symbolic links on target computers running Mac OS X computers.
<b>Automount</b>	This policy allows you to specify directories that are auto mounted when you access them. Auto mounts are useful for nfs, samba, and boot mounts/partitions.

## Task Policies

Group Policy	Description
<b>Run a Script File</b>	The script policy lets you specify a text-based script file to execute on Unix systems. The script is copied to the local machine at the next group policy refresh interval and immediately run. The script is run as the root user account. The shell script policy is executed every time the system reboots and on the first refresh interval after a change is made to the policy.
<b>Crontab/cron.d</b>	The Cron Policy allows you to specify <code>crontab</code> and <code>/etc/cron.d</code> files. Cron policies are files run at a regularly scheduled interval and include the following lines: <ul style="list-style-type: none"> <li>• minute (0-59)</li> <li>• hour (0-23)</li> <li>• day of the month (1-31)</li> <li>• month of the year (1-12)</li> <li>• day of the week (0-6 with 0=Sunday)</li> <li>• Command to run</li> </ul> Certain distributions support only <code>crontab</code> , and do not support <code>/etc/cron.d</code> files. Please refer to your platform's documentation for more information.

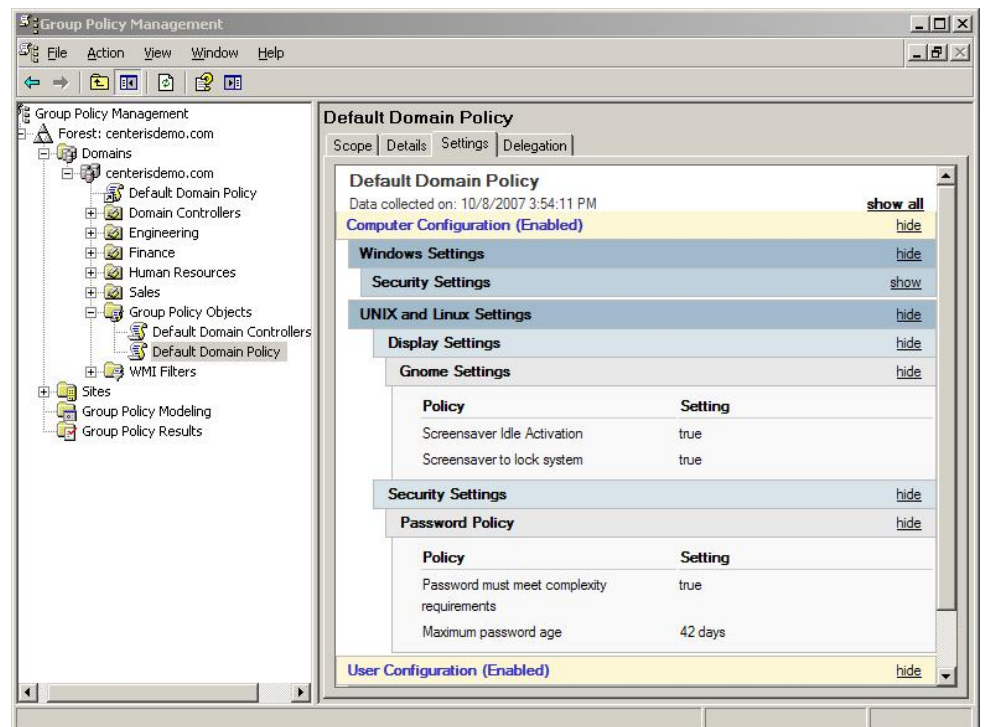
## Active Directory Security Policies

Joining a Mac to Active Directory gives you the ability to apply generic Active Directory security policies to Mac computers, users, and groups. For example, after using Likewise to join a Mac to a domain, you can

apply such policies as password complexity, minimum and maximum password length, and password aging requirements.

### Viewing Reports on Group Policy Settings

Likewise integrates its group policies into the Microsoft Group Policy Management Console so that you can use the console to manage Mac OS X policies. For example, you can view a report that shows the settings for a Likewise group policy. Here's an example:



### ABOUT LIKewise

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

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

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