



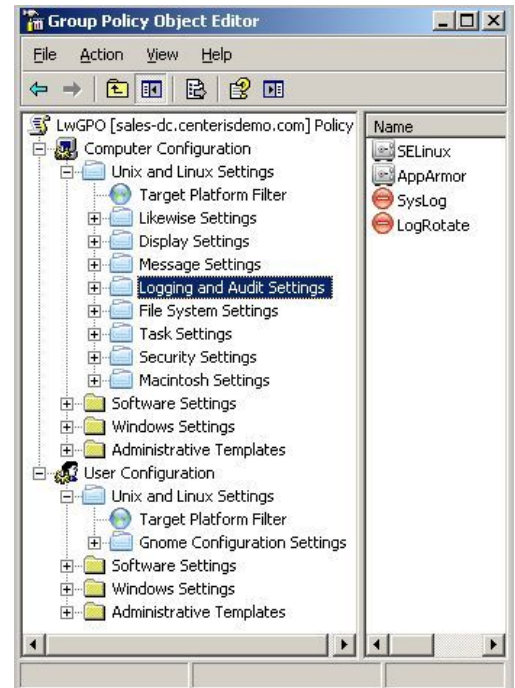
## Group Policies for Linux, Unix And Mac OS X Computers

### USE GROUP POLICIES WITH LINUX, UNIX, AND MAC OS X

- Centrally manage Unix, Linux, and 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
- Apply GConf settings to Gnome desktops with more than 2,000 user policies.
- Target policies at different platforms.
- View reports about group policies in the Group Policy Management Console.

### Overview

The group policy management solution in Microsoft Active Directory lets administrators define settings for servers and workstations. Local policy settings can be applied to all machines, and for those that are part of a domain, an administrator 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 Linux, Unix, and Mac OS X computers. The Likewise policies are integrated into the Microsoft Group Policy Object Editor.



### How Group Policy Works with Unix, Linux, and Mac OS X

Likewise group policies work similar to Windows group policies. After Likewise joins a Unix, Mac OS X, or Linux computer to Active Directory, the Likewise Group Policy Agent runs in the background on the Unix or Linux computer. The Likewise Group Policy Agent determines the list of group policy objects that are applied to a system. Likewise has implemented a set of client-side extensions for policies specific to Unix, Mac OS X, and Linux. These policies are irrelevant to Windows computers because the corresponding Unix or Linux client-side extensions do not exist on a Windows computer.

### Unix, Linux, and Mac OS X Policies

Likewise adds support for configuring Unix and Linux system settings with group policies. You can use the following policies to manage and protect Linux, Unix, and Mac OS X computers.

### Security Policies

Likewise allows you to enforce a subset of the Windows security policies on a Unix or Linux computer. When enabled, these settings apply to local system accounts.

Group Policy	Description
<b>Maximum Password Age</b>	This security setting determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the Minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days.
<b>Minimum Password Age</b>	This security setting determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days, or you can allow changes immediately by setting the number of days to 0. The minimum password age must be less than the maximum password age, unless the maximum password age is set to 0, indicating that passwords will never expire. If the maximum password age is set to 0, the minimum password age can be set to any value between 0 and 998.
<b>Minimum Password Length</b>	This security setting determines the least number of characters that a password for a user account may contain. You can set a value of between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0.  Certain Unix and Linux distributions require the minimum password length of 5 characters and will always enforce this minimum length. The enforcement of this policy may be dependent on the specific distribution of Linux or Unix you are running.

<p><b>Password Complexity</b></p>	<p>This security setting determines whether passwords must meet complexity requirements.</p> <p>If this policy is enabled, passwords must meet the following minimum requirements:</p> <ul style="list-style-type: none"> <li>• Not contain the user's account name or parts of the user's full name that exceed two consecutive characters</li> <li>• Be at least six characters in length</li> <li>• Contain characters from three of the following four categories:             <ul style="list-style-type: none"> <li>– English uppercase characters (A through Z)</li> <li>– English lowercase characters (a through z)</li> <li>– Base 10 digits (0 through 9)</li> <li>– Non-alphabetic characters (for example, !, \$, #, %)</li> </ul> </li> </ul> <p>Complexity requirements are enforced when passwords are changed or created.</p>
<p><b>Sudo</b></p>	<p>This policy specifies a <code>sudo</code> configuration file for target computers running Linux, Unix, or Mac OS X. The <code>sudo</code> configuration file is copied to the local machine and replaces the existing <code>sudo</code> file. A <code>sudo</code> file can reference local users and groups or Active Directory users and groups. Sudo, or superuser do, allows a user to run a command as root or as another user.</p>

## Authentication and Identification Policies

Group Policy	Description
<p><b>Refresh Kerberos Tickets Automatically</b></p>	<p>This policy automatically refreshes Kerberos tickets on target Linux, Unix, and 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.</p>
<p><b>Allow Offline Logon Support</b></p>	<p>This policy allows target computers running Linux, Unix, or 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>.</p>

<p><b>ID Mapping Cache Expiration Time</b></p>	<p>This policy sets the expiration time for the ID mapping cache on target Linux, Unix, and 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.</p>
<p><b>ID Mapping Negative Cache Expiration Time</b></p>	<p>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 Linux, Unix, or Mac OS X.</p>
<p><b>Winbind Cache Expiration Time</b></p>	<p>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 Unix, Linux, and 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.</p>
<p><b>Machine Account Password Expiration Time</b></p>	<p>This policy sets the machine account password's expiration time on target Unix, Linux, and Mac OS X computers. The expiration time specifies when machine account passwords are reset in Active Directory.</p>
<p><b>Depth of Nested Group Expansion</b></p>	<p>This policy sets the level of nested group expansion on target Linux, Unix, and 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.</p>

<p><b>Replacement Characters for Names with Spaces</b></p>	<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 Linux, Unix, and Mac OS X computers.</p>
<p><b>Allow Access to Samba Server Null-Password Accounts</b></p>	<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>
<p><b>Digitally Sign Client Communications</b></p>	<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>
<p><b>Digitally Sign Server Communications</b></p>	<p>This policy controls whether a server offers or requires SMB signing. The policy modifies the following file on target Linux, Unix, and 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>
<p><b>Send Encrypted Passwords to Third-Party SMB Servers</b></p>	<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>

<p><b>Set the Maximum Tolerance for Kerberos Clock Skew</b></p>	<p>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.</p> <p>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 Linux, Unix, and Mac OS X hosts.</p>
<p><b>Set the Samba Hostname Resolver Cache Timeout</b></p>	<p>This policy sets Samba's hostname cache resolver timeout on target Linux, Unix, and 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.</p>
<p><b>Set the Samba Server LDAP Connection Timeout</b></p>	<p>This policy sets the time, in seconds, that a Samba server is to wait to connect to an LDAP server before the connection fails.</p>
<p><b>Turn Off Client LANMAN Authentication</b></p>	<p>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.</p>
<p><b>Turn On Client NTLMv2 Authentication</b></p>	<p>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.</p>
<p><b>Minimum UID-GID Value</b></p>	<p>This policy specifies the minimum UID-GID value for target Linux, Unix, and Mac OS X computers. The lowest minimum value that you can set is 50; the highest minimum is 9999.</p>

## Logon Policies

Group Policy	Description
<b>Acquire Kerberos Tickets on Logon</b>	This policy acquires Kerberos tickets when a computer running Unix, Linux, or 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 a ticket in memory, leave the string value field empty.
<b>Log on Using Kerberos Authentication</b>	This policy grants target Linux, Unix, and 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 Linux, Unix, or 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 Unix, Linux, or 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 Linux, Unix, or 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.

<p><b>Show a Denied Logon Rights Message</b></p>	<p>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 Linux, Unix, and Mac OS X.</p>
<p><b>Create a Home Directory for a User Account at Logon</b></p>	<p>This policy automatically creates a home directory for a user account on target Linux, Unix, and 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.</p>
<p><b>Copy Template Files When Creating a Home Directory</b></p>	<p>This policy adds the contents of <code>skeleton</code> to the home directory created for a user account on target computers running Linux, Unix, or Mac OS X. Using the <code>skeleton</code> directory ensures that all users begin with the same settings.</p>
<p><b>File Creation Mask for the Contents of the Home Directory</b></p>	<p>This policy sets permissions for the files in the home directory that is created when a user logs on target Linux, Unix, and 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.</p>
<p><b>Log Debugging Information</b></p>	<p>This policy logs debugging information for the Likewise <code>winbind</code> daemon, <code>lwiauthd</code>, on target computers running Linux, Unix, or Mac OS X.</p>
<p><b>Show a Password Expiration Warning</b></p>	<p>This group policy sets the number of days to display a warning before a password expires on target Linux computers. Setting the number of days to 0 disables the warning. Without setting this policy, the default warning time is 5 days.</p>

## Display Policies

Group Policy	Description
<b>Display Screen Saver When a Session Is Idle</b>	This policy displays the screen saver after a session becomes idle on target computers running a version of Linux or Unix that includes Gnome desktop 2.12 or later.
<b>Lock the Screen with the Screen Saver</b>	This policy locks the screen when the screen saver appears on target computers running a version of Linux or Unix that includes Gnome desktop 2.12 or later. You can use this policy to help prevent unauthorized access to idle machines. If you do not specify the lockout interval in the policy titled Screensaver time till lockout is enforced, this policy locks the screen when screen saver becomes active.
<b>Set the Screen Saver Idle Delay</b>	This policy specifies the minutes of inactivity before the screen saver is displayed on target Unix and Linux computers that include Gnome desktop 2.12 or later.
<b>Change the Screen Saver Theme Interval</b>	This policy sets the interval when the screen saver's theme changes on target Unix or Linux computers that include Gnome desktop 2.12 or later.
<b>Set the Screen Lockout Interval</b>	This policy sets the lockout interval for the Lock the Screen with the Screen Saver group policy. You can use this policy on target computers running a version of Linux or Unix that includes Gnome desktop 2.12 or later.
<b>Display a Keyboard in the Screen Saver</b>	This policy displays a virtual keyboard in the screen saver on target Linux and Unix computers that include Gnome desktop 2.12 or later. You can use this policy to help a user with limited dexterity unlock a computer. You can also use this policy for kiosk installations that have a touch screen and no keyboard.
<b>Embed a Keyboard Command in the Screen Saver</b>	This policy embeds a keyboard command in the screen saver on target computers running a version of Linux or Unix that includes Gnome desktop 2.12 or later. You can use the embedded keyboard command for kiosk installations that have a touch screen and no keyboard. The command that you associate with this policy must implement an XEmbed plug interface and output a window XID on the standard output.
<b>Show a Screen Saver Logout Option</b>	This policy shows a logout option in the screen saver's unlock dialog on target computers running a version of Linux or Unix that includes Gnome desktop 2.12 or later.

<b>Screen Saver Time till the Logout Option Is Available</b>	This policy sets a delay before the logout option becomes available in the unlock dialog on target Unix and Linux computers that include Gnome desktop 2.12 or later. For this policy to work, you must define the Show Screensaver Logout Option group policy.
<b>Run a Logout Command from the Screen Saver Dialog</b>	This policy runs a command when a user logs out from the screen saver's dialog on target computers running a version of Linux or Unix that includes Gnome desktop 2.12 or later. It is recommended that you use this command only to log the user out without any other interaction.
<b>Show a Switch User Option with the Screen Saver</b>	This policy displays an option to switch user in the screen saver's unlock dialog on target computers running a version of Linux or Unix that includes Gnome desktop 2.12 or later.

### 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 Linux, Unix, or 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> (on Unix) or <code>agetty</code> (on Linux) 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 Linux, Unix, or Mac OS X. The message of the day, which appears after a user logs in but before the <code>logon</code> 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>SELinux</b>	This policy creates a Security-Enhanced Linux group policy for target computers running Red Hat Enterprise Linux. The policy applies your settings to the <code>/etc/sysconfig/selinux</code> file on target computers.
<b>AppArmor</b>	This policy specifies an AppArmor security profile for target computers that are running SUSE Linux Enterprise. An AppArmor security profile defines the system resources and privileges that an application can use.
<b>SysLog</b>	This policy creates a syslog for target computers running Unix, Linux, or 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 Unix, Linux, and 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 <code>nfs</code> , <code>samba</code> , and <code>boot mounts/partitions</code> .

<b>File System Mounts (fstab)</b>	<p>This policy adds mount entries to the file systems table, or <code>fstab</code>, on target computers running Unix or Linux (but not Mac OS X). You can add the following kinds of file systems to <code>fstab</code>: Common Internet File System (cifs); Linux Native File System (ext2); New Linux Native File System (ext3); ISO9660 CD-ROM (iso9660); Network File System (NFS); Network File System version 4 (NFS4).</p>
-----------------------------------	---

## Task Policies

Group Policy	Description
<b>Run a Script File</b>	<p>The script policy lets you specify a text-based script file to execute on Unix or Linux 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.</p>
<b>Crontab/cron.d</b>	<p>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:</p> <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> <p>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.</p>

## Macintosh Policies

The group 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.

<p><b>Use Firewall Stealth Mode</b></p>	<p>This policy sets the built-in firewall on target computers running Mac OS X to operate in stealth mode.</p> <p>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.</p>
<p><b>Use Secure Virtual Memory</b></p>	<p>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.</p>
<p><b>Make AppleTalk Active</b></p>	<p>This policy makes AppleTalk active on target Mac OS X computers. You can also use this policy to make AppleTalk inactive.</p>
<p><b>Set DNS Servers and Search Domains</b></p>	<p>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.</p>

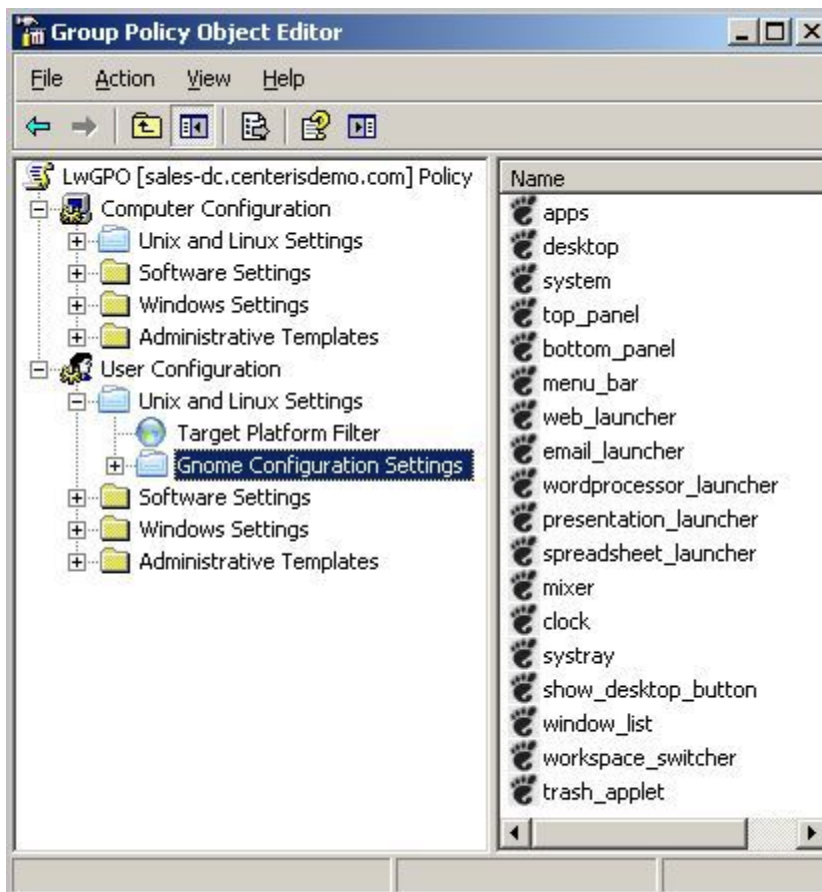
### User Policies for Gnome Desktops

Likewise lets you set group policies for Linux user settings -- policies based on the Gnome GConf project to define desktop and application preferences such as the default web browser.

There are several thousand Gnome-based group policies. They include user settings for applications like the browser, help viewer, and main menu. They also include settings for tailoring the keyboard for accessibility, specifying URL handlers, and configuring volume manager. For example, you can set a user policy to define whether the Gnome volume manager automatically mounts removable storage drives when they are inserted into a computer.

Likewise comes with schemas in ZIP file format for a number of common platforms, including Fedora, Red Hat, Debian, CentOS, Ubuntu, and several versions of SUSE. If the schemas for your target platform are not included with Likewise, you can copy them from your Linux platform to a location that you can access from a Windows administrative desktop that runs the Likewise Console.

To set the policies, you use the Group Policy Object Editor. After you add the Gnome schemas for your Linux platform, the policies appear in the Unix and Linux User Settings folder under User Configuration:



### Filtering Group Policies by Target Platform

You can set Likewise's Unix and Linux group policies to target all versions of the following platforms. Some group policies apply only to specific platforms.

- Apple Mac OS X
- CentOS Linux
- Debian Linux
- Fedora Linux
- Hewlett-Packard HP-UX
- IBM AIX
- OpenSUSE Linux
- Red Hat Linux

- Red Hat Enterprise Linux (ES and AS)
- Sun Solaris
- SUSE Linux
- SUSE Linux Enterprise Desktop
- SUSE Linux Enterprise Server
- Ubuntu Linux

### 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 Linux, Unix, and Mac OS X policies. For example, you can view a report that shows the settings for a Likewise group policy. Here's an example:

