## Contents

<table>
<thead>
<tr>
<th>Preface</th>
<th>7</th>
<th>Document Revision History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>15</td>
<td>The Common Criteria Configuration</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>About Common Criteria</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>Assumptions About the Environment of the Configuration</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>Assumptions About the Usage of the Common Criteria Configuration</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>How to Use This Guide</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>Best Practices</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>Getting Additional Information</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>19</td>
<td>Installing Common Criteria with Mac OS X or Mac OS X Server</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>Installing the Evaluated Configuration of Mac OS X</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Installing the Evaluated Configuration of Mac OS X Server</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>23</td>
<td>Setting Up the Common Criteria Configuration</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Set Up System Preferences</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Disable Software Update</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>Screen Saver</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>CDs &amp; DVDs</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>Sharing</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>Accounts</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>Date &amp; Time</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Energy Saver</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Airport</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Do this task for both Mac OS X and Mac OS X Server.</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Bluetooth</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Do this task for both Mac OS X and Mac OS X Server.</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Restore LOM Factory Defaults</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>System Setup</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>Directory Access</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>IMAP and POP3 Mail Servers</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>Set an Open Firmware Password</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>Turn On Auditing</td>
</tr>
<tr>
<td>Page</td>
<td>Content</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>Audit Classes, Audit Events, and User Masks</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>Command-Line Programs</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>audit</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>auditreduce</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>praudit</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>Managing Audit Log Files</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Deleting Audit Records</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>Audit Control Files</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>audit_class</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>audit_control</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>audit_event</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>audit_user</td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>audit_warn</td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>Audit Log Files</td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>Appendix A  Mac OS X Audit Event Classes</td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>Appendix B  Audit Record Format</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>Appendix C  Using Terminal</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>Notation Conventions</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>Summary</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>Commands and Other Terminal Text</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>Command Parameters and Options</td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>Using Terminal</td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>Correcting Typing Errors</td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>Repeating Commands</td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>Including Paths Using Drag-and-Drop</td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>Commands Requiring Root or Administrator Privileges</td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>Editing Settings Files</td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>Getting Online Help for Commands</td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>Manpage General Info</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>Appendix D  notify Configuration File</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>notify Configuration File</td>
<td></td>
</tr>
</tbody>
</table>
### Document Revision History

This table describes revisions to the Common Criteria Administration Guide.

<table>
<thead>
<tr>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
</table>
| April 2, 2005   | • Modified instructions for setting the global umask to account for differences in certain Panther configurations. This command has been added to pages 32 and 75: `sudo chmod 644 /Library/Preferences/.GlobalPreferences.plist`
<p>|                 | • Added change history page.                                                               |
| November 5, 2008| • Changed version on title page                                                             |
|                 | • Copyright page, changed references to Apple Computer Inc. to Apple Inc.                  |
|                 | • Changed year to 2008                                                                     |
| November 5, 2008| • How to use this guide: Directions added to download evaluated version of cc guide from security website.|
|                 | • How to use this guide: added directions for user to get software from a secure site.    |
|                 | • In Chapter 1 Common Criteria Configuration:                                              |
|                 | • Changed version of Mac OS X to 10.6                                                     |
|                 | • Removed mention of other versions.                                                      |
|                 | • Changed version of OS from Leopard to Snow Leopard.                                     |
|                 | • Added English only comment to chapter 1 About Common Criteria                            |
|                 | • added new configurations, MacBook, MacBook Pro, Mac Pro, Mac Mini, mention Intel processors.|
|                 | • Removed mention of PPC processors                                                       |
| November 5, 2008| • In Assumptions about the Environment                                                     |
|                 | • mention secured protocols ssh 2.0                                                        |
|                 | • In Assumptions about the Usage of the Common Criteria configuration.                     |
|                 | • Added UTRAIN requirement                                                                 |
|                 | • Added UTRUST requirement                                                                  |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
</table>
| November 5, 2008 | • In How to Use this Guide  
  • Added comment that CCGuide must be downloaded from secure apple site  
  • In Getting Additional Information  
  • Updated configuration information to SnowLeopard, and version to 10.6. removed other configurations.  
  • Added comment to report security flaws.  
  • In Chapter 2 Installing Common Criteria  
    • Updated configuration information to SnowLeopard, and version to 10.6. removed other configurations.  
    • In Installing the latest version of Mac OS X: Updated configuration information to SnowLeopard, and version to 10.6. removed other configurations.  
    • Changed direction for users to “Type” to “Enter.”  
    • Changed Journaled to Journaling.  
    • Removed instructions to install update to the evaluated configuration since no update is needed.  
    • Added comments that software must be downloaded from secure server.  
    • Deleted steps for installing Common Criteria tools since tools are included in SnowLeopard.  
  • In Chapter 3 Setting Up the Common Criteria Configuration  
    • changed Security preferences to include firewall settings  
    • In Sharing edited steps to match interface changes  
    • In Accounts, edited steps to match interface changes  
    • In energy saver added step to click options.  
    • In firmware Password application, update the URL  
    • In Set Password Policy, edited command to add a space  
    • In umask edited first step  
    • In Configure secure shell, added a configuration  
    • Removed references to Classic  
    • Changed terminal command to sshd_config file.  
  • In Chapter 4, Changing Groups, edited man statement  
  • In Chapter 5, in Adding a new User Account  
    • edited steps to clarify user's name  
    • In Deleting a User Account, edited intro for clarification  
    • Edited step 4  
  • In Chapter 6 Adding a user via the Command Line step 1 reformatted and edited command examples  
    • Deleted appendix D and E  
  • January 30, 2009  
    • In Chapter 1 Added Best Practices section  
    • In Chapter 2, removed Latest version update instructions since they don't apply.  
    • In Chapter 5, added Limiting su Rights to only Admin Users  
    • changed http: to https: for apple support urls
<table>
<thead>
<tr>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 30, 2009</td>
<td>• In Chapter 1, clarified explanation of the evaluated configuration</td>
</tr>
<tr>
<td></td>
<td>• removed mention of the Common Criteria tools</td>
</tr>
<tr>
<td></td>
<td>• Removed statement that some versions of the OS have CC tools.</td>
</tr>
<tr>
<td></td>
<td>• In Assumptions about the Usage of CC Added exact text from</td>
</tr>
<tr>
<td></td>
<td>UTRAIN, and UTRUST.</td>
</tr>
<tr>
<td></td>
<td>• In How to Use this guide Added comment that the CC guide</td>
</tr>
<tr>
<td></td>
<td>must be download from the secure apple website</td>
</tr>
<tr>
<td></td>
<td>• In Best Practices added statement about 3rd party browsers</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>January 30, 2009</td>
<td>• In Chapter 2, Removed Common Criteria Tools installation steps</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>January 30, 2009</td>
<td>• In Chapter 3, Changed password policy to current</td>
</tr>
<tr>
<td></td>
<td>• Updated Open Firmware information</td>
</tr>
<tr>
<td></td>
<td>• Updated Configure Secure Shell information</td>
</tr>
<tr>
<td></td>
<td>• In Choosing secure passwords, updated info to current policy</td>
</tr>
<tr>
<td></td>
<td>• In Admin, updated directories to match current.</td>
</tr>
<tr>
<td></td>
<td>• Updated audit procedures</td>
</tr>
<tr>
<td>January 30, 2009</td>
<td>• Deleted checklist appendix</td>
</tr>
<tr>
<td>February 23, 2009</td>
<td>• Added new content to Turn ON Auditing</td>
</tr>
<tr>
<td></td>
<td>• Added EFI information to Firmware password</td>
</tr>
<tr>
<td></td>
<td>• Globally updated any outdated apple support URLs</td>
</tr>
<tr>
<td></td>
<td>• changed all apple support <a href="http://support.apple.com">http://support.apple.com</a> to https://</td>
</tr>
<tr>
<td></td>
<td>support.apple.com</td>
</tr>
<tr>
<td></td>
<td>• Added the word &quot;(UTRAIN)&quot;and (UTRUST) to the previously added</td>
</tr>
<tr>
<td></td>
<td>direct quotes from the Security Framework, so the can be searched</td>
</tr>
<tr>
<td></td>
<td>on utrain, and utrust.</td>
</tr>
<tr>
<td></td>
<td>• Replaced if sudo... with if root account...</td>
</tr>
<tr>
<td></td>
<td>• Updated version numbers</td>
</tr>
<tr>
<td></td>
<td>• Update 019 number</td>
</tr>
<tr>
<td>June 17, 2009</td>
<td>• Updated instances of nicl to dscl on pages 46, 51, 52 per radar</td>
</tr>
<tr>
<td></td>
<td>bug: <a href="">rdar://problem/6881163</a> Common Criteria: Replace all</td>
</tr>
<tr>
<td></td>
<td>references to Netinfo with Directory Services in the guide</td>
</tr>
<tr>
<td>June 23, 2009</td>
<td>• Changed all comments &quot;10.6 or later &quot; to just 10.6</td>
</tr>
<tr>
<td></td>
<td>• Synced evaluated hardware with Security target 1.5.4.2 page, 12</td>
</tr>
<tr>
<td></td>
<td>• removed reference to DVD-Rom to match Security Target 1.5.4.2</td>
</tr>
<tr>
<td></td>
<td>• Under Assumptions About the Environment of the Configuration</td>
</tr>
<tr>
<td></td>
<td>added: The processing resources of the TOE will be located within</td>
</tr>
<tr>
<td></td>
<td>controlled access facilities which will prevent unauthorized</td>
</tr>
<tr>
<td></td>
<td>physical access. - The TOE hardware and software critical to</td>
</tr>
<tr>
<td></td>
<td>security policy enforcement will be protected from unauthorized</td>
</tr>
<tr>
<td></td>
<td>physical modification.</td>
</tr>
<tr>
<td></td>
<td>• Added comment to Assumptions about the usage of the CCC</td>
</tr>
<tr>
<td></td>
<td>users are trained to protect the data belonging to them.</td>
</tr>
<tr>
<td>Date</td>
<td>Notes</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| June 24, 2009 | • added with “Security Target”  
• Deleted UTRAIN  
• Deleted UTRUST sentence  
• How to use this Guide: Changed url to https://www.apple.com/support/security/commoncriteria  
• Best Practices: added word “recommended”  
• Getting Additional Information... deleted period in url  
• deleted AFP FTP, and SMBCFS  
• added Atsec Information Security  
• changed url to http://www.atsec.com/01/company-certifications.html  
• Changed to "Federal Office for Information Security (BSI)"  
• Changed url to http://www.bsi.de/english/department3.htm  
• Installing CC added info on Common Criteria tools.  
• ‘Added “Set Password Policy” cross reference  
• Installing the Evaluated Configuration on Mac OSX Server  
• added info on Common Criteria tools  
• Changed to "do not select any services. Clear all checkboxes."  
• Setup System Preferences Added Click the "Show All" button and click Accounts  
• Accounts: "Show fast user switching menu as"  
• energy saver: Replaced with “Start up automatically after a power failure”  
• Managing Audit Log Files moved to chapter 6  
• Set Password Policy deleted.  
• Added Abstract Machine Test Utility  
• Changed Audit Startup to “Turn On Auditing”  
• Deleted Modifying the Audit system                                                                                                                                                                                                                                                                                                                                                     |
| June 25, 2009 | If the settings are dimmed, click the lock icon and enter an administrator name and password.  
Select Off from the “Automatic login” pop-up menu. Click the Firewall tab.  
If the firewall is off, click on the Start button to turn on the firewall"  
Added lick on the Advanced button and then select "Block All Incoming Connections".  
This will block all incoming connections except those required for basic Internet services, such as DHCP, Bonjour, and IPSec.  
• Verify that "Automatically allow signed software to receive incoming connections" is checked.                                                                                                                                                                                                                                                                                                                                 |
<table>
<thead>
<tr>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
</table>
| June 26, 2009   | • Added Airport section  
• Added Bluetooth section  
• Added Disable IMAP and POP3 section  
• edited for "Network Account Server  
• deleted references to Classic.  
• Moved Turn on Auditing to Chapter 6  
• Disable Password Hints: changed command to "sudo defaults write /Library/Preferences/com.apple.loginwindow RetriesUntilHint 0"  
• Set Password Policy: Removed sentence:  
• Configure Secure Shell- Replace with "to either accept passwords or public key authentication only."  
• Added "Ciphers"  
• Added Using Terminal section  
• Added sections on Software and Configurations from Security Target 1.5.4.1.2 and 1.5.4.3  
• Using Passwords in Mac OS X added: TOE procedures  
• Choosing Secure Passwords: added must  
• Setting the umask... "To set the umask for files you create as the logged-on user"  
• "The lowest umask value that any user should use is 002. A higher umask value can be chosen, but a lower number allows other users to modify the data." |
| July 15, 2009   | • Replace all references to 'TOE' with "The Common Criteria Evaluated Configuration"  
• Add a new appendix at the end of this doc containing the content of the notify.conf(5) man page file  
• Updated copyright to 2009  
• The Common Criteria Configuration: added default installation  
• added Intel Pentium and Xeon-based processors with the EM64T extension  
• Changed DVD drive, from "CD-ROM drive".  
• Removed references to the Security Target, |
| July 24, 2009   | • How to use this guide: "The Common Criteria evaluated configuration consists of the default installation of Mac OS X version 10.6 and Mac OS X server version 10.6.  
• add some information about identifying that the DVDs received are the correct OS and that the package has not been tampered with.  
• Deleted information on Common Criteria tools  
• Deleted information on verifying disk images |
<table>
<thead>
<tr>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
</table>
| July 30, 2009 | • Added The evaluated configuration includes only the default packages; do not install any additional packages during installation.  
• Rewrote steps for installing Mac OS X Server.  
• Deleted firewall tab references.  
• Added Mac OS Server info to Screen Saver.  
• Deleted step 3 or Energy Saver  
• Added Bluetooth setting for Mac OS X server  
• Rewrote steps for Password hints  
• Changed password policy command to `pwpolicy -n /Local/Default -n adminusername -setglobalpolicy MinChars=8 requiresAlpha=1 requiresNumeric=1 usingHistory=5 maxFailedLoginAttempts=5 maxMinutesUntilChangePassword=129600`  
• Configure Secure Shell, changed setting PublicKeyAuthentication to Yes  
• Software added The evaluated configuration is a subset of the software packages contained on the DVDs for the distributed Mac OS X product, consisting of only the packages installed during default installation of MAC OS X version 10.6 or MAC OS X Server version 10.6.  
• configurations Added The automated password quality checking mechanism is configured  
• Added also: For SSH, the "none" cipher (no encryption), and the "none" keyed hash function (no HMAC) are not allowed in the evaluated configuration."  
• Turning Auditing on Deleted.  
• Added statement Auditing is turned on by default so there are no further steps to take to turn on auditing. Audit logs are rotated automatically by the auditd daemon. The auditd daemon is launched by launchd on demand. |
| August 10, 2009 | • Removed reference to CAPP on pg 14  
• Edited paragraph pg 14  
• Edited heading pg 14  
• Fixed typo ar on page 15  
• Edited and removed link on page 15  
• Added information on correct apple dvd, pg 17  
• edited cross reference pg 17 |
| August 24, 2009 | • Added key information on page 29 |
| August 31, 2009 | • Changed globally system version to Mac OS X 10.6 (Snow Leopard)  
• Added generic hints as a section in the Using Terminal Appendix C.  
• Set up System preferences, edited step 4.  
• Detected step 6-8  
• Disable software updated, deleted step 3.  
• Accountst step 5, added If not already selected.  
• Added Retore LOM Factory Defaults section  
• Changed command for Setting password police  
• added section Disable System Services with terminal commands. |
<table>
<thead>
<tr>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 15, 2009</td>
<td>• deleted pubkeyAuthentication information on page 31, Configure Secure Shell</td>
</tr>
</tbody>
</table>
On copyright page:  
Updated version to 2.1  
changed date to 09-21-2009  

•
This guide provides the information needed to set up, use, and administer Mac OS X and Mac OS X Server in compliance with the Common Criteria specification.

About Common Criteria

Common Criteria is an international standard that helps to ensure the security of computer systems in a network environment. You can optimize the security of your network by bringing each system into conformance with the standard defined by Common Criteria. To do so you must ensure that the hardware and software settings of each system match the specific configuration evaluated and certified as secure by the Common Criteria specification. The Common Criteria evaluation for Mac OS X and Mac OS X Server was performed with a configuration referred to in this document as the evaluated configuration. A Mac OS X operating system running and tested on the hardware and firmware in the evaluated configuration is referred to as the Common Criteria Evaluated Configuration.

The evaluated configuration consists of:
• Mac OS X 10.6 (Snow Leopard) or Mac OS X Server 10.6 (Snow Leopard) default installation (without selecting any additional packages during the installation) on any of the following computers: iMac, MacBook, or MacBook Pro, Mac Mini, or Mac Pro, with Intel Pentium and Xeon-based processors with the EM64T extension.

Note: Do not install any operating system other than Mac OS X or Mac OS X Server on the Common Criteria configuration.

The Common Criteria configuration refers to the English Language version of Mac OS X only.
The Common Criteria configuration includes one or more of the above computers connected to a local network via Ethernet. It can also include connected peripheral devices including the following:

- Display monitor
- Keyboard
- Mouse
- DVD drive
- Fixed disk drives
- Printer
- Audio Adapter
- Network Adapter

Assumptions About the Environment of the Configuration

Several assumptions are made about the physical environment of the Common Criteria configuration.

- The processing resources of the Common Criteria Evaluated Configuration will be located within controlled access facilities which will prevent unauthorized physical access. The hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- All systems with which the Common Criteria Evaluated Configuration communicates, and the communication paths themselves, are assumed to be under the same management as the Common Criteria configuration and abide by the same security policies.
- All connections to peripheral devices and all network connections not using the secured protocols SSH v2.0 reside within the controlled access facilities. The Common Criteria Evaluated Configurations only address security concerns related to the manipulation of the Common Criteria Evaluated Configuration through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.

Assumptions About the Usage of the Common Criteria Configuration

The Common Criteria configuration is assured to provide effective security measures in a cooperative, non-hostile environment only if it is installed, managed, and used in accordance with the instructions in this guide. The following conditions are assumed to exist in the environment where the Common Criteria configuration is employed:

- There will be one or more competent individuals assigned to manage the Common Criteria configuration and the security of the information it contains.
- Users are trained to protect the data belonging to them.
• The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided in this guide.
• Authorized users possess the necessary authorization to access at least some of the information managed by the Common Criteria configuration and are expected to act in a manner that contributes to the security of the environment and the information it contains.
• Users are trained to use the security functionality provided by the system appropriately.
• Users are trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their data.

How to Use This Guide
The information in this guide supersedes related information in other Mac OS X and Mac OS X Server documentation. If there is any discrepancy between the information in this guide and related information in other documentation, the information provided in this guide takes precedence in regards to addressing the requirements of the Common Criteria evaluated configuration.

Be sure you are using the most recent version of this guide, and that is has been acquired from the secure site at:
https://www.apple.com/support/security/commoncriteria/

To use the Common Criteria configuration, you must install the required software and set up the software according to the Common Criteria specification to achieve the evaluated configuration. The Common Criteria evaluated configuration consists of the default installation of Mac OS X 10.6 (Snow Leopard) and Mac OS X server 10.6 (Snow Leopard). See Chapters 2 and 3 for instructions.

Next, see Chapter 4 for information on using your systems in a safe and secure way.

Finally, Chapters 5 and 6 have information on administering the Common Criteria configuration, including instructions for using the command line to do management tasks.

Best Practices
Due to the security challenges presented by internet applications such as browsers, and to maintain a known configuration and prevent the execution of unevaluated 3rd party code, use of non-Apple-supplied web browsers is not recommended. In addition, Safari should be updated regularly to insure it is provided with the most current security updates.
Getting Additional Information

Mac OS X and Mac OS X Server come with guides that explain their features and provide instructions on configuring, managing, and troubleshooting them. All of the guides are available as PDF files from https://www.apple.com/support/

<table>
<thead>
<tr>
<th>This guide</th>
<th>Tells you how to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac OS X v10.6 Snow Leopard Installation and Setup Guide</td>
<td>Install and set up Mac OS X.</td>
</tr>
<tr>
<td>Mac OS X Server Getting Started Version 10.6 Snow Leopard</td>
<td>Get to know the features of Mac OS X Server and do initial setup.</td>
</tr>
<tr>
<td>Mac OS X Server User Management Version 10.6 Snow Leopard</td>
<td>Create and manage user, group, and computer accounts and set up managed preferences and Mac OS X clients.</td>
</tr>
<tr>
<td>Mac OS X Server File Server Administration Version 10.6 Snow Leopard</td>
<td>Share selected server volumes or folders among server clients using NFS protocols.</td>
</tr>
<tr>
<td>Mac OS X Server Web Technologies Administration Version 10.6 Snow Leopard</td>
<td>Set up and manage a web server, including WebDAV, WebMail, and web modules.</td>
</tr>
<tr>
<td>Mac OS X Server Network Services Administration Version 10.6 Snow Leopard</td>
<td>Set up, configure, and administer services on the server.</td>
</tr>
<tr>
<td>Mac OS X Server Open Directory Administration Version 10.6 Snow Leopard</td>
<td>Manage directory and authentication services.</td>
</tr>
<tr>
<td>Mac OS X Server Introduction to Command-Line Administration Version 10.6 Snow Leopard</td>
<td>Use commands and configuration files to perform server administration tasks in a UNIX command shell. Using IP failover is documented in this guide.</td>
</tr>
</tbody>
</table>

Additional information is available at these locations on the web:

- **Apple Security Website:**
  https://www.apple.com/support/security/

- **Atsec Information Security evaluation lab website:**
  http://www.atsec.com
  http://www.atsec.com/01/atsec-resources-and-faq-for-it-standards.html#r1

- **Federal Office for Information Security (BSI) website:**
  http://www.bsi.de/english/department3.htm

- **Apple Documentation**
  https://www.apple.com/support/

To report security flaws or subscribe to the security-announce mailing list to receive notifications about product security:

- **Apple Security Website:**
  https://www.apple.com/support/security/
Installing Common Criteria with Mac OS X or Mac OS X Server

This chapter describes how to install the software needed to operate a Macintosh computer in the Common Criteria evaluated configuration.

To get started setting up the Common Criteria evaluated configuration you must use only an official copy of Mac OS X 10.6 (Snow Leopard) or Mac OS X Server 10.6 (Snow Leopard) DVD delivered directly from Apple. The packaging must be unopened and the DVD marked with the Apple logo. The DVD must be labeled with the version Mac OS X10.6 (Snow Leopard) or Mac OS X Server 10.6 (Snow Leopard).

Installing the Evaluated Configuration of Mac OS X

The instructions in this section tell you how to install the specific version of Mac OS X 10.6 (Snow Leopard) used to certify the evaluated configuration. No additional updates are needed and any additional updates will depart from the Common Criteria Evaluated Configuration. For more information on the evaluated configuration, see “About Common Criteria” on page 15.

What You Need

You need the following installation disks to install the specific version of Mac OS X used to certify the evaluated configuration:

- Mac OS X 10.6 (Snow Leopard) installation disks
  You need the Mac OS X 10.6 (Snow Leopard) installation disks. You must use only official Apple disks, purchased from Apple, and marked with the Apple logo. If your computer shipped with Mac OS X 10.6 (Snow Leopard) you can use the installation disks that came with your system.

Step 1: Install Mac OS X 10.6 (Snow Leopard)

Use the installation discs for Mac OS X 10.6 (Snow Leopard) to install the software.

To install Mac OS X:

1. Turn on the computer and insert the first Mac OS X install disc.
2. Restart the computer while holding down the C key.
The computer starts up from the install disc. You can release the C key when you see the Apple logo.

3 Proceed through the Installer panes, following the onscreen instructions. The evaluated configuration includes only the default packages; do not install any additional packages during installation.

4 When the Select Destination pane appears, select the volume where you want to install Mac OS X.

5 Click Options, then click Erase and Install.

   The destination volume will be completely erased before Mac OS X is installed on it.

6 Choose Mac OS Extended (Journaled) from the “Format disk as:” pop-up menu.

7 The installer displays progress information and automatically restarts the computer during installation. Insert the next installation disc when prompted.

Step 2: Perform initial setup using Setup Assistant

The Setup Assistant program opens automatically after you install Mac OS X 10.6 (Snow Leopard). Setup Assistant leads you through an initial setup process by displaying settings and instructions in a sequence of panes.

When you are prompted for a password, be sure to choose a secure password. During the initial installation of Mac OS X no password quality rules have been defined by default. Therefore initial password must be carefully chosen to at least meet the minimum password policy, which will be configured later. For more information on choosing secure passwords, see, “Choosing Secure Passwords” on page 34.

When setup is complete, the computer restarts automatically. Now you can log in as the administrator user created during setup and continue with the next step.

Installing the Evaluated Configuration of Mac OS X Server

The instructions in this section tell you how to install the specific version of Mac OS X Server 10.6 (Snow Leopard) used to certify the evaluated configuration. For more information on the evaluated configuration, see, “About Common Criteria” on page 15.

Note: The instructions in this section cover installing on a server that, at least for the duration of the installation process, has a keyboard and display attached and has an optical drive (internal or external). It is possible to install the software on a server that does not have a keyboard, display, or optical drive. For information on installing software remotely from an administrator computer, see the getting started guide included with Mac OS X Server 10.6 (Snow Leopard).

What You Need

You need the following installation software to install the specific version of Mac OS X Server used to certify the evaluated configuration:
• **Installation discs for Mac OS X Server 10.6 (Snow Leopard).**
  Use the installation discs included with your Xserve system or with your copy of Mac OS X Server.

  **Note:** If your installation discs are for a version of Mac OS X Server earlier than 10.6 (Snow Leopard), you must obtain Mac OS X Server 10.6 (Snow Leopard).

**Step 1: Install Mac OS X Server 10.6 (Snow Leopard)**
Use the installation discs for Mac OS X Server 10.6 (Snow Leopard) to install the server software.

To install Mac OS X Server:

1. Turn on the computer and insert the first Mac OS X Server install disc.
2. Restart the computer while holding down the C key.
   The computer starts up from the install disc. You can release the C key when you see the Apple logo.
3. Proceed through the Installer's panes by following the onscreen instructions. The evaluated configuration includes only the default packages. Do not install any additional packages during installation.
4. When the Install Mac OS X Server pane appears, choose Utilities > Disk Utility.
5. In the list of volumes, select the volume on which you want to install Mac OS X Server, and then click Erase.
6. Choose Mac OS Extended (Journaled) from the Format pop-up menu.
7. Enter a volume name in the Name field, if needed, and then click, Erase.
8. When the volume has been erased, choose Disk Utility > Quit Disk Utility.
9. When the Install Mac OS X Server pane appears, click Continue follow the onscreen instructions.
10. When the Select Destination pane appears, select the volume where you want to install Mac OS X Server and click Install.
11. The installer displays progress information and automatically restarts the computer during installation. Insert the next installation disc if you are prompted to do so.
12. Follow the instructions provided to set up Mac OS X Server. When you get to the “Transfer an Existing Server” pane, select Set up a new server.

**Step 2: Perform initial server setup using Server Assistant**
The Server Assistant program opens automatically after you install Mac OS X Server. Server Assistant leads you through an initial setup process by displaying settings and instructions in a sequence of panes.
To set up Mac OS X Server:

1. Before configuring settings in Server Assistant’s panes, fill out the Mac OS X Server worksheet.

   The worksheet and supplemental information you need is in the getting started guide that’s included with Mac OS X Server 10.6 (Snow Leopard). You can also obtain the worksheet and getting started guide from the Mac OS X Server website at the following address:
   https://www.apple.com/server/resources/

2. Start up your computer if it is off, and Server Assistant opens automatically.

3. Enter the setup data you’ve recorded on the worksheet as you move through Server Assistant’s panes, following the onscreen instructions.

   Make sure that any DHCP or DNS servers you specify for the server you’re setting up to use are running.

4. When you reach the Administrator Account pane, specify a password. During the initial installation of Mac OS X Server no password quality rules have been defined by default. Therefore initial password must be carefully chosen to at least meet the minimum password policy, which will be configured later. For more information on choosing secure passwords, see, “Choosing Secure Passwords” on page 34.

5. When you reach the Services pane, deselect all services.

6. When you reach the Network Defaults, select Users and Groups.

7. After all setup data has been entered, Server Assistant displays a summary of the data.

8. Review the setup data you entered. Click Go Back if you want to change any of the settings.

9. To initiate server setup, click Apply.

   When server setup is complete, the server restarts automatically. Now you can log in as the administrator user created during setup and continue with the next step.
Setting Up the Common Criteria Configuration

This chapter describes the steps required to set up the Common Criteria configuration.

The tasks you do depend on whether you’re setting up the Common Criteria configuration on Mac OS X or Mac OS X Server. For each task, you’re told whether you need to complete part of all of it depending on the operating system you setting up.

To set up the Common Criteria configuration, log in as an administrator and do the following tasks:

Set Up System Preferences

Security
For Mac OS X do the whole task. For Mac OS X Server do all except step 5.
1 Open System Preferences and click Security.
2 Click the General tab.
3 If the settings are dimmed, click the lock icon and enter an administrator name and password.
4 Select the “Require a password immediately after sleep or screen saver begins” checkbox, and choose immediately from the pop-up menu.
5 Select the “Require password to unlock each Secure System preferences pane” checkbox.

Note: Skip this step if you’re setting up Mac OS X Server. This option is not available on Mac OS X Server.

Disable Software Update
Do this task for both Mac OS X and Mac OS X Server.
1 Open System Preferences and click Software Update.
2 Deselect “Check for updates.”
Screen Saver
Do this task for both Mac OS X and Mac OS X Server.
1. Open System Preferences and click Desktop & Screen Saver.
2. Click the Screen Saver button.
3. Select a screen saver in the list, or select the "Use random screen saver" checkbox to see a different screen saver each time the screen saver is activated.
4. Drag the “Start screen saver” slider to choose when the screen saver starts. To insure security, the screensaver time should be set to 15 minutes or less, based on your organizational policy.

CDs & DVDs
Do this task for both Mac OS X and Mac OS X Server.
1. Open System Preferences and click CDs & DVDs.
2. Choose Ignore from the "When you insert a music CD” pop-up menu.
3. Choose Ignore from the "When you insert a picture CD” pop-up menu.
4. Choose Ignore from the "When you insert a video DVD” pop-up menu.

Sharing
1. Open System Preferences and click Sharing.
2. If settings are dimmed, click the lock icon and enter an administrator name and password.
3. Turn on the Remote Login service by selecting its checkbox, and then turn off all other services in the list.

Accounts
Do this task for both Mac OS X and Mac OS X Server.
1. Open System Preferences and click Accounts.
2. If settings are dimmed, click the lock icon and enter an administrator name and password.
3. Click Login Options.
4. Choose Off, from the “Automatic login” pop-up menu.”
5. In the “Display login window as” section, select the “Name and password” button if not already selected and not grayed out.
6. Deselect the “Show the Restart, Sleep, and Shut Down buttons” checkbox.
7. Deselect the “Show fast user switching menu as” checkbox.

Date & Time
Do this task for both Mac OS X and Mac OS X Server.
Date & Time preferences should be set to use a network time server to ensure correct time entries in the audit log.
Note: If you correctly configured your computer to use a network time server during setup, you don't need to perform this step.

To set Date & Time preferences to the Common Criteria configuration:
1. Open System Preferences and click Date & Time.
2. If settings are dimmed, click the lock icon and enter an administrator name and password.
3. Select the "Set Date & Time automatically" checkbox. Then enter the fully qualified DNS name or IP address of the network time server for your network.

Energy Saver
Do this task for Mac OS X Server only.
1. Open System Preferences and click Energy Saver.
2. If settings are dimmed, click the lock icon and enter an administrator name and password.
3. Deselect the “Start up automatically after a power failure” checkbox.

Airport
Do this task for both Mac OS X and Mac OS X Server.
Airport should be disabled.
1. Open System Preferences and click Network.
2. If settings are dimmed, click the lock icon and enter an administrator name and password.
3. Select Airport.
4. Click “Turn Airport off.”

Bluetooth
Do this task for both Mac OS X and Mac OS X Server.
Bluetooth should be disabled.
1. Open System Preferences and click Bluetooth.
2. Deselect the Bluetooth On checkbox.

Restore LOM Factory Defaults
Do this task for Mac OS X Server only, and only if the Server Monitor is monitoring servers.
1. Open /Applications/Server/Server Monitor.
2. Select server from the list.
4. Select “Restore LOM Factory Defaults.”
System Setup

Directory Access
Do this task for both Mac OS X and Mac OS X Server.
1 Open Systems Preferences and click Accounts.
2 If settings are dimmed, click the lock icon and enter an administrator name and password.
3 Click Login Options.
4 In the “Network Account Server” section, click the Join or Edit button.
5 Click the “Open Directory Utility.”
6 If settings are dimmed, click the lock icon and enter an administrator name and password.
7 Click Services and turn off all items in list that are not dimmed.
8 Click Apply.

IMAP and POP3 Mail Servers
Do this task for Mac OS X Server if the Mail service is enabled.
1 In Server Admin, click the arrow on the local server services to view the list of enabled services.
2 Click the Mail service.
3 Click “Configure Mail Service.”
4 Deselect the “Enable Pop” and “Enable IMAP” checkboxes.
5 Click the Continue.

Set an Open Firmware Password
Do this task for both Mac OS X and Mac OS X Server.

When Open Firmware password protection is turned on using PowerPC-based models, it:
• Prevents using the C key to start up from a CD-ROM disc
• Prevents using the N key to start up from a NetBoot server
• Prevents using the T key to start up in Target Disk Mode (on computers that offer this feature)
• Prevents starting up in Verbose mode by pressing Command-V
• Prevents starting up a system in single-user mode by pressing Command-S during startup
• Prevents resetting Parameter RAM (PRAM) by pressing Command-Option-P-R during startup
• Requires the password to use Startup Manager, accessed by pressing the Option key during startup
• Requires the password to enter commands after starting up in Open Firmware, which is done by pressing Command-Option-O-F during startup
• Prevents startup in Safe Boot mode by pressing the shift key during startup.

When Open Firmware password protection is turned on using Intel-based models, it:
• Prevents using the C key to start up from a CD-ROM disc
• Prevents using the N key to start up from a NetBoot server
• Prevents using the D key to start up from the Diagnostic volume of the Install DVD.
• Prevents using the T key to start up in FireWire Target Disk Mode (on computers that offer this feature)
• Prevents starting up in Verbose mode by pressing Command-V
• Prevents starting up a system in single-user mode by pressing Command-S during startup
• Prevents starting up a system in safe-boot mode by pressing the shift key during startup
• Prevents resetting Parameter RAM (PRAM) by pressing Command-Option-P-R during startup
• Requires the password to use Startup Manager, accessed by pressing the Option key during startup

Prevents startup in Safe Boot mode by pressing the shift key during startup.

Note: The Open Firmware password does not prevent someone with physical access to the computer from restarting it or turning it off.

Preparing a Computer for Open Firmware Password Protection
To maximize the effectiveness of the Open Firmware Password, do the following:
• Use a secure password that contains both numerals and letters in the first eight characters.
• In the Users control panel, Accounts pane of System Preferences, or Server Admin application (whichever applies to your computer), strictly limit Admin user status to trusted personnel.
• Restrict physical access to the computer. Place the computer in a locked room, and lock the cover latch or use the security lock port.
• Make sure that you have selected the Mac OS X System folder for your startup device that you plan to protect.
• If your startup device is correctly selected, you should be able to select it in Startup Disk preferences, close the preference pane, and not receive a dialog box prompting you to save the changes. If you do receive this dialog, saving the changes sets your startup device.
Important: If you reset the PRAM or Open Firmware, you need to reselect your startup device before resetting the Open Firmware password.

Warning: The Open Firmware password can be reset by either of the following:
- Any administrator designated in the Accounts pane of System Preferences
- A user with physical access to the inside of the computer

Setting the Open Firmware Password
To set an Open Firmware password you must be running firmware version 4.1.7 or later.

To turn on the Open Firmware Password:
1. Startup from the Mac OS X 10.6 (Snow Leopard) install DVD, and then choose Utilities > Firmware Password Utility.
2. Select the “Require password to change Open Firmware settings” checkbox.
   Enter your password in the Password and Verify fields.

Important: Do not include an uppercase “U” in the password. For more information see this article on the Apple Support website, at the following address:
https://support.apple.com/kb/TA21330

3. Click OK. A confirmation dialog appears.
4. Click the lock to prevent further changes.
5. Choose File > Quit.

For more information on Open Firmware, see this article in the AppleCare Knowledge Base:
https://support.apple.com/kb/HT1352

Turn On Auditing
Auditing should be turned on. For information on turning on auditing, see: Chapter 6, “Mac OS X Auditing Administrator’s Guide,” on page 57.

Disable Password Hints
Do this task for both Mac OS X and Mac OS X Server.
1. Open System Preferences and click Accounts.
2. Select Login Options.
3. If the settings are dimmed, click the lock icon and enter an administrator name and password.
4. Deselect “Show password hints.”
Set Password Policy
Common Criteria require minimum password settings for both Mac OS X and Mac OS X Server. After the initial installation of Mac OS X and Mac OS X Server there are no password quality rules defined by default.

To set the following password policy:
- Minimum password length to 8 characters
- Password is required to have a character in [A-Z][a-z]
- Password is required to have a character in [0-9]
- Account is disabled if the failed login count exceeds 5 attempts
- Require to change the password after 90 days

1. Enter the following in Terminal, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

```
sudo /usr/bin/pwpolicy -n /Local/Default -setglobalpolicy "minChars=8 requiresAlpha=1 requiresNumeric=1 maxFailedLoginAttempts=5 maxMinutesUntilChangePassword=129600"
```

You may use a higher number of characters if a more secure password is desired. For more information on pwpolicy, refer to the man page documentation by entering:

```
man pwpolicy
```

Disable System Services
Enter the following commands in Terminal:

```
sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/com.apple.UserNotificationCenter.plist
sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/org.samba.winbindd.plist
sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/com.apple.IIDCAssistant.plist
sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/com.apple.RFBEventHelper.plist
sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/com.apple.RFBRegisterMDNS_ScreenSharing.plist
sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/com.apple.wikid.quicklook.plist
sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/com.apple.servermgrp.plist
sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/com.apple.blued.plist
sudo /bin/launchctl unload -w /System/Library/LaunchDaemons/com.apple.systempreferences.installer.plist
```
Set the Global umask
Do this task for both Mac OS X and Mac OS X Server.
The umask determines the level of permissions for newly created files.

1 To set the umask for all users on the system:, enter the following commands in Terminal:

```bash
sudo defaults write /Library/Preferences/.GlobalPreferences NSUmask Value
```

Use one of the following values to set the permission level:

<table>
<thead>
<tr>
<th>Value</th>
<th>Permission level</th>
</tr>
</thead>
<tbody>
<tr>
<td>63 (octal equivalent 077)</td>
<td>Only the user can read newly created files.</td>
</tr>
<tr>
<td>23 (octal equivalent 027)</td>
<td>The user and members of their default group can read newly created files.</td>
</tr>
<tr>
<td>18 (octal equivalent 022)</td>
<td>All users can read newly created files.</td>
</tr>
</tbody>
</table>

**Warning:** Setting group, or all, access to files will may allow any private, or confidential information on these files to be visible to others. To prevent private files being accessed, the user should create a directory and change the permissions to restrict all but their own access.

2 Then enter this command:

```bash
sudo chmod 644 /Library/Preferences/.GlobalPreferences.plist
```

Configure Secure Shell
Do this task for both Mac OS X and Mac OS X Server.
Configure the secure shell (ssh) by editing the `/etc/sshd_config` file. The sshd should be configured to either accept passwords or public key authentication only.

To configure the secure shell, make the following settings in the `sshd_config` file:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PasswordAuthentication</td>
<td>yes</td>
</tr>
<tr>
<td>ChallengeResponseAuthentication</td>
<td>no</td>
</tr>
<tr>
<td>GSSAPIAuthentication</td>
<td>no</td>
</tr>
<tr>
<td>HostBasedAuthentication</td>
<td>no</td>
</tr>
<tr>
<td>kbdInteractiveAuthentication</td>
<td>no</td>
</tr>
<tr>
<td>KerberosAuthentication</td>
<td>no</td>
</tr>
<tr>
<td>KerberosOrLocalPasswd</td>
<td>no</td>
</tr>
<tr>
<td>PAMAuthenticationViaKbdInt</td>
<td>no</td>
</tr>
<tr>
<td>PubkeyAuthentication</td>
<td>no</td>
</tr>
<tr>
<td>RhostsAuthentication</td>
<td>no</td>
</tr>
</tbody>
</table>
In the `sshd_config` file, all options are listed, but are commented out. To set the options above to the required settings, you must uncomment them and change them to the setting shown. For more information on editing settings files, see, “Editing Settings Files” on page 94.

**Software**

The evaluated configuration is a subset of the software packages contained on the DVDs for the distributed Mac OS X product, consisting of only the packages installed during default installation of MAC OS X 10.6 (Snow Leopard) or MAC OS X Server 10.6 (Snow Leopard).

Additional software may be installed by either the administrator or the user with the following restrictions:

- Applications owned by root and with the SUID bit set must not be installed.
- Applications owned by any group with group ID below 100 and the SGID bit set must not be installed.
- Applications executed with root privileges and providing services to untrusted users (such as additional services) must not be installed.
- Kernel extension must not be installed or even loaded.

**Configurations**

The evaluated configuration is defined with the following constraints:

- The set of software packages forming the Common Criteria Evaluated Configuration must be installed during installation time in accordance with the installation instructions provided in the Common Criteria guidance document.
- Only local user databases for password based authentication are allowed to be used by the Directory Service mechanism.
- The automated password quality checking mechanism is configured as described in the “Set Password Policy” section. See: “Set Password Policy” on page 29.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RhostsRSAAuthentication</td>
<td>no</td>
</tr>
<tr>
<td>RSAAuthentication</td>
<td>no</td>
</tr>
<tr>
<td>Ciphers</td>
<td>aes128-cbc</td>
</tr>
<tr>
<td></td>
<td>aes192-cbc</td>
</tr>
<tr>
<td></td>
<td>aes256-cbc</td>
</tr>
<tr>
<td></td>
<td>3des-cbc</td>
</tr>
<tr>
<td></td>
<td>blowfish-cbc</td>
</tr>
<tr>
<td></td>
<td>arcfour128</td>
</tr>
<tr>
<td></td>
<td>cast128-cbc,</td>
</tr>
<tr>
<td></td>
<td>hmac-sha1</td>
</tr>
<tr>
<td></td>
<td>hmac-md5</td>
</tr>
</tbody>
</table>
• The root account is disabled for interactive login. Administrators use the ‘sudo’ application to gain root privileges.
• The initial configuration outlined in the Common Criteria guidance document representing the evaluated configuration must be achieved before users are allowed to interact with the Common Criteria Evaluated Configuration.
• Mac OS X supports different networking protocols, including IPv4 and IPv6. Only IPv4 is supported in the evaluated configuration.
• Darwin offers support for multiple file systems. In the evaluated configuration, the HFS+ file system is supported.
• Mac OS X supports a wide range of protocols and network services. In the evaluated configuration, the TCP/IP protocol, the NFS client, and SSH services are supported. NFS is allowed to be used in the evaluated configuration, but is not covered by security functional claims in this ST.
• For SSH, the “none” cipher (no encryption), and the “none” keyed hash function (no HMAC) are not allowed in the evaluated configuration.
• Apple provides several Mac OS X software applications that are considered outside the scope of the defined Common Criteria Evaluated Configuration and thus not part of the evaluated configuration. Services outside this evaluation include:
  • E-mail services
  • Web server services
  • Remote apple events
  • Print sharing services
  • File sharing services
  • Unencrypted base services, such as FTP or the r-utilities
  • Classic programming support (Old Macintosh OS compatibility support)
  • Mac OS X contains a watchdog timer to restart services and provide stability; however, this timer is disabled in the evaluated configuration.
Using Mac OS X in a Secure Manner

This chapter discusses how to use Mac OS X in a safe and secure way.

Using Passwords in Mac OS X
Mac OS X is designed to give you the safest and most secure computing environment available. The best thing you can do to keep the information on your computer secure is to choose a good password for your user account.

There are several different types of passwords in Mac OS X:
- **User account passwords** allow users to log in to their home folders. This is often referred to as a "login password."
- **Administrator passwords** are required to perform many tasks on the computer, including setting system preferences, installing software, and administering user accounts. An administrator password is an administrator user’s login password.
- **The Open Firmware password** allows you to prevent others from starting your computer using a CD or other disk with an operating system on it.

Those responsible for the Common Criteria Evaluated Configuration must establish and implement procedures to ensure that information is protected in an appropriate manner.

- DAC protections on security-critical files such as configuration files and authentication databases must always be set up correctly.
- Network and peripheral cabling must be approved for the transmittal of the most sensitive data held by the system. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted unless one of the secure protocols provided by the Common Criteria Evaluated Configuration is used for the communication with another trusted entity.
- Those responsible for the Common Criteria Evaluated Configuration must ensure that procedures and/or mechanisms are provided to assure that after system failure or other discontinuity, recovery without a protection (i.e., security) compromise is obtained.
• Those responsible for the Common Criteria Evaluated Configuration must ensure that the system is configured so that only an administrative user can introduce new trusted software into the system.

Choosing Secure Passwords
Regardless of the type of password you are creating, follow these guidelines for choosing a secure password:

• Passwords must contain a minimum of 8 characters. An administrator may have set a minimum password length for the system. You will need to consult with your administrator to find the minimum number of password characters that are acceptable.
• Passwords must contain letters, numbers, and symbols in combinations that won’t be easily guessed by unauthorized users. Passwords must not consist of actual words. Use a mix of uppercase and lowercase letters, numbers, punctuation, and symbols.
• Passwords must have a character in [A-Z][a-z]
• Passwords must have a character in [0-9]
• Use a different password for each resource you need to protect.
• Don’t provide hints for passwords.
• Don’t use any information that’s easy to guess, such as your address, birth date, or child’s name.
• Don’t share your passwords with anyone.
• Don’t store your passwords in an obvious place, such as stuck to your computer, or in a file that can be accessed by others.

To avoid potential problems with your password, you must follow these additional guidelines:
• Avoid characters that can’t be entered on computers the user will be using or that might require a special key combination to enter correctly on different keyboards and platforms.
• Do not use passwords that contain leading spaces or trailing spaces.
• Some remote services may require use of only ASCII characters in passwords. The password policy is not enforced for the administrator. When the administrator changes his/her password, he/she must manually verify that the new password complies with the password quality rules defined under section ‘Set Password Policy’ in Chapter 3.

Logging Out at the End of a Session
If you leave your computer unattended, the system may be vulnerable to unauthorized access by someone using your computer and username. To prevent someone accessing your computer, log out before you leave.
Logging out will end your session. You will be required to quit all running applications and save any open documents. When you return to the computer, enter your login name and password to continue working.

**To log out:**

1. Choose Apple menu > Log Out “User” (your account name appears in the menu).
2. You may get some confirmation dialogs. Click Log Out.

**Note:** To log out of a remote (ssh) user session, enter “exit” in the shell. This will stop the local “ssh” process.

### Setting the umask for Individual Users

The umask determines the level of permissions for newly created files. To set the umask for files you create as the logged-on users, enter the following in Terminal:

```
defaults write -g NSUmask -int value
```

Use one of the following values to set the permission level:

<table>
<thead>
<tr>
<th>Value</th>
<th>Permission level</th>
</tr>
</thead>
<tbody>
<tr>
<td>63 (octal equivalent 077)</td>
<td>Only the user can read newly created files.</td>
</tr>
<tr>
<td>23 (octal equivalent 027)</td>
<td>User and members of their default group can read newly created files.</td>
</tr>
<tr>
<td>18 (octal equivalent 022)</td>
<td>All users can read newly created files.</td>
</tr>
</tbody>
</table>

You must log out and log back in for the umask to take effect. The lowest umask value that any user should use is 002. A higher umask value can be chosen, but a lower number allows other users to modify the data.

**Warning:** Setting permissions to group, or all, will allow any private, or confidential information in these directories to be visible to others. To prevent private files being accessed the user should create a directory and restrict the permissions.

### Setting Permissions for Disks, Folders, and Files

To control access to your important information, Mac OS X automatically sets permissions for disks, folders, and files. You can only change permissions to items that you own.

Be sure that the permissions set are appropriate. For most purposes files should be accessible to the other members of your group. If you have private or confidential information, the default permissions of the files may allow others to see it. To prevent others from accessing personal information, create a directory and set its permissions to “owner.” Then place your confidential files into it. No other users will be allowed into the directory.
Mac OS X provides distinct permissions for three types of users:

- The "owner" of the item, which is usually the name of the person who created the item, or yourself
- Any member of the group assigned to the item by Mac OS X
- Any other user with access to the computer

There are four levels of permission:

- Read & Write allows a user to open the item to see its contents and change it.
- Read Only allows a user to open the item to see its contents, but not change the contents or copy them.
- Write Only makes a folder into a drop box. Users can copy items to the drop box, but cannot open the drop box to see its contents. Only the owner of the drop box can open it to take items out.
- No Access blocks all access to the item so that users can't open the item, change its contents, or copy its contents.
Setting Permissions in the Mac OS X interface
You can change these permissions for an item using the Info window in the Finder. 
**Warning:** Be sure that appropriate permissions levels are set for your files to ensure that private, or confidential information is not disclosed.

**To change permissions for an item:**
1. Select the item you want to set permissions for, then choose File > Get Info and click Ownership & Permissions, if necessary.
2. Choose a permission for yourself from the pop-up menu at the top of the Ownership & Permissions pane. If the menu is dimmed, you don't have permission to change this setting.
3. To change permissions for the owner, group, or others, click Detail. If necessary, click the lock icon and, when prompted, enter the name and password of an administrator user of your computer.
4. Choose permissions for each type of user from the Access pop-up menus.
   If you are setting permissions for a folder or disk and you want to apply the same permissions to every item contained in the folder or disk, click "Apply to enclosed items."

Setting Permissions Using UNIX Commands
Since Mac OS X is built on a UNIX core, you can set permissions by entering UNIX commands in Terminal.
**Warning:** Be sure that appropriate permissions levels are set for your files to ensure that private, or confidential information is not disclosed.

Understanding UNIX Permissions
Each file or directory has 3 types of security groups:
- **Owner:** The owner or creator of the file or directory
- **Group:** The group to which the file or directory is assigned
- **All Others:** Anyone who isn't the owner or is not assigned to the group associated with the file or directory.

Each security group is assigned a code that controls that group's permissions:
- **r** (read) allows the user to see the item but not make changes.
- **w** (write) allows the user to see and make changes to the item.
- **x** (execute) allows the user to run scripts or programs.
- **"-"** (access) means access is turned off.

To view permissions for files and directories in Terminal, enter the `ls -l` command. For each file or directory listed, you see the permissions, owner and group name, and file or directory name.
Examples:
The following file (-) displays read, write, and executable permissions for owner (rwx),
group (rwx) and all others (rwx):
   -rwxrwxrwx

The following file (-) displays read, write, and executable permissions for owner (rwx),
and group (rwx), but no permissions for others (---):
   -rwxrwx---

The following file (-) displays read, write, and executable permissions for owner (rwx),
but no permissions for group (---) or others (---):
   -rwx------

The following file (-) displays read and write, but no executable permissions for owner
(rw-), group (rw-), and others (rw-):
   -rw-rw-rw-

The following file (-) displays read, write, and executable permissions for owner (rwx),
but only read and executable for group (r-x) and others (r-x):
   -rwxr-xr-x

The following file (-) displays read, write, and executable permissions for owner (rwx),
but only read for group (r-) and others (r-):
   -rwxr--r--

For more information on permissions in UNIX, refer to the man page by entering:
   man ls

Changing Permissions
Use the chmod command to change permissions for an item.

The syntax of the command is as follows:
chmod security group change type permission file or directory

The options for each item in the command are described below.

Security group: The person or group whose permission you are changing. Can be any
of the following:
• u - user
• g - group
• o - other
• all - all
Type of change: Whether you are adding or subtracting the permission:
- “+” - add permission
- “-” - subtract permission

Permission: The permission you are changing:
- r - read
- w - write
- x - execute

File or directory: The name of the file or directory to change:

Examples:
chmod go-w myfile
Removes write access for group and others for the file myfile.
chmod go+rw myfile1 myfile2
Adds read and write access for group and others for files myfile1 and myfile2.
chmod ugo+rwx myfile1
Adds read, write, and execute for everyone for myfile1.

For more information on changing UNIX permissions, refer to the chmod man page by entering:

man chmod

Changing the Owner
Use the chown command to change the owner of a file or directory.

The syntax of the command is as follows:
chown username file or directory

For example, to change the owner of file1 to the user jdoe, enter:
chown jdoe file1

For more information on changing UNIX ownership, refer to the chown man page by entering:

man chown
Changing the Group

Use the `chgrp` command to change the group of a file or directory.

The syntax of the command is as follows:

```
chgrp groupname file or directory
```

For example: to change the group of file1 and file2 to the group ateam, enter:

```
chgrp ateam file1 file2
```

For more information on changing UNIX groups, refer to the `chgrp` man page by entering:

```
man chgrp
```
This chapter describes how to perform administrative tasks when using the Common Criteria configuration.

About Administrator Accounts
When you set up Mac OS X or Mac OS X Server, you create a user account that has full administrator access or an administrator account. A person with an administrator account can create other user accounts, install software in the Applications and Library folders, and change computer settings.

When you create new user accounts, you specify whether the user is an administrator or regular user. If you don’t want the user to be able to change preferences or install software on the computer, don’t give the user administrator access.

To keep your computer secure, don’t share an administrator name and password with anyone. Be sure to log out when you leave your computer, or set Security preferences to require a password. If you leave your computer while you’re logged in, someone could sit down at your computer while you’re away and make changes using your administrator privileges.

For added security, don’t set an administrator to be automatically logged in when the computer starts up. If you do, someone could simply restart the computer to gain access as an administrator. Administrators should create a user account without administrator access to use when they are doing tasks that don’t require administrator access.

Limiting su Rights to Only Administrator Users
After the initial installation, the created user is an administrative user, (defined by the right to execute sudo and su if the root account is enabled.) For normal non-administrator usage there must be a new user created that does not have the rights to call sudo. If the root account is enabled, the su application must be restricted to administrative users.
To limit the `su` rights to just administrators:

1. In Terminal enter:
   ```
   chgrp admin /usr/bin/su
   chgrp admin /usr/bin/su
   chmod 4750 /usr/bin/su
   ```

Adding a New User Account

You can create individual user accounts for each person who uses your computer. Each new user has a separate home folder and can adjust his or her own preferences without affecting other users.

**To add a new user account:**

1. Choose Apple () > System Preferences.
2. Click Accounts.
3. If some settings are dimmed, click the lock icon and enter an administrator name and password.
4. Click Add (+).
5. Choose the type of account from the “New account” pop-up menu.
6. Enter the user's name.
7. A default short name is generated automatically. If you want to use a different name, enter the new name in the “Short name” field.
8. Enter the user’s password in the Password and Verify fields.
Changing a Password
If you are the administrator of your computer, you can change your password and the password for other user accounts.

1. Choose Apple () > System Preferences and click Accounts.
2. If some settings are dimmed, click the lock icon and enter an administrator name and password.
3. Choose the account you wish to change.
4. Click in the Password box and modify the password.
5. Enter your new password again in the Verify box.

Deleting a User Account
If you are an administrator for your computer, you can delete user accounts which are no longer needed.

When you delete a user account, you can choose to archive the user's files or delete them.

Important: If the user’s account is encrypted (FileVault is turned on), turn FileVault off for the user before you delete the account. For information about turning FileVault off, search Mac OS Help for “FileVault.”

To delete a user account:

1. Choose Apple () > System Preferences and click Accounts.
2. If some settings are dimmed, click the lock icon and enter an administrator name and password.
3. Select the user account you want to delete, then click Delete (-).
4. Select “Save the home folder in a disk image” to archive the user’s files on the computer, or select “Delete the home folder” to remove the user account and all of the user’s files.

If you saved the user’s files, they are stored in a disk image in the Deleted Users folder, which is in the Users folder on your Mac OS X disk. To see the saved files, double-click the disk image in the Deleted Users folder. You can drag the disk image to the Trash to delete the files.
Setting the Default Permissions for New Files

The default access permissions assigned to all newly created files and folders are determined by the umask setting in the system’s global preferences file. The global umask setting applies to all users on the computer. You can change the global umask setting by using the `defaults` utility in Terminal. For general information about using Terminal, including getting detailed information about the `defaults` utility, see Appendix C, “Using Terminal,” on page 91.

To change the global umask setting:

- Enter the following command in Terminal, replacing `value` with one of the values in the table:

  ```
  defaults write /Library/Preferences/.GlobalPreferences NSUmask value
  ```

<table>
<thead>
<tr>
<th>Value</th>
<th>Permission level</th>
</tr>
</thead>
<tbody>
<tr>
<td>63 (octal equivalent 077)</td>
<td>Only the user who creates a file can read it.</td>
</tr>
<tr>
<td>23 (octal equivalent 027)</td>
<td>The user and members of the user’s primary group can read files newly created by the user.</td>
</tr>
<tr>
<td>18 (octal equivalent 022)</td>
<td>All users can read newly created files.</td>
</tr>
</tbody>
</table>

**Note:** A change of the global umask setting takes effect after you log out.

**Warning:** Setting permissions to group, or all, will allow any private, or confidential information in these directories to be visible to others. To prevent private files being accessed the user should create a directory and restrict the permissions.

Administering User and Group Accounts With UNIX Commands

You can administer user and group accounts by using the `dscl` and other command-line utilities in Terminal. For general information about using Terminal, including getting detailed information about specific commands and utilities, see Appendix C, “Using Terminal,” on page 91.

This section covers command-line procedures for:

- Adding a user account
- Removing a user account
- Modifying a user account
- Adding a new group
- Removing a group
- Adding a user to a group
- Removing a user from a group
Adding a User Account via the Command Line

You can create new user accounts by using `dscl` and other commands and utilities in Terminal. When you create a user account via the command line, you must also set values for basic attributes of a user account such as short name, long name, user ID, primary group ID, and home directory location.

By Apple convention, a new group account is created to match each new user account. The new group account has the same short name and ID number as the new user account. The following procedure includes instructions for creating a new matching group.

If you are not following Apple convention, you need to know the ID number of the user's primary group. If you need to create a group (other than the conventional group that matches the new user account), follow the instructions in “Adding a New Group via the Command Line” on page 49 before adding a new user.

To add a user account:

1. In Terminal, identify an unused user ID number by entering the following commands to display lists of assigned user ID and group ID numbers.

   ```bash
   dscl . list /Groups PrimaryGroupID | awk '{ print $2 }' | sort -n
   dscl . list /Users UniqueID | awk '{ print $2 }' | sort -n
   ```

   After you enter each of these commands, the `dscl` utility displays a list of assigned ID numbers resembling this example:

   ```
   -2
   0
   1
   99
   25
   26
   27
   70
   71
   74
   75
   76
   77
   78
   79
   501
   ```

   **Important:** Pick an ID number that isn't on either list and is greater than 500.

2. Invoke the interactive mode of the `dscl` utility, specifying the computer you’re using as the source of directory service data:
dscl localhost
In interactive mode, the dscl utility displays the current directory and a "->" character as a prompt. (Specifically, dscl displays the current directory in the directory domain, not the current directory in the file system.)

3 Change the current directory to /Local/Default/Users by entering:
   cd /Local/Default/Users

4 Authenticate as an administrator by entering the following command, replacing adminusername with your admin user name, and entering your admin password when prompted:
   auth adminusername

5 Create a new user account, replacing jsmith with the new user account’s short name:
   create jsmith

6 Specify the path to the new user’s home directory in /Users/:
   create jsmith home /Users/jsmith

7 Specify the new user’s default UNIX shell:
   create jsmith shell /bin/bash

8 Specify the user ID, replacing 502 with the new user’s ID number:
   create jsmith uid 502

9 Specify the new user’s primary group ID, replacing 502 with the primary group ID:
   create jsmith gid 502
   If you’re following Apple convention, use the same ID number here as in the previous step. (You’ll create a new group account for this ID number in step 12.)

10 Specify the long name for the new user account, replacing New User with the actual long name:
    create jsmith realname "New User"

11 Review the settings of your new user account by entering the following command, replacing jsmith with the new user account’s short name as before:
    read jsmith
    The dscl utility displays the settings for your new user account. They will resemble this example:
    _writers_passwd: jsmith
    _writers_picture: jsmith
    _writers_tim_password: jsmith
    AppleMetaNodeLocation: /Local/Default
    NFSHomeDirectory: /Users/jsmith
    PrimaryGroupID: 502
    RealName: New User
RecordName: jsmith
UniqueID: 502
UserShell: /bin/bash

12 Change the current directory to /Local/Default/Groups:
   cd /Local/Default/Groups
   If you’re not following the Apple convention of creating a new group account to match
   the new user account, skip to step 17.

13 Authenticate as an administrator with your admin user name, entering your admin
   password when prompted:
   auth adminusername

14 Create the new group account, replacing jsmith with the new account’s short name:
   create jsmith

15 Specify the group ID, replacing 502 with the ID number:
   create jsmith gid 502

16 Review the settings of your new group account by entering the following command,
   replacing jsmith with the new account’s short name as before:
   read jsmith
   The dscl utility displays the settings for your new group account. They will resemble
   this example:
   AppleMetaNodeLocation: /Local/Default
   PrimaryGroupID: 502
   RecordName: jsmith

17 Quit the dscl utility by entering:
   quit
   The dscl utility displays Goodbye, and then the standard shell prompt appears.

18 Assign a password to the account by entering the following command, replacing
   jsmith with the new account’s short name:
   sudo passwd jsmith
   You will be prompted for your admin password, then the new user password, and
   finally the new user password again (for verification).

19 Create the home directory for the new user, replacing jsmith with the new account’s
   short name:
   sudo mkdir ~jsmith

20 Assign ownership of the home directory to the new user and group accounts, replacing
   userName with the short name of the new user account and groupName with the
   short name of the user account’s primary group account:
   sudo chown userName:groupName ~userName
If you followed the Apple convention of creating a new group account to match the new user account, the short names for both are the same. If you didn’t follow the Apple convention, the group whose short name you specify must exist. If it doesn’t exist yet, create it as described in “Adding a New Group via the Command Line” on page 49 before doing this step.

The user account is now complete. The new user account can now be used for login.

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```

**Removing a User Account via the Command Line**

You can remove accounts by using the `dscl` utility in Terminal.

**To delete a user account:**

1. In Terminal, invoke the interactive mode of the `dscl` utility, specifying the computer you’re using as the source of directory service data:
   ```
   dscl localhost
   ```

2. Change the current directory to `/Local/Default/Users` by entering:
   ```
   cd /Local/Default/Users
   ```

3. Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:
   ```
   auth adminusername
   ```

4. Delete the user account by entering the following command, replacing `jsmith` with the user account’s short name:
   ```
   delete jsmith
   ```

5. Quit the `dscl` utility by entering:
   ```
   quit
   ```

*Note:* This does not remove a user’s home directory and the data that may be stored there. You can use the Finder to drag a deleted user’s home directory to the Trash. A user account usually has a matching group of the same name. For information on deleting this group, see “Removing a Group via the Command Line” on page 51.

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```
Modifying a user Account via the Command Line
You can change the value of an attribute in a user account by using the `dscl` utility in Terminal.

The following table describes user account attributes you can modify using `dscl`:

<table>
<thead>
<tr>
<th>Description</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home directory</td>
<td>home</td>
</tr>
<tr>
<td>Terminal Shell</td>
<td>shell</td>
</tr>
<tr>
<td>Real Name</td>
<td>realname</td>
</tr>
<tr>
<td>Primary Group ID</td>
<td>gid</td>
</tr>
</tbody>
</table>

To change a user account attribute to a new value:
1. In Terminal, invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:
   ```
dscl localhost
   ```
2. Change the current directory to `/Local/Default/Users` by entering:
   ```
cd /Local/Default/Users
   ```
3. Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:
   ```
auth adminusername
   ```
4. Set the user attribute to the desired value by entering the following command, replacing `jsmith` with the user account's short name, `attribute` with the name of the attribute whose value you wish to change, and `newvalue` with the value:
   ```
create jsmith attribute newvalue
   ```
5. Quit the `dscl` utility by entering:
   ```
quit
   ```
   For more information on using the Directory Service Command Line utility, see the man pages by entering:
   ```
man dscl
   ```

Adding a New Group via the Command Line
You can create new group accounts by using `dscl` and other commands and utilities in Terminal. When you create a group account via the command line, you must also set values for basic attributes of a group account such as short name and group ID.

To add a group account:
1. In Terminal, identify an unused group ID number by entering the following command to display a list of assigned group ID numbers.
   ```
dscl . list /Groups PrimaryGroupID | awk '{ print $2 }' | sort -n
   ```
The `dscl` utility displays a list of assigned ID numbers resembling this example:

```
-2
0
1
99
25
26
27
70
71
74
75
76
77
78
79
501
```

**Important:** Pick an ID number that isn't on either list and is greater than 500.

2 Invoke the interactive mode of the `dscl` utility, specifying the computer you're using as the source of directory service data:

```
dscl localhost
```

3 Change the current directory to `/Local/Default/Groups` by entering:

```
cd /Local/Default/Groups
```

4 Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:

```
auth adminusername
```

5 Create the new group, replacing `officegroup` with the new group account's short name:

```
create officegroup
```

6 Specify the group ID, replacing `600` with the primary group id

```
create officegroup gid 600
```

7 Review the settings of your new group by entering the following command, replacing `officegroup` with the new group account's short name:

```
read officegroup
```

The `dscl` utility displays the settings for your new group account. They will resemble this example:

```
AppleMetaNodeLocation: /Local/Default
```
8 Quit the dscl utility by entering:
   
   quit

   For more information on using the Directory Service Command Line utility, see the man pages by entering:

   man dscl

   **Removing a Group via the Command Line**
   You can remove accounts by using the dscl utility in Terminal.

   **To delete a group account:**
   1 In Terminal, invoke the interactive mode of the dscl utility, specifying the computer you’re using as the source of directory service data:
      
      dscl localhost
   2 Change the current directory to /Local/Default/Groups by entering:
      
      cd /Local/Default/Groups
   3 Authenticate as an administrator by entering the following command, replacing adminusername with your admin user name, and entering your admin password when prompted:
      
      auth adminusername
   4 Delete the group by entering the following command, replacing officegroup with the group account’s short name:
      
      delete officegroup
   5 Quit the dscl utility by entering:
      
      quit

   **Adding a user to a Group via the Command Line**
   You can add users to a group by using the dscl utility in Terminal.

   **To add a user to a group:**
   1 In Terminal, invoke the interactive mode of the dscl utility, specifying the computer you’re using as the source of directory service data:
      
      dscl localhost
   2 Change the current directory to /Local/Default/Groups by entering:
      
      cd /Local/Default/Groups
   3 Authenticate as an administrator by entering the following command, replacing adminusername with your admin user name, and entering your admin password when prompted:
      
      auth adminusername
4 Add a user to a group by entering the following command, replacing *jsmith* with the short name of the user account and *officegroup* with the short name of the group account:

```
append officegroup users jsmith
```

5 Review the new settings of the group by entering the following command, replacing *officegroup* with the group account’s short name:

```
read officegroup
```

The *dscl* utility displays the settings for the group account. They will resemble this example:

```
AppleMetaNodeLocation: /Local/Default
GroupMembership: origuser jsmith
PrimaryGroupID: 600
RecordName: officegroup
```

6 Quit the *dscl* utility by entering:

```
quit
```

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```
man dscl
```

**Removing a User from a Group via the Command Line**

You can remove users from a group by using the *dscl* utility in Terminal.

**To remove a user from a group:**

1 In Terminal, invoke the interactive mode of the *dscl* utility, specifying the computer you’re using as the source of directory service data:

```
dscl localhost
```

2 Change the current directory to `/Local/Default/Groups` by entering:

```
cd /Local/Default/Groups
```

3 Authenticate as an administrator by entering the following command, replacing *adminusername* with your admin user name, and entering your admin password when prompted:

```
auth adminusername
```

4 View the current members of the group by entering (replacing *officegroup* with the group account’s short name):

```
read officegroup
```

The *dscl* utility displays the settings for the group account. They will resemble this example, which shows the group named officegroup has users jsmith, mjones, and tblack as members:

```
AppleMetaNodeLocation: /Local/Default
```
GroupMembership: mjones jsmith tblack
PrimaryGroupID: 600
RecordName: officegroup

5 Delete the user by entering the following command, replacing jsmith with the short name of the user account and officegroup with the short name of the group account:

```bash
delete officegroup users jsmith
```

6 Review the new settings of the group:

```bash
read officegroup
```

The dscl utility displays the settings for the group, showing the user you removed is no longer a group member, as in this example:

AppleMetaNodeLocation: /Local/Default
GroupMembership: mjones tblack
PrimaryGroupID: 600
RecordName: officegroup

7 Quit the dscl utility by entering:

```bash
quit
```

For more information on using the Directory Service Command Line utility, see the man pages by entering:

```bash
man dscl
```

**Revoking a User's Right to Access the System**

There are times when it is necessary to revoke a user's ability to access the system. This involves two steps:

- Prevent the user from logging in.
- Terminate all of a user's processes. This can be done by forcing a user to log out and then killing any remaining processes or by just killing all of a user's processes.

**Preventing Users From Logging In**

To removing the ability of a user to log in, the administrator should use the following command

To disable a user account:

1 In Terminal, invoke the interactive mode of the dscl utility, specifying the computer you’re using as the source of directory service data:

```bash
dsc1 localhost
```

2 Change the current directory to /Local/Default/Users by entering:

```bash
cd /Local/Default/Users
```
3 Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:
   auth adminusername

4 Disable the user by entering the following command, replacing `jsmith` with the short name of the user account:
   change jsmith AuthenticationAuthority ;ShadowHash; ;DisabledUser;

5 Quit the dscl utility by entering:
   quit
   For more information on using the Directory Service Command Line utility, see the man pages by entering:
   man dscl

   To re-enable an account that has been disabled:
   1 In Terminal, invoke the interactive mode of the dscl utility, specifying the computer you're using as the source of directory service data:
      dscl localhost
   2 Change the current directory to `/Local/Default/Users` by entering:
      cd /Local/Default/Users
   3 Authenticate as an administrator by entering the following command, replacing `adminusername` with your admin user name, and entering your admin password when prompted:
      auth adminusername
   4 Enable the user by entering the following command, replacing `jsmith` with the short name of the user account:
      change jsmith AuthenticationAuthority ;DisabledUser; ;ShadowHash;
   5 Quit the dscl utility by entering:
      quit
      For more information on using the Directory Service Command Line utility, see the man pages by entering:
      man dscl
Terminating All of a User’s Processes
After disabling the user, you need to kill all active processes that are currently running.

**Important:** Unconditionally killing all of a user’s processes will cause the user to lose any unsaved data.

1. To command all processes to clean up and exit by entering the following command, replacing `jsmith` with the user name:
   
   ```bash
   sudo killall -TERM -u jsmith
   ```

2. Wait a few seconds to allow the previous command to execute. To terminate all user processes unconditionally by entering the following command, replacing `jsmith` with the user name:
   
   ```bash
   sudo killall -9 -u jsmith
   ```

   For more information on terminating processes, refer to the man page documentation by entering:
   
   ```bash
   man killall
   ```

Abstract Machine Test Utility

Execute the Abstract Machine Test Utility in order to verify that the low level functions necessary to enforce the requirements of the CAPP are working correctly.

```bash
/usr/sbin/amt
```

For more information about `amt(1)` see its man page.

Run `amt(1)` anytime or periodically via a cron job.
Mac OS X Auditing
Administrator’s Guide

This chapter describes how to customize the audit subsystem using the command-line and file-based interfaces provided in the Common Criteria configuration.

The audit subsystem allows authorized administrators to create, read, and delete audit information regarding the Common Criteria configuration. The audit subsystem creates a log of auditable events, and allows the administrator to read all audit information from the records in a manner suitable for interpretation. The default location for these files is the /var/audit directory. The audit subsystem alerts the administrator to conditions such as potential audit data loss due to lack of disk space.

Tools are provided in the Common Criteria configuration for reading, sorting, creating, and modifying the audit log. These tools allow administrators to include or exclude audited events from the set of possible events, based on user identity and the success or failure of the audit.

Auditing is turned on by default so there are no further steps to take to turn on auditing. Audit logs are rotated automatically by the auditd daemon. The auditd daemon is launched by launchd on demand.

The Audit Utility
The audit subsystem is controlled by the audit utility (/usr/sbin/audit). This utility transitions the system in and out of audit operation.

The default configuration of the audit mechanism is controlled by a set of configuration files in /etc/security.

If auditing is enabled, the /etc/rc startup script will start the audit daemon at system startup. All the features of the daemon are controlled by the audit utility and audit_control file.
The audit subsystem generates warnings when relevant events such as storage space exhaustion and errors in operation are recognized during audit startup or log rotation. These warnings are communicated to the `audit_warn` script, which can then communicate these events to the authorized administrator. For more information, see “audit_warn” on page 66.

/etc/security/audit_control
/etc/security/audit_control - Specifies the detailed settings for the audit mechanism. Control flags can be specified to handle any occurrence that prevents audit events from being logged. The following control flag in the policy flags field specifies to halt the system if audit event logging fails:

```
policy:ahlt
```

- In order to stop running processes if audit event logging fails, do not specify the 'cnt' flag in the policy flags field. For more information about the audit_control flags, see the `audit_control(5)` man page.

Audit Classes, Audit Events, and User Masks
The audit classes, events, and user masks make the configuration of audit information more manageable by allowing administrators to finely control which events are logged in audit records.

The `audit_class` file defines a number of classes that events are normally categorized under. For more information, see Appendix A, “Mac OS X Audit Event Classes,” on page 69. The `audit_event` file maps an auditable event to a particular class; the list of auditable events extends to userspace events such as `AUE_login` so it supports the capture of user-submitted audit records. For more information, see “audit_event” on page 65.

Audit flags are defined in terms of audit classes. Audit flags can be for the whole system, or specific flags can be used for a particular user. Audit flags can include or exclude classes of events from the audit record stream based on the outcome of the event. For example, the outcome could be success, failure or both. For more information see: “audit_user” on page 65.

When a user logs in, the system-wide audit flags from the `audit_control` file are combined with the user-specific audit flags (if any) from the `audit_user` file, and together establish the process preselection mask for the user. The preselection mask determines which events will generate audit records for the given user.
If the preselection mask is changed, it is recommended that you restart the computer to ensure that all components are producing audit events consistently.

**Command-Line Programs**

**audit**

Auditing is managed by the `audit` utility. The `audit` utility follows this syntax:

```
audit [-nst] [file]
```

The `audit` utility controls the state of the auditing sub-system. The optional file operand specifies the location of the `audit_control` input file. The default file is:

```
default /etc/security/audit_control
```

You can use the following options with `audit`:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-n</code></td>
<td>Forces the audit system to close the existing audit log file and rotate to a new log file in a location specified in the audit control file.</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>Specifies that the audit system should [re]start and re-read its configuration from the audit control file. A new log file will be created.</td>
</tr>
<tr>
<td><code>-t</code></td>
<td>Specifies that the audit system should terminate. Log files are closed and renamed to indicate the time of the shutdown.</td>
</tr>
<tr>
<td><code>-i</code></td>
<td>Initializes and starts auditing. This option is currently for Mac OS X only and requires auditd to be configured to run under Launchd(8).</td>
</tr>
</tbody>
</table>

For more information on using `audit`, see the man pages in Terminal, by typing:

```
man audit
```

**auditreduce**

The `auditreduce` utility allows you to select events that have been logged in the audit records. Matching audit records are printed to the standard output in their raw binary form. If no filename is specified, the standard input is used by default. Use the `praudit` utility to print the selected audit records in human-readable form. For more information on `praudit`, see, “praudit” on page 61.

The `auditreduce` tool follows this syntax:

```
```
You can use the following options with auditreduce:

<table>
<thead>
<tr>
<th>Option</th>
<th>Formatting and description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-A</td>
<td>Selects all records.</td>
</tr>
<tr>
<td>-a</td>
<td>YYYYMMDD[HH[MM[SS]]]</td>
</tr>
<tr>
<td></td>
<td>Selects records that occurred after or on the given date-time.</td>
</tr>
<tr>
<td>-b</td>
<td>YYYYMMDD[HH[MM[SS]]]</td>
</tr>
<tr>
<td></td>
<td>Selects records that occurred before the given date-time.</td>
</tr>
<tr>
<td>-c</td>
<td>flags</td>
</tr>
<tr>
<td></td>
<td>Selects records matching the given audit classes specified as a comma-separated list of audit flags. For more information on audit flags, see, “audit_control” on page 63.</td>
</tr>
<tr>
<td>-d</td>
<td>YYYYMMDD</td>
</tr>
<tr>
<td></td>
<td>Selects records that occurred on a given date. Cannot be used with -a or -b option flags.</td>
</tr>
<tr>
<td>-e</td>
<td>euid</td>
</tr>
<tr>
<td></td>
<td>Selects records with the given effective user.</td>
</tr>
<tr>
<td>-f</td>
<td>egid</td>
</tr>
<tr>
<td></td>
<td>Selects records with the given effective group.</td>
</tr>
<tr>
<td>-g</td>
<td>gid</td>
</tr>
<tr>
<td></td>
<td>Selects records with the given real group.</td>
</tr>
<tr>
<td>-r</td>
<td>ruid</td>
</tr>
<tr>
<td></td>
<td>Selects records with the given real user.</td>
</tr>
<tr>
<td>-u</td>
<td>auid</td>
</tr>
<tr>
<td></td>
<td>Selects records with the given audit ID.</td>
</tr>
<tr>
<td>-j</td>
<td>id</td>
</tr>
<tr>
<td></td>
<td>Selects records having a subject token with matching ID.</td>
</tr>
<tr>
<td>-m</td>
<td>event</td>
</tr>
<tr>
<td></td>
<td>Selects records with the given event name or number.</td>
</tr>
<tr>
<td>-o</td>
<td>object = value</td>
</tr>
<tr>
<td>file =</td>
<td>Selects records containing the given path name.</td>
</tr>
<tr>
<td>file =</td>
<td>“/usr” matches paths starting with usr.</td>
</tr>
<tr>
<td>file =</td>
<td>“~/usr” matches paths not starting with usr.</td>
</tr>
<tr>
<td>msgqid =</td>
<td>Selects records containing the given message queue id.</td>
</tr>
<tr>
<td>pid =</td>
<td>Selects records containing the given process id.</td>
</tr>
<tr>
<td>semid =</td>
<td>Selects records containing the given semaphore id.</td>
</tr>
<tr>
<td>shmid =</td>
<td>Selects records containing the given shared memory id.</td>
</tr>
</tbody>
</table>

**Examples:**

To select all records associated with effective user ID root from the

```
audit log /var/audit/20031016184719.20031017122634:
```

```
auditreduce -e root /var/audit/20031016184719.20031017122634
```
To select all setlogin(2) events from that log:

```
auditreduce -m AUE_SETLOGIN /var/audit/20031016184719.20031017122634:
```

For more information on using `auditreduce`, see the man pages in Terminal, by typing:

```
man auditreduce
```

**praudit**

The `praudit` utility prints the contents of the audit records. The audit records are displayed in standard output (`stdout`). If no filename is specified, standard input (`stdin`) is used by default.

The `praudit` tool uses this syntax:

```
praudit [options] audit-trail-file [...]
```

You can use `praudit` with the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l</td>
<td>Prints the entire record in the same line. If this option is not specified, every token is displayed in a different line.</td>
</tr>
<tr>
<td>-r</td>
<td>Prints records in their raw format. This option is separate from <code>-a</code>.</td>
</tr>
<tr>
<td>-s</td>
<td>Prints the tokens in their &quot;short&quot; form. Short ASCII representations for record and event type are displayed. This option is separate from <code>-r</code>.</td>
</tr>
<tr>
<td>del</td>
<td>Specifies the delimiter. The default delimiter is the comma.</td>
</tr>
</tbody>
</table>

If raw or shortform are not specified, tokens are printed in their long form. That is, events are displayed according to their descriptions given in `audit_event`; UIDs and GIDs are expanded to their actual ASCII representation, date and time is displayed in standard date format, and so on.

For more information on using `praudit`, see the man pages in Terminal, by typing:

```
man praudit
```

**Managing Audit Log Files**

If auditing is enabled, the auditing subsystem adds records of auditable events to an audit log file. The name of an audit log file consists of the date and time it was created, followed by a period, and the date and time it was terminated, for example:

```
20040322183133.20040322184443.
```

The audit subsystem appends records to only one audit log file at any given time. The currently active file has a suffix ".not_terminated" instead of a date and time.
Audit log files are stored in the directories specified in the `audit_control` file. The audit subsystem creates an audit log file in the first directory specified.

When less than the 'minfree' amount of disk space is available on the volume containing the audit log file, the audit subsystem will:

- Issue an `audit_warn` soft warning
- Terminate the current audit log file
- Create a new audit log file in the next specified directory

Once all directories specified have exceeded this 'minfree' limit, auditing will resume in the first directory again. However, if that directory is full, an auditing subsystem failure may occur.

Administrators may also choose to terminate the current audit log file and create a new one manually using the `audit` utility. This action is commonly referred to as “rotating the audit logs.”

Use `audit -n` to rotate the current log file. Use `audit -s` to force the audit subsystem to reload its settings from the `audit_control` file (this will also rotate the current log file).

For more information on audit log files, see, “The Audit Utility” on page 57.
Deleting Audit Records

An administrator can clear the audit trail by deleting audit files. Administrators can delete audit files from the command line.

Example:

$ sudo rm /var/audit/20031016184719.20031017122634

Warning: The administrator should not delete the currently active audit log.

Audit Control Files

There are several text files the audit system uses to control auditing and write audit records. The default location for these files is the /etc/security directory.

audit_class

The audit_class file contains descriptions of the auditable event classes on the system. Each auditable event is a member of an event class. Each line maps an audit event mask (bitmap) to a class and a description.

Example entries in this file are:

0x00000000:no:invalid class
0x00000001:fr:file read
0x00000002-fw:file write
0x00000004:fa:file attribute access
0x00000080:pc:process
0xffffffff:all:all flags set

File Location

/etc/security/audit_class

For more information on using audit_class, see the man pages in Terminal, by typing:

man audit_class

audit_control

The audit_control file contains several audit system parameters. Each line of this file is of the form parameter:value.
You can use audit_control with the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir</td>
<td>The directory where audit log files are stored. There may be more than one of these entries. Changes to this entry can only be enacted by restarting the audit system. For more information on how to restart the audit system, see, “audit” on page 59.</td>
</tr>
<tr>
<td>flags</td>
<td>Specifies which audit event classes are audited for all users. For more information on how to audit events for individual users, see, “audit_user” on page 65.</td>
</tr>
<tr>
<td>naflags</td>
<td>Contains the audit flags that define what classes of events are audited when an action cannot be attributed to a specific user.</td>
</tr>
<tr>
<td>minfree</td>
<td>The minimum free space required in the directory audit logs are being written to. When the free space falls below this limit a warning will be issued.</td>
</tr>
</tbody>
</table>

**Audit Flags**

Audit flags are a comma delimited list of audit classes as defined in the audit_class file. Event classes may be preceded by a prefix that changes their interpretation. For more information, see, “audit_class” on page 63.

The following prefixes can be used for each class:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Record successful events</td>
</tr>
<tr>
<td>-</td>
<td>Record failed events</td>
</tr>
<tr>
<td>^</td>
<td>Record both successful and failed events</td>
</tr>
<tr>
<td>^+</td>
<td>Don’t record successful events</td>
</tr>
<tr>
<td>^-</td>
<td>Don’t record failed events</td>
</tr>
</tbody>
</table>

**Default**

The following settings appear in the default audit_control file:

dir:/var/audit
flags:lo,ad,-all,^-fc,^-cl
minfree:20
naflags:lo

The flags parameter above specifies the system-wide mask corresponding to login/logout events, administrative events, and all failures except for failures in creating or closing files.

**File Location**

/etc/security/audit_control
For more information on using `audit_control`, see the man pages in Terminal, by typing:

```
man audit_control
```

**audit_event**
The `audit_event` file contains descriptions of the auditable events on the system. Each line maps an audit event number to a name, a description, and a class. Entries are of the form:
```
eventnum:eventname:description:eventclass
```
Each eventclass should have a corresponding entry in the `audit_class` file. For more information on `audit_class`, see “audit_class” on page 63.

Example entries in this file are:
```
0:AUE_NULL:indir system call:no
1:AUE_EXIT:exit(2):pc
2:AUE_FORK:fork(2):pc
3:AUE_OPEN:open(2):fa
```

**File Location**

/etc/security/audit_event

The values for the events in this file must match the values in the `bsm_kevents.h` file.

For more information on using `audit_event`, see the man pages in Terminal, by typing:

```
man audit_event
```

**audit_user**
The `audit_user` file specifies which audit event classes are to be audited for the given users. If specified, these flags are combined with the system-wide audit flags in the `audit_control` file to determine which classes of events to audit for that user. These settings take effect when the user logs in.

Each line maps a user name to a list of classes that should be audited and a list of classes that should not be audited.

Entries are of the form:
```
username:alwaysaudit:neveraudit
```
In this example `alwaysaudit` is a set of event classes that are always audited, and `neveraudit` is a set of event classes that should not be audited. These sets can indicate the inclusion or exclusion of multiple classes, and whether to audit successful or failed events. For more information about audit flags, see “audit_control” on page 63.
Example entries in this file are:

root:lo,ad:no
jdoe:-fc,ad:+fw

These settings would cause login and administrative events that succeed on behalf of user root to be audited. No failure events are audited. For the user jdoe, failed file creation events are audited, administrative events are audited, and successful file write events are never audited.

**File Location**

/etc/security/audit_user

For more information on using `audit_user`, see the man pages in Terminal, by typing:

`man audit_user`

**audit_warn**

`audit_warn` runs when `auditd` generates warning messages. The default `audit_warn` is a script whose first parameter is the type of warning; the script appends its arguments to `/etc/security/audit_messages`. Administrators may replace this script with a more comprehensive one would take different actions based on the type of warning. For example, a low-space warning could result in an email message being sent to the administrator.

An example script is below:

```
#!/bin/sh
echo "Audit warning: $@ " >> /etc/security/audit_messages
```

This example script simply appends all of its arguments to the `audit_messages` file.

Below is the list of warnings generated by `audit_warn` with their associated arguments.

<table>
<thead>
<tr>
<th>Warning</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>audit_warn allhard</code></td>
<td>All directories listed in <code>audit_control</code> are completely out of space. The number of occurrences of this event is shown as <code>count</code> in the example.</td>
</tr>
<tr>
<td><code>audit_warn allsoft</code></td>
<td>All directories listed in <code>audit_control</code> have reached their “soft” limit. This is the threshold value specified in the <code>audit_control</code> file for the <code>minfree</code> entry.</td>
</tr>
<tr>
<td><code>audit_warn ebusy</code></td>
<td>The audit system is already running.</td>
</tr>
<tr>
<td><code>audit_warn getacdir dir</code></td>
<td>The <code>auditd</code> could not write to the given directory specified in the <code>audit_control</code> file.</td>
</tr>
<tr>
<td><code>audit_warn hard dir</code></td>
<td>The given directory is completely out of space.</td>
</tr>
<tr>
<td><code>audit_warn nostart</code></td>
<td>Auditing could not be started.</td>
</tr>
<tr>
<td><code>audit_warn postsigterm</code></td>
<td>An error occurred during the <code>auditd</code> shutdown.</td>
</tr>
</tbody>
</table>
For more information on using `audit_warn`, see the man pages in Terminal, by typing:

```
man audit_warn
```

---

<table>
<thead>
<tr>
<th>Warning</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>audit_warn soft dir</code></td>
<td>Remaining space in the given directory has reached the threshold value specified in the <code>audit_control</code> file.</td>
</tr>
<tr>
<td><code>audit_warn tmpfile</code></td>
<td>The temporary audit lock file already exists. This also indicates a fatal error in <code>auditd</code> startup.</td>
</tr>
</tbody>
</table>

---

**Audit Log Files**

The `dir` entry in the `audit_control` file specifies where audit logs are to be stored.

Multiple `dir` entries are permitted. The log files are created with names of the form `date.date` for log files that are closed (terminated), and `date.not_terminated` for the current log file that has not been closed. The date portion of the log file name is of the form `yyyymmddHHMMSS` with the hours in 24-hour format.
Mac OS X Audit Event Classes

The table below contains the audit event class names and descriptions.

The name of the event is used in the `audit_control` file for the `flags` and `naflags` entries, and in the `audit_user` file for the `alwaysaudit` and `never audit` fields of the user record.

**Audit Event Classes**

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Null value; turns off event preselection</td>
</tr>
<tr>
<td>fr</td>
<td>File read, open for read</td>
</tr>
<tr>
<td>fw</td>
<td>File write, open for write</td>
</tr>
<tr>
<td>fa</td>
<td>File attribute access</td>
</tr>
<tr>
<td>fm</td>
<td>File attribute modify</td>
</tr>
<tr>
<td>fc</td>
<td>File create</td>
</tr>
<tr>
<td>fd</td>
<td>File delete</td>
</tr>
<tr>
<td>cl</td>
<td>File close</td>
</tr>
<tr>
<td>pc</td>
<td>Events related to processes (kill, signal, etc.)</td>
</tr>
<tr>
<td>nt</td>
<td>Network events</td>
</tr>
<tr>
<td>ip</td>
<td>System V IPC</td>
</tr>
<tr>
<td>na</td>
<td>Non-attributable events</td>
</tr>
<tr>
<td>ad</td>
<td>Administrative</td>
</tr>
<tr>
<td>io</td>
<td>Login or logout</td>
</tr>
<tr>
<td>ap</td>
<td>Application-generated events</td>
</tr>
<tr>
<td>io</td>
<td>The ioctl() system call</td>
</tr>
<tr>
<td>ex</td>
<td>The exec() system call</td>
</tr>
<tr>
<td>ot</td>
<td>Miscellaneous</td>
</tr>
<tr>
<td>all</td>
<td>Sets the flags for all events</td>
</tr>
</tbody>
</table>
This appendix describes the format of the various audit records.

The format of the record definitions is the same as that used by BSM (http://dlc.sun.com/pdf/806-1789/806-1789.pdf).

This section contains the definitions of new tokens and audit records created for Mac OS X.

Notes:
• socket-inet tokens appear only when the system parameters are valid and the socket is successfully looked up.
• socket-unix Token describes a socket for the Unix address family.

socket-unix Token

<table>
<thead>
<tr>
<th>Token ID</th>
<th>Socket Family</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 byte</td>
<td>2 bytes</td>
<td>104 bytes</td>
</tr>
</tbody>
</table>

- The socket token in the form of that specified in the 1995 BSM specification:

socket token

<table>
<thead>
<tr>
<th>Token ID</th>
<th>Socket type</th>
<th>Local port</th>
<th>Local address</th>
<th>Remote port</th>
<th>Remote address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 byte</td>
<td>2 bytes</td>
<td>2 bytes</td>
<td>4 bytes</td>
<td>2 byte</td>
<td>4 bytes</td>
</tr>
</tbody>
</table>

- The in_addr token contains an Internet address. This 4-byte value is an Internet Protocol address. The token has two fields: a token ID that identifies this token as an in_addr token and an Internet address.

in_addr token

<table>
<thead>
<tr>
<th>Token ID</th>
<th>Internet address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 byte</td>
<td>4 bytes</td>
</tr>
</tbody>
</table>
The `ipc_perm` token in these records will have the seq ID and key set to 0. The creator UID is the same as owner UID, and creator GID is the same as owner GID.

The audit records created of OS X are as follows:

**accept**
- system call `accept` see `accept(2)`
- event ID 33  AUE_ACCEPT
- event class nt (0x00000100)
- audit record
  - header-token
  - argument-token (1, "fd", file descriptor)
  - `<socket-inet token>` if AF_INET socket
  - `<path token>` if AF_UNIX socket
  - `<path token>` canonical path of socket file
  - subject-token
  - return-token

**add_profile**
- system call `add_profile`
- event ID 324  AUE_ADDPROFILE
- event class pc (0x00000080)
- audit record
  - header-token
  - subject-token
  - return-token

**auditctl**
- system call `auditctl`
- event ID 352  AUE_AUDITCTL
- event class ad (0x00000800)
- audit record
  - header-token
  - path-token
  - `[attr-token]`
  - subject-token
  - return-token

**auditon: A_SETQCTRL**
- system call `auditon` see `auditon(2)`
- event ID 146  AUE_AUDITON_SQCTRL
- event class ad (0x00000800)
- audit record
  - header-token
  - argument-token (3, "setqctrl:aq_hiwater", hiwater)
  - argument-token (3, "setqctrl:aq_lowater", lowater)
  - argument-token (3, "setqctrl:aq_bufsz", output buffer size)
  - argument-token (3, "setqctrl:aq_delay", max write delay)
  - argument-token (3, "setqctrl:aq_minfree", %min fs free)
  - subject-token
return-token

bind
system call bind  see bind(2)
event ID 34  AUE_BIND
event class nt  (0x00000100)
audit record
header-token
argument-token  (1, "fd", file descriptor)
<socket-inet token> if AF_INET socket
<path token> if AF_UNIX socket
<path token> canonical path of socket file
subject-token
return-token

chflags
system call chflags  see chflags(2)
event ID 303  AUE_CHFLAGS
event class fm  (0x00000008)
audit record
header-token
argument-token  (2, "flags", flags)
path-token
[attr-token]
subject-token
return-token

connect
system call connect  see connect(2)
event ID 32  AUE_CONNECT
event class nt  (0x00000100)
audit record
header-token
argument-token  (1, "fd", file descriptor)
<socket-inet token> if AF_INET socket
<path token> if AF_UNIX socket
<path token> canonical path of socket file
subject-token
return-token

exchangedata
system call exchangedata
event ID 338  AUE_EXCHANGEDATA
event class fm  (0x00000008)
audit record
header-token
path-token
[attr-token]
path-token
[attr-token]
subject-token
fchflags
system call fchflags see fchflags(2)
event ID 304  AUE_FCHFLAGS
event class fm  (0x00000008)
audit record
    <valid file descriptor>
    header-token
    argument-token  (2, "flags", flags)
    [path-token]
    [attr-token]
    subject-token
    return-token
    <non-file descriptor>
    header-token
    argument-token  (1, "no path:fd:", fd)
    argument-token  (2, "flags", flags)
    subject-token
    return-token

flock
system call flock  see flock(2)
event ID 314  AUE_FLOCK
event class fm  (0x00000008)
audit record
    <valid file descriptor>
    header-token
    argument-token  (2, "operation", operation)
    [path-token]
    [attr-token]
    subject-token
    return-token
    <non-file descriptor>
    header-token
    argument-token  (1, "no path: fd", fd)
    argument-token  (2, "operation", operation)
    subject-token
    return-token

fpathconf
system call fpathconf see fpathconf(2)
event ID 327  AUE_FPATHCONF
event class fa  (0x00000004)
audit record
    <valid file descriptor>
    header-token
    [path-token]
    [attr-token]
    subject-token
return-token
<non-file descriptor>
header-token
argument-token (1, "no path:fd:", fd)
subject-token
return-token

fstat
system call fstat  see fstat(2)
event ID 326  AUE_FSTAT
event class fa  (0x00000004)
audit record
<valid file descriptor>
header-token
[path-token] [attr-token]
subject-token
return-token
<non-file descriptor>
header-token
argument-token (1, "no path:fd:", fd)
subject-token
return-token

ftruncate
system call ftruncate see ftruncate(2)
event ID 330  AUE_FTRUNCATE
event class fm  (0x00000008)
audit record
<valid file descriptor>
header-token
[path-token] [attr-token]
subject-token
return-token
<non-file descriptor>
header-token
argument-token (1, "no path:fd:", fd)
subject-token
return-token

futimes
system call futimes see futimes(2)
event ID 318  AUE_FUTIMES
event class  (0x00000009)
audit record
<valid file descriptor>
header-token
[path-token] [attr-token]
subject-token
getattriblist
system call  getattriblist
event ID  335  AUE_GETATTRLIST
event class fa  (0x00000004)
audit record
  header-token
  path-token
  [attr-token]
  subject-token
  return-token

getdirentries
system call  getdirentries  see getdirentries(2)
event ID  328  AUE_GETDIRENTRIES
event class fr  (0x00000001)
audit record
  <valid file descriptor>
  header-token
  [path-token]
  [attr-token]
  subject-token
  return-token
  <non-file descriptor>
  header-token
  argument-token  (1, "no path:fd:", fd)
  subject-token
  return-token

getdirentriesattr
system call  getdirentriesattr
event ID  337  AUE_GETDIRENTRIESATTR
event class fa  (0x00000004)
audit record
  <valid file descriptor>
  header-token
  [path-token]
  [attr-token]
  subject-token
  return-token
  <non-file descriptor>
  header-token
  argument-token  (1, "no path:fd:", fd)
  subject-token
  return-token
getfh
    system call  getfh see getfh(2)
    event ID  322  AUE_GETFH
    event class fa  (0x00000004)
    audit record
        header-token
        path-token
        [attr-token]
        subject-token
        return-token

getfsstat
    system call  getfsstat see getfsstat(2)
    event ID  301  AUE_GETFSSTAT
    event class fa  (0x00000004)
    audit record
        header-token
        subject-token
        return-token

init_process
    system call  init_process
    event ID  356  AUE_INITPROCESS
    event class pc  (0x00000080)
    audit record
        header-token
        subject-token
        return-token

kdebug_trace
    system call  kdebug_trace
    event ID  325  AUE_KDEBUGTRACE
    event class pc  (0x00000080)
    audit record
        header-token
        subject-token
        return-token

ktrace
    system call  ktrace see ktrace(2)
    event ID  306  AUE_KTRACE
    event class pc  (0x00000080)
    audit record
        <valid process ID>
        header-token
        argument-token  (2, "ops", ops)
        argument-token  (3, "trpoints", trpoints)
        process-token
        path-token
        [attr-token]
loadsharedfile
  system call  load_shared_file  
  event ID  347  AUE_LOADSHFILE  
  event class fr  (0x00000001)  
  audit record  
    header-token  
    argument-token  (4, "base addr", ba)  
    path-token  
    [attr-token]  
    subject-token  
    return-token

map_fd
  system call  map_fd  
  event ID  357  AUE_MAPFD  
  event class no  (0x00000000)  
  audit record  
    <valid file descriptor>  
    header-token  
    argument-token  (3, "va", va)  
    [path-token]  
    [attr-token]  
    subject-token  
    return-token  
    <non-file descriptor>  
    header-token  
    argument-token  (3, "va", va)  
    argument-token  (1, "no path:fd:", fd)  
    subject-token  
    return-token

minherit
  system call  minheri  see minherit(2)  
  event ID  340  AUE_MINHERIT  
  event class pc  (0x00000080)  
  audit record  
    header-token  
    argument-token  (1, "addr", addr)  
    argument-token  (2, "len", memory segment size)
Appendix B  Audit Record Format

mkfifo
system call  mkfifo  see mkfifo(2)
event ID  315  AUE_MKFIFO
event class fc  (0x00000010)
audit record
  header-token
  path-token
  [attr-token]
  subject-token
  return-token

mlock
system call  mlock  see mlock(2)
event ID  332  AUE_MLOCK
event class no  (0x00000000)
audit record
  header-token
  subject-token
  argument-token  (1, "addr", addr)
  argument-token  (2, "len", memory segment size)
  return-token

mmap
system call  mmap  see mmap(2)
event ID  210  AUE_MMAP
event class no  (0x00000000)
audit record
  <valid file descriptor>
    header-token
    argument-token  (1, "addr", segment addr)
    argument-token  (2, "len", segment length)
    [path-token]
    [attr-token]
    subject-token
    return-token
  <non-file descriptor>
    header-token
    argument-token  (1, "addr", segment addr)
    argument-token  (2, "len", segment length)
    argument-token  (1, "no path:fd:", fd)
    subject-token
    return-token
mprotect
system call mprotect see mprotect(2)
event ID 311 AUE_MPROTECT
event class (0x00000008)
audit record
  header-token
  argument-token (1, "addr", address of memory)
  argument-token (2, "len", memory segment size)
  argument-token (3, "protection", protection)
  subject-token
  return-token

munlock
system call munlock see munlock(2)
event ID 333 AUE_MUNLOCK
event class no (0x00000000)
audit record
  header-token
  subject-token
  argument-token (1, "addr", addr)
  argument-token (2, "len", memory segment size)
  return-token

newsystemsharedregions
system call new_system_shared_regions
event ID 349 AUE_NEWSYSTEMSHREG
event class ot (0x00010000)
audit record
  header-token
  subject-token
  return-token

nfssvc
system call nfssvc see nfssvc(2)
event ID 321 AUE_NFSSVC
event class ot (0x00010000)
audit record
  header-token
  subject-token
  return-token

open
system call open see open(2)
event ID 72 AUE_OPEN_R
event class fr (0x00000001)
event ID 73 AUE_OPEN_RC
event class fc,fr (0x00000011)
event ID 75 AUE_OPEN_RTC
event class fc,fd,fr (0x00000031)
event ID 74 AUE_OPEN_RT
event class fd,fr (0x00000021)
  event ID 80 AUE_OPEN_RW
  event class fr,fw (0x00000003)
  event ID 81 AUE_OPEN_RWC
  event class fr,fw,fc (0x00000013)
  event ID 83 AUE_OPEN_RWTC
  event class fr,fw,fc,fd (0x00000033)
  event ID 82 AUE_OPEN_RWT
  event class fr,fw,fd (0x00000023)
  event ID 76 AUE_OPEN_W
  event class fw (0x00000002)
  event ID 77 AUE_OPEN_WC
  event class fw,fc (0x00000012)
  event ID 79 AUE_OPEN_WTC
  event class fw,fc,fd (0x00000032)
  event ID 78 AUE_OPEN_WT
  event class fw,fd (0x00000022)

audit record
header-token
path-token  path provided to system call
  [path-token]  path as the kernel knows it, if valid
[vnode-token]
sms-token
subject-token

pid_for_task
  system call  pid_for_task
  event ID 359 AUE_PIDFORTASK
  event class pc (0x00000080)
  audit record
header-token
argument-token  (1, "port", target port)
  [argument-token]  (2, "pid", returned PID)
sms-token
subject-token
return-token

pthread_kill
  system call  __pthread_kill  see pthread_kill(2)
  event ID 350 AUE_PTHREADKILL
  event class pc (0x00000080)
  audit record
header-token
argument-token  (1, "thread port", thread_port)
sms-token
subject-token
return-token

pthread_sigmask
  system call  pthread_sigmask  see pthread_sigmask(2)
  event ID 351 AUE_PTHREADSIGMASK
  event class pc (0x00000080)
  audit record

header-token
subject-token
return-token

profile
system call profil see profil(2)
event ID 305 AUE_PROFILE
event class pc (0x00000080)
audit record
header-token
argument-token (4, "scale", scale)
subject-token
return-token

ptrace
system call ptrace see ptrace(2)
event ID 302 AUE_PTRACE
event class pc (0x00000080)
audit record
<valid process ID>
header-token
argument-token (1, "request", request)
argument-token (3, "addr", addr)
argument-token (4, "data", data)
process-token
subject-token
return-token
<invalid process ID>
header-token
argument-token (1, "request", request)
argument-token (3, "addr", addr)
argument-token (4, "data", data)
argument-token (2, "pid", pid)
subject-token
return-token

quotactl
system call quotactl see quotactl(2)
event ID 323 AUE_QUOTACTL
event class ad (0x00000080)
audit record
header-token
argument-token (2, "command", cmd)
argument-token (3, "uid", id)
path-token
[attr-token]
subject-token
return-token

reboot
system call reboot see reboot(2)
event ID 308  AUE_REBOOT
event class ad
audit record
    header-token
    argument-token (1, "howto", howto)
    subject-token
    return-token

recvmsg
system call recvmsg see recvmsg(2)
event ID 190  AUE_RECVMSG
event class nt (0x00000100)
audit record
    header-token
    argument-token (1, "fd", file descriptor)
<socket-inet token> if AF_INET socket
<path token> if AF_UNIX socket
<path token> canonical path of socket file
    subject-token
    return-token

recvfrom
system call recvfrom see recvfrom(2)
event ID 191  AUE_RECVFROM
event class nt (0x00000100)
audit record
    header-token
    argument-token (1, "fd", file descriptor)
<socket-inet token> if AF_INET socket
<path token> if AF_UNIX socket
<path token> canonical path of socket file
    subject-token
    return-token

resetsharedfile
system call reset_shared_file
event ID 348  AUE_RESETSHFILE
event class ot (0x00010000)
audit record
    header-token
    argument-token (1, "base addr", ba)
    subject-token
    return-token

revoke
system call revoke see revoke(2)
event ID 309  AUE_REVOKE
event class cl
audit record
    header-token
    path-token

Appendix B  Audit Record Format
searchfs
system call searchfs
event ID 339 AUE_SEARCHFS
event class fa (0x00000004)
audit record
header-token
path-token
[attr-token]
subject-token
return-token

semclose
system call sem_close see sem_close(2)
event ID 343 AUE_SEMCLOSE
event class ip (0x00000200)
audit record
header-token
argument-token (1, "sem", sem)
subject-token
return-token

semconfig
system call semconfig
event ID 341 AUE_SEMCONFIG
event class ip (0x00000200)
audit record
header-token
subject-token
return-token

semopen
system call sem_open see sem_open(2)
event ID 342 AUE_SEMOPEN
event class ip (0x00000200)
audit record
header-token
text-token (semaphore name)
argument-token (2, "flags", flags)
argument-token (3, "mode", mode)
argument-token (4, "value", value)
[ipc_perm-token]*
subject-token
return-token

semunlink
system call sem_unlink see sem_unlink(2)
event ID 344 AUE_SEMUNLINK
Appendix B  Audit Record Format

event class ip  (0x00000200)
audit record
  header-token
text-token  (semaphore name)
  [ipc_perm-token]*
subject-token
return-token

setattrlist
  system call  setattrlist
  event ID  336  AUE_SETATTRLIST
event class  (0x00000008)
audit record
  header-token
  path-token
  [attr-token]
  subject-token
return-token

shmopen
  system call  shm_open  see shm_open(2)
event ID  345  AUE_SHMOPEN
event class ip  (0x00000200)
audit record
  header-token
text-token  (shared memory object name)
  argument-token  (2, "flags", flags)
  argument-token  (3, "mode", mode)
  [ipc_perm-token]*
subject-token
return-token

shmunlink
  system call  shm_unlink  see shm_unlink(2)
event ID  346  AUE_SHMUNLINK
event class ip  (0x00000200)
audit record
  header-token
text-token  (shared memory object name)
  [ipc_perm-token]*
subject-token
return-token

sendmsg
  system call  sendmsg  see sendmsg(2)
event ID  188  AUE_SENDMSG
event class nt  (0x00000100)
audit record
  header-token
  argument-token  (1, "fd", file descriptor)
<socket-inet token>if AF_INET socket
<path token>if AF_UNIX socket
<path token> canonical path of socket file
subject-token
return-token

sendto
system call sendto see sendto(2)
event ID 184 AUE_SENDTO
event class nt (0x00000100)
audit record
  header-token
  argument-token (1, "fd", file descriptor)
  <socket-inet token> if AF_INET socket
  <path token> if AF_UNIX socket
  <path token> canonical path of socket file
subject-token
return-token

setlogin
system call setlogin see setlogin(2)
event ID 307 AUE_SETLOGIN
event class lo (0x00001000)
audit record
  header-token
  [text-token] (login name)
subject-token
return-token

setprivexec
system call setprivexec
event ID 320 AUE_SETPRIVEXEC
event class pc (0x00000100)
audit record
  header-token
  argument-token (1, "flag", flag)
subject-token
return-token

setpriority
system call setpriority see priority(2)
event ID 312 AUE_SETPRIORITY
event class pc, ot (0x00001080)
audit record
  header-token
  argument-token (1, "which", which)
  argument-token (2, "who", who)
  argument-token (3, "priority", priority)
subject-token
return-token

setsid
system call setsID    see setsid(2)
event ID 319  AUE_SETSID
event class pc  (0x00000100)
audit record
  header-token
  subject-token
  return-token

setsockopt
system call setsockopt see setsockopt(2)
event ID 35  AUE_SETSOCKOPT
event class nt  (0x00000100)
audit record
  header-token
  argument-token  (1, "fd", file descriptor)
  subject-token
  return-token

settimeofday
system call settimeofday see settimeofday(2)
event ID 313  AUE_SETTIMEOFDAY
event class ad  (0x00000800)
audit record
  header-token
  subject-token
  return-token

shutdown
system call shutdown see shutdown(2)
event ID 46  AUE_SHUTDOWN
event class ad  (0x00000800)
audit record
  header-token
  argument-token  (1, "fd", file descriptor)
  subject-token
  return-token

socket
system call socket see socket(2)
event ID 183  AUE_SOCKET
event class nt  (0x00000100)
audit record
  header-token
  argument-token  (1, "domain", d)
  argument-token  (2, "type", type)
  argument-token  (3, "protocol", protocol)
  subject-token
  return-token

socketpair
system call socketpair see socketpair(2)
event ID  317  AUE_SOCKETPAIR
event class nt  (0x00000100)
audit record
  header-token
  argument-token  (1, "domain", d)
  argument-token  (2, "type", type)
  argument-token  (3, "protocol", protocol)
subject-token
return-token

swapoff
  system call  macx_swapoff
  event ID  355  AUE_SWAPOFF
  event class ad  (0x00000800)
audit record
  header-token
  path-token
  [attr-token]
subject-token
return-token

swapon
  system call  macx_swapon
  event ID  28  AUE_SWAPON
  event class ad  (0x00000800)
audit record
  header-token
  argument-token  (4, "priority", priority)
  path-token
  [attr-token]
subject-token
return-token

sysctl
  system call  __sysctl  see sysctl(3)
  event ID  331  AUE_SYSCTL
  event class ad  (0x00000800)
audit record
  header-token
  subject-token
  argument-token  (1, "name", name) [one for each name segment]
  [argument-token]  (5, "newval", newval) [new value is integer]
  [text-token]  [new value is a string]
return-token

task_for_pid
  system call  task_for_pID
  event ID  358  AUE_TASKFORPID
  event class pc  (0x00000080)
audit record
  header-token
<valid process ID>
argument-token (1, "target port", target port)
argument-token (3, "task port", returned task port)
process-token
subject-token
return-token
<valid process ID>
argument-token (1, "target port", target port)
argument-token (2, "process", pid)
subject-token
return-token

truncate
system call truncate see truncate(2)
event ID 329  AUE_TRUNCATE
event class (0x00000008)
audit record
header-token
path-token
[attr-token]
subject-token
return-token

umask
system call umask see umask(2)
event ID 310  AUE_UMASK
event class pc (0x00000080)
audit record
header-token
argument-token (1, "new mask", numask)
argument-token (0, "prev mask", previous mask)
subject-token
return-token

undelete
system call undelete see undelete(2)
event ID 334  AUE_UNDELETE
event class (0x00000008)
audit record
header-token
path-token
[attr-token]
subject-token
return-token
Using Terminal

This appendix describes how to use Terminal to execute UNIX commands, run UNIX utilities, and view online information about commands and utilities.

To access a UNIX shell command prompt, you open the Terminal application. In Terminal, you can enter commands and run command-line utilities. You can use the `man` command to view online documentation for most common commands.

Notation Conventions
The following conventions are used for UNIX commands and utilities throughout this book.

Summary

<table>
<thead>
<tr>
<th>Notation</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>monospaced font</td>
<td>A command or other terminal text</td>
</tr>
<tr>
<td>[text_in_brackets]</td>
<td>An optional parameter</td>
</tr>
<tr>
<td>(one</td>
<td>other)</td>
</tr>
<tr>
<td>underlined</td>
<td>A parameter you must replace with a value</td>
</tr>
<tr>
<td>[...]</td>
<td>A parameter that may be repeated</td>
</tr>
<tr>
<td>&lt;anglebrackets&gt;</td>
<td>A displayed value that depends on the computer’s configuration</td>
</tr>
</tbody>
</table>

Commands and Other Terminal Text
Commands or command parameters that you might enter, along with other text that normally appears in a Terminal window, are shown in this font. For example,

You can use the `doit` command to get things done.

Each command you can enter is shown on a line by itself. For example,

`doit`

To use this command, enter “doit” at the command prompt in a Terminal window, then press the Return key.
Command Parameters and Options
Most commands require one or more parameters to specify command options or the item to which the command is applied.

Parameters You Must Enter as Shown
If you need to enter a parameter as shown, it appears following the command in the same font. For example,

doit -w later -t 12:30

To use the command in the above example, enter the entire line as shown.

Parameter Values You Provide
If you need to supply a value, its placeholder is underlined and has a name that indicates what you need to provide. For example,

doit -w later -t hh:mm

In the above example, you need to replace \texttt{hh} with the hour and \texttt{mm} with the minute, as shown in the previous example.

Optional Parameters
If a parameter is available but not required, it appears in square brackets. For example,

doit [-w later]

To use the command in the above example, enter either \texttt{doit} or \texttt{doit -w later}. The result might vary but the command will be performed either way.

Alternative Parameters
If you need to enter one of a number of parameters, they’re separated by a vertical line and grouped within parentheses (|). For example,

doit -w (now|later)

To perform the command, you must enter either \texttt{doit -w now} or \texttt{doit -w later}.

Using Terminal
To enter shell commands or run command-line tools and utilities, you need access to a UNIX shell prompt. Both Mac OS X and Mac OS X Server include Terminal, an application you can use to start a UNIX shell command-line session on the computer.

To open Terminal:
- Double-click the Terminal application icon in the Finder, located in the Utilities folder in the Applications folder.

Terminal presents a prompt when it’s ready to accept a command. The prompt you see depends on Terminal and shell preferences, but often includes the name of the host you’re logged in to, your current working directory, your user name, and a prompt symbol. For example, if you’re using the default bash shell and the prompt is
mycomputer:~ admin$

you’re logged in to a computer named “mycomputer” as the user named “admin” and your current directory is the admin’s home directory (~).

**To enter a command:**
- Wait for a prompt to appear in the Terminal window, then enter the command and press Return.

If you get the message “command not found,” check your spelling.

**Correcting Typing Errors**
To correct a typing error before you press Return to issue the command, use the Delete key or press Control-H to erase unwanted characters and reenter.

To ignore what you have entered and start again, press Control-U.

**Repeating Commands**
To repeat a command, press Up Arrow until you see the command, then press Return.

To repeat a command with modifications, press Up Arrow until you see the command, press Left Arrow or Right Arrow to skip over parts of the command you don’t want to change, press Delete to remove characters, enter the desired characters, then press Return to execute the command.

**Including Paths Using Drag-and-Drop**
To include a fully qualified file name or directory path in a command, stop typing where the item is required in the command and drag the folder or file from a Finder window into the Terminal window.

**Commands Requiring Root or Administrator Privileges**
Some commands used to manage a computer must be executed by an administrator user or the root user. If you get a message such as “permission denied,” the command probably requires root privileges.

You can execute one command at a time as the root user, which is an administrator implicitly, by beginning each command with `sudo`. For example:

```bash
sudo passwd newuser
```

To use `sudo`, you must be logged in as an administrator.

If you haven’t used `sudo` recently, you’re prompted to enter the administrator password.
Editing Settings Files
Files containing audit settings can be edited with any text editor. Terminal may be used in conjunction with Vi or emacs text editor tools included with Mac OS X.

For more information on using text editors with Terminal, see the vi or emacs man pages by entering:

```
man vi
```

or

```
man emacs
```
Getting Online Help for Commands

Onscreen help is available for most commands and utilities.

*Note:* Not all techniques work for all commands, and some commands have no onscreen help.

To view onscreen information about a command, try the following:

- **Enter the command without any parameters or options.** This will often list a summary of options and parameters you can use with the command.
  
  *Example:*
  
  ```
  sudo dscl
  ```

- **Enter `man command`, where `command` is the command you’re curious about.** This usually displays detailed information about the command, its options, parameters, and proper use.
  
  *Example:*
  
  ```
  man dscl
  ```

  For help using the `man` command, enter:

  ```
  man man
  ```

- **Enter the command followed by a `-help`, `-h`, `--help`, or `help` parameter.**
  
  *Examples:*
  
  ```
  chown help
  vi -h
  mkdir --help
  ```

Manpage General Info

The man pages for the system calls: shmat, shmget, and shmcti, contain an incorrect statement concerning the permissions required to operate on shared memory.

When operating on shared memory, the write permission bit for others is not applied. (i.e. when the uid or gid of the calling application does not match the uid or gid of the shared memory segment)

The man page for the system call: semop, contains an incorrect statement concerning the permissions required to perform the semop operation on a semaphore. The caller must always possess write permissions to operate on the semaphore.
For the notifyd(8) man page, only the -d and -shm_pages options are correctly described. The rest of the man page options are incorrect. notifyd(8) is the server for the Mac OS X notification system described in notify(3). It supports Darwin notifications by listening for incoming notifications and redelivering those notifications to interested processes in a variety of ways. notifyd(8) checks a client's read access to a key at the time the client registers. However, if the key's access change after the client registers, notifyd continues to allow the client read access.
The notifyd reads configuration data from notify.conf file. notify.conf contains configuration information for notification names that can be registered with the notifyd daemon. This file must be owned by root and must not be world writable.

Lines starting with ‘#’ and empty lines are interpreted as comments. The configuration parameters on each line are separated by either tabs or blank characters. The first word of a configuration line is the keyword specifying the rule type. The second word is the notification name the rule applies to. The notification name can specify one specific notification name or a complete subtree of notification names. A specific notification name can be identified by a name without a trailing dot. A complete subtree is specified by a trailing dot for the notification name. In the given example,

"com.apple.system.timezone" is a specific destination name the rule applies to. The rule specifying "com.apple.system." applies to all notification names which start with "com.apple.system.".

The remaining arguments for each rule depend on the chosen rule type. The following possible rule types can be configured. This list describes the purpose of each keyword and the allowed options that follow the notification name.

**monitor**

The monitor keyword allows the specification of a file which is monitored for changes. The file must be owned by root and the owning group must also be root. Notification clients that have registered for the configured notification name receive a notification when the monitored file changes.

**set**

The set keyword allows the specification of a state value for the corresponding notification name. The state value can be a 64-bit integer value which is maintained for the notification name.
**reserve**
The reserve keyword allows the specification of access rights for a notification name. The first option in the rule that follow the notification name specifies the owning UID of the notification name. The second option specifies the owning GID of the notification name. The last value specifies the permissions that are enforced for sending an receiving notifications using the notification name. The permissions are similar to UNIX permission bits, except that the execution bit is missing: the first doublet of the character string specifies the permissions if the UID of the process sending or receiving notifications is equal to the owning UID specified for the notification name. The second doublet specifies the permissions if the GID of the process sending or receiving notifications is equal to the owning GID specified for the notification name. The last doublet specifies the permissions if the UID and GID of the process sending or receiving notifications is not equal to the owning UID or GID specified for the notification name.

Allowed permissions are:
- r for allowing to receive (read) notifications,
- w for allowing to send (write) notifications,
- - for disallowing either r or w.

**quit**
The quit keyword terminates the parsing of the configuration file. All rules before the quit keyword are read and applied. All trailing configuration rules are skipped.

**EXAMPLES**
The following configuration rules are examples:
- All notification names below com.apple.system are owned by root, everybody can receive notifications, but only root is allowed to send notifications reserve com.apple.system.0 0 rwr-r-
- The file /etc/localtime is watched and when it changes, a notification is sent to com.apple.system.timezone monitor com.apple.system.timezone /etc/localtime

**SEE ALSO**
notify 3,
notifyd 8