Apple Security Checklist Companion

2nd Edition

A practical guide for automating security standards in the Apple Enterprise with the Casper Suite

September 2009

JAMF Software has made all efforts to ensure that this guide is accurate.

JAMF Software
1011 Washington Ave South
Suite 350
Minneapolis, MN 55415
(612) 605-6625

Contents

Introduction

Target Audience

The Apple Security Checklist Companion (ASCC) is intended for IT practitioners engaged in governance, compliance and security related to Macintosh OS X computers.

How to Use This Guide

The ASCC is a companion document to be used in conjunction with Mac OS X Security Configuration Guide For Version 10.5 Leopard (v.2) published in January of 2009. Please download a copy from the link found below and become familiar with the security guidelines set forth by Apple with contributions made by the NSA, NIST and DISA.

Using Apple's guidelines as the authoritative source for security standards on Mac OS X, the ASCC provides you with an index of how to automate compliance with these standards using the Casper Suite.

Acknowledgements

JAMF Software would like to thank Apple Computer for not only publishing the security guide, but for the guidance they have provided regarding security on the platform. Additionally, we'd like to thank the security experts from our customer community for the insights that they have lent us as we have grown our understanding in this increasingly critical area for the Mac OS.

Regulatory Compliance Frameworks

The increased need for security automation is driven by organizations looking to provide a more secure computing environment as well as being driven by regulatory mandates.

For government institutions, the current iteration of the Federal Desktop Core Configuration (FDCC) does not include Mac OS computers. For those in the public sector, Sarbanes-Oxley requirements are not clearly articulated for Apple hardware, leaving the responsible system administrator at a loss for how to comply specifically when administering Apple hardware.

This companion document follows the Apple guide in providing a "How to automate..." the What and the Why provided by Apple. As standards continue to emerge, this document will be updated to reflect the evolving landscape of security on Mac OS platform. Appendix A looks more in depth at Sarbanes-Oxley controls and supercedes the document titled "Security and Casper."

Useful Links on Security Concerns

Mac OS X Security Configuration Guides

http://www.apple.com/support/security/guides/

Mac OS X v10.5 (Leopard)

Mac OS X Security Configuration Guide *
Mac OS X Server Security Configuration Guide

Mac OS X v10.4 (Tiger)

Mac OS X Security Configuration Guide
Mac OS X Server Security Configuration Guide

Mac OS X v10.3 (Panther)

Client Security Configuration Guide
Server Security Configuration Guide

* There are additional links found within each of these guides. As a matter of practicality, this document is based on the Mac OS X v10.5 (Leopard) security guide and the links found on pages 16 and 17 provide a wealth of information from Apple and US Government agencies and should be pursued as part of any inquiry into securing Mac OS client machines.

Installing Mac OS X

For hardening security on Mac OS X systems and maintaining the security Apple provides the Mac OS X Security Configuration guide as a source of instructions and recommendations. By using The Casper Suite your chosen security configuration can be implemented and maintained throughout the life cycle of your managed Macs. This document, which is based off of the Apple Security Checklist (ASC) that is included in the Mac OS X Security Configuration guide, details the deployable objects and the Casper Suite deployment mechanisms that can be used to implement Apple's recommended security actions.

Installation Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Securely erase the Mac OS X partition before installation	29	Script	Casper Imaging
Install Mac OS X using Mac OS Extended disk formatting	20	OS Image	Casper Imaging
Do not install unnecessary packages	30	OS Image	Casper Imaging
Do not transfer confidential information in Setup Assistant	32	OS Image	Casper Imaging
Do not connect to the Internet	31	OS Image, Stand Alone JSS	Casper Imaging and JSS on a FireWire drive
Create administrator accounts with difficult-to-guess names	33	Script, DMG	Casper Imaging, Casper Remote, Policy
Create complex passwords for administrator accounts	33	N/A	All Casper Suite products have support for complex passwords.
Do not enter a password-related hint; instead, enter help desk contact information	33	Script, Managed Preference	Casper Remote, Policy
Enter correct time settings	33, 91	Script, DMG	Casper Imaging, Casper Remote, Policy
Use an internal Software Update server	34	Setting, Managed Preference	JSS
Update system software using verified packages	37	Software Update Server PKG, DMG HTTP Downloads	Casper Imaging, Casper Remote, Policy
Repair disk permissions after installing software or software updates	37	Setting	Casper Imaging, Casper Remote, Policy

Protecting System Hardware

When hardening Mac OS X desktop systems after installation, protect your system hardware with the following:

Action Items from **ASC Page** are managed by a **Deployable Object** using the appropriate **Deployment Mechanism**.

Hardware Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Restrict access to rooms that have computers	N/A	N/A	N/A
Store computers in locked or secure containers when not in use	N/A	N/A	N/A
Disable Wi-Fi Support Software	43	Script-Complete Removal, Managed Preference-Disable Only	Casper Imaging, Casper Remote, Policy, Resource Kit
Disable Bluetooth Support Software	44	Script-Complete Removal, Managed Preference-Disable Only	Casper Imaging, Casper Remote, Policy, Resource Kit
Disable Audio Recording Support Software	46	Script	Casper Imaging, Casper Remote, Policy
Disable Video Recording Support Software	47	Script	Casper Imaging, Casper Remote, Policy
Disable USB Support Software	48	Script	Casper Imaging, Casper Remote, Policy, Resource Kit
Disable FireWire Support Software	49	Script	Casper Imaging, Casper Remote, Policy

Securing Global System Settings

When hardening Mac OS X desktop systems during installation, initialization or updating, reference the following:

Action Items from **ASC Page** are managed by a **Deployable Object** using the appropriate **Deployment Mechanism**.

Global System Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Require an Open Firmware or EFI password	55	DMG, OS Image, Script	Casper Imaging, Casper Remote, Policy
Create an access warning for the login window	57	DMG, OS Image, Script, *Managed Preference	Casper Imaging, Casper Remote, Policy
Create an access warning for the command line	59	DMG, OS Image, Script	Casper Imaging, Casper Remote, Policy

Securing Accounts

When hardening Mac OS X desktop systems during installation, initialization or updating, reference the following:

Action Items from **ASC Page** are managed by a **Deployable Object** using the appropriate **Deployment Mechanism**.

Account Configuration Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Create an administrator account and a standard account for each administrator	61	JSS Setting, QuickAdd, Script	Casper Imaging, Casper Remote
Create a standard or managed account for each nonadministrator	64	QuickAdd, Script	Casper Imaging, Casper Remote, Policy
Set parental controls for managed accounts	64	Script, DMG, Managed Preference	Casper Imaging, Casper Remote, Policy
Restrict sudo users to access required commands	69	Script, DMG	Casper Imaging, Casper Remote, Policy
Securely configure LDAPv3 access	72	Script, DMG	Casper Imaging, Casper Remote, Policy
Securely configure Active Directory access	72	Script, DMG	Casper Imaging, Casper Remote, Policy
Use Password Assistant to generate complex passwords	73	Setting	Casper Remote, Policy
Authenticate using a smart card, token, or biometric device	75, 76	DMG	Casper Imaging, Casper Remote, Policy
Set a strong password policy	77	Script, Unix Command	Casper Imaging, Casper Remote, Policy
Secure the login keychain	78	Script, Unix Command	Casper Imaging, Casper Remote, Policy
Secure keychain items	80	Script, Unix Command	Casper Imaging, Casper Remote, Policy
Create keychains for specialized purposes	79	Script, Unix Command	Casper Imaging, Casper Remote, Policy
Use a portable drive to store keychains	82	DMG	Casper Imaging, Casper Remote, Policy

Securing System Preferences

When hardening Mac OS X desktop systems during installation, initialization or updating, reference the following:

Action Items from **ASC Page** are managed by a **Deployable Object** using the appropriate **Deployment Mechanism**.

System Preferences Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Log in with administrator privileges	86	Script, DMG, *Managed Preference	Casper Imaging, Casper Remote, Policy
Enable MobileMe only for user accounts without access to critical data	87	Script, DMG, *Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure MobileMe preferences	87	Script, DMG, *Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Accounts preferences	89	Script, DMG, *Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Appearance preferences	92	Script, DMG, Managed Preference	Casper Imaging, Casper Remote, Policy
Change the number of recent items displayed	93	Script, DMG, Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Bluetooth preferences	94	Script, DMG, *Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure CD & DVD preferences	95	Script, DMG, *Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Date & Time preferences	96	Script	Casper Imaging, Casper Remote, Policy
Securely configure Desktop & Screen Saver preferences	97	Script, User Environment Package, *Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Display preferences	99	Script, Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Dock preferences	99	Script, User Environment Package, Unix Command, Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Energy Saver preferences	100	Script, Resource Kit, Managed Preference	Casper Imaging, Casper Remote, Policy
Configure Exposé & Spaces Preferences	102	Script, Unix Command	Casper Imaging, Casper Remote, Policy
Securely configure Keyboard & Mouse preferences	103	Script, Unix Command, Managed Preference	Casper Imaging, Casper Remote, Policy

System Preferences Action Items Cont.

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Securely configure Network preferences	105	Script, User Environment Package, Unix Command	Casper Imaging, Casper Remote, Policy
Securely configure Parental Control preferences	106	DMG, Managed Preference	Casper Imaging, Casper Remote, Policy
Security configure Print & Fax preferences	109	Script, User Environment Package	Casper Imaging, Casper Remote, Policy
Securely configure QuickTime preferences	111	DMG	Casper Imaging, Casper Remote, Policy
Securely configure Security preferences	112	Script, Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Sharing preferences	117	Script, Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Software Update preferences	119	Script, Policy, JSS Setting, User Environment Package, Unix Command	Casper Imaging, Casper Remote, Policy, JSS Setting
Securely configure Sound preferences	120	Script, User Environment Package	Casper Imaging, Casper Remote, Policy
Securely configure Speech preferences	121	Script, Managed Preference	Casper Imaging, Casper Remote, Policy
Securely configure Spotlight preferences	123	Script, Unix Command	Casper Imaging, Casper Remote, Policy
Securely configure Startup Disk preferences	125	Script, Unix Command	Casper Imaging, Casper Remote, Policy
Securely configure Time Machine preferences	126	Script, Unix Command, *Managed Preference	Casper Imaging, Casper Remote, Policy

Securing Data Using Encryption

When hardening Mac OS X desktop systems during installation, initialization or updating, reference the following:

Action Items from **ASC Page** are managed by a **Deployable Object** using the appropriate **Deployment Mechanism**.

Encryption (DAR) Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Assign POSIX access permissions based on user categories	132	Script, Unix Command, Composer Setting	Casper Imaging, Casper Remote, Policy
Review and modify folder flags	132	Script, Unix Command, Composer Setting	Casper Imaging, Casper Remote, Policy
Restrict permissions on User Home Folders	133	Script, Unix Command	Casper Imaging, Casper Remote, Policy
Strip setuid bits from some programs	134	Script, Unix Command, Composer Setting	Casper Imaging, Casper Remote, Policy

Backup Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Securely encrypt and backup your data	156	Script, Managed Preference	Casper Imaging, Casper Remote, Policy

Information Assurance with Applications

When hardening Mac OS X desktop systems during installation, initialization or updating, reference the following:

Action Items from **ASC Page** are managed by a **Deployable Object** using the appropriate **Deployment Mechanism**.

Application Configuration Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Configure Mail using SSL	158	Script, *Managed Preference	Casper Imaging, Casper Remote, Policy
Verify certificate validity	162	Script	Casper Imaging, Casper Remote, Policy
Request MobileMe identity certificate	170	Script	Casper Imaging, Casper Remote, Policy
Secure iChat communications	168	Script, *Managed Preference	Casper Imaging, Casper Remote, Policy
Create a strong password for iTunes	171	N/A	N/A
Secure remote access using VPN	172	DMG, Script, *Managed Preference	Casper Imaging, Casper Remote, Policy
Turn firewall protection on	174	Script, Resource Kit, Managed Preference	Casper Imaging, Casper Remote, Policy

Information Assurance with Services

When hardening Mac OS X desktop systems during installation, initialization or updating, reference the following:

Action Items from **ASC Page** are managed by a **Deployable Object** using the appropriate **Deployment Mechanism**.

Services Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Limit the list of administrators allowed to use sudo	167	OS Image, DMG	Casper Imaging, Casper Remote, Policy
Disable Bonjour	185	Script	Casper Imaging, Casper Remote, Policy
Secure BTMM access through Security Preferences	188	Script, User Environment Package, Managed Preference	Casper Imaging, Casper Remote, Policy
Set up screen sharing through VNC with password protection	190	Script, DMG	Casper Imaging, Casper Remote, Policy
Establish key-based SSH connections	195	Script	Casper Imaging, Casper Remote, Policy
Create an SSH secure tunnel	199	Script	Casper Imaging, Casper Remote, Policy
Configure ARD to manage remote tasks	203	Script, Built In Feature	Casper Imaging, Casper Remote, Policy

Advanced Security Management

When hardening Mac OS X desktop systems during installation, initialization or updating, reference the following:

Action Items from **ASC Page** are managed by a **Deployable Object** using the appropriate **Deployment Mechanism**.

Advance Management Action Items

Action Item	ASC Page	Deployable Object	Deployment Mechanism
Create an authorization right to the dictionary to authorize users	212	Script, Managed Preference	Casper Imaging, Casper Remote, Policy
Create a digital signature	216	Script	Casper Imaging, Casper Remote, Policy
Enable security auditing	221	Script	Casper Imaging, Casper Remote, Policy
Configure security auditing	222	Script	Casper Imaging, Casper Remote, Policy
Generate auditing reports	222	Script	Casper Imaging, Casper Remote, Policy
Enable local logging	219	Script, Managed Preference	Casper Imaging, Casper Remote, Policy
Enable remote logging	220	Script, Managed Preference	Casper Imaging, Casper Remote, Policy
Install a file integrity checking tool	216	DMG	Casper Imaging, Casper Remote, Policy
Create a baseline configuration for file integrity checking	216	OS Image	N/A
Install an antivirus tool	222	DMG	Casper Imaging, Casper Remote, Policy
Configure the antivirus tool to automatically download virus definition files	222	DMG, Managed Preference	Casper Imaging, Casper Remote, Policy

*Available as a template in the JSS

Appendix A - Meeting Sarbanes-Oxley Objectives

There are seven Control Objectives that relate to desktop management under Sarbanes-Oxley requirements that are met through the Casper Suite.

They are:

- Grant the appropriate level of access in order to provide administrators functionality appropriate to their role.
- Log the actions of each individual administrator.
- Ensure that no illegal or unauthorized software can be run on corporate assets by excluding applications from execution.
- Allow remote administrators to observe or control a computer in a way that is secure and audited.
- Rapidly change access credentials for remote computers
- Ensure that desktop screen savers activate after a set amount of time and require a password to unlock.
- Ensure that data transmission is encrypted.

Appendix A - Meeting Sarbanes-Oxley Objectives

While most system administrators governed by Sarbanes-Oxley are fluent in the terminology of the framework, a brief explanation of controls is provided below.

Automated Controls are performed by computers and are binary in nature; they always function as designed and are not subject to intermittent error or human intervention.

Access Controls define the appropriate access for different users and grant them rights and privileges to sensitive information.

Control Objectives define the desired state and are used to measure the success or failure of a policy or procedure.

Corrective Controls are aimed at restoring the system to its expected state.

Detective Controls detect when an unwanted event occurs as a result of human factors as well as en vironmental and security issues; we need detective controls to alert us when an unwanted event transpires.

Preventative Controls are aimed at avoiding unwanted situations.

Role Based Administrator Access

Control Objectives

- Grant the appropriate level of access in order to provide administrators functionality appropriate to their role.
- Log the actions of each individual administrator.

Within the Casper Suite, individuals can be added to the system to perform the tasks for which they are responsible (see fig. 1).

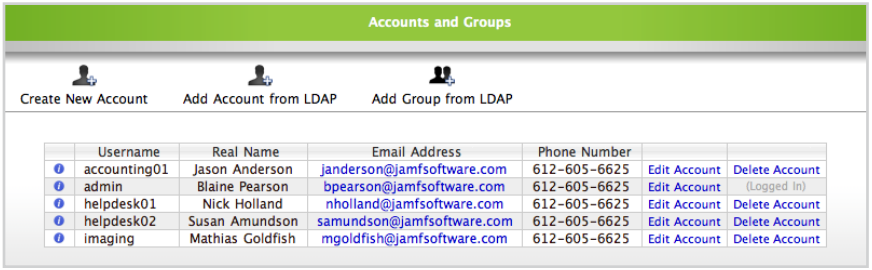


fig. 1

Role Based Administrator Access

These users can be added via LDAP and assigned appropriate privileges (see fig. 2).

	Grant All Privileges Revoke All Privileges
JSS - Home Tab Privileges	
	Change Password
JSS - Inventory Tab Privileges	
	View Inventory Tab
	Perform Advanced Searches
	Save Advanced Searches
	View Saved Searches
	Add Computers Manually
	View Details on Inventory Items
	View License Serial Numbers
	Download Files Attached to Inventory Items
	View Computer Logs
	Edit Inventory Items
	Edit Autorun Data
	Delete Inventory Items
JSS - Management Tab Privileges	
	View Management Tab
	Manage Policies
	Manage PreStages
	Manage Restricted Software
	Manage Smart Computer Groups
	Manage Static Computer Groups
	Manage Management Preferences
	Manage Self Service Preferences
	Manage Scheduled Tasks
	Manage Directory Bindings
	Manage Distribution Points
	Manage Software Update Servers
	Manage NetBoot Servers
JSS - Logs Tab Privileges	
	View Logs Tab
	Flush Policy Histories
JSS - Settings Tab Privileges	
	View Settings Tab
	Manage JSS Accounts
	Manage LDAP Servers
	Manage Buildings and Departments
	Manage Network Segments
	Manage General JSS Settings
	View Database/Web Application Health
	Flush Database Logs
	Mass Edit Locations/Servers
	Mass Edit Warranties
	Mass Edit Autorun Data
	Mass Add SSH Accounts
	Mass Edit SSH Accounts

JSS - Settings Tab Inventory Privileges	
	Manage Inventory Preferences
	Manage Peripheral Types
	Manage Removable MAC Address
	Manage Custom Reports
	Manage Saved Searches
	Manage Licensed Software
	Manage Supressed Inventory Items
Recon Privileges	
	Add Hardware
	Add Computers Remotely
	QuickAdd Packages
Casper Admin Privileges	
	Use Casper Admin
	Save with Casper Admin
Casper Imaging Privileges	
	Use Casper Imaging
	Customize a Configuration
	Store Autorun Data
	Create Local Accounts
	Bind to Active Directory Locally
	Set Open Firmware Locally
	Modify Network Settings Locally
	Set ARD Fields Locally
	Use Advanced Options Locally
Casper Remote Privileges	
	Use Casper Remote
	Install/Uninstall Software Remotely
	Run Scripts Remotely
	Map Printers Remotely
	Add Dock Items Remotely
	Manage Local User Accounts Remotely
	Change Casper's SSH Accounts Remotely
	Bind to Active Directory Remotely
	Set Open Firmware/EFI Passwords Remotely
	Reboot Computers Remotely
	Perform Maintenance Tasks Remotely
	Search for Files/Processes Remotely
VNC Privileges	
	Observe Remote Computers
	Observe Remote Computers Without Asking at Login Window
	Observe Remote Computers Without Asking
	Control Remote Computers
	Control Remote Computers Without Asking at Login Window
	Control Remote Computers Without Asking

fig. 2

Role Based Administrator Access

When an individual administrator logs into any of the Casper Suite applications, his actions are logged in the database. The example provided below illustrates a sample log listing which users controlled a particular desktop computer (see fig. 3). Creating users and assigning their rights falls under Access Control; the logging of events allows for a Procedure that audits the veracity of the Control.

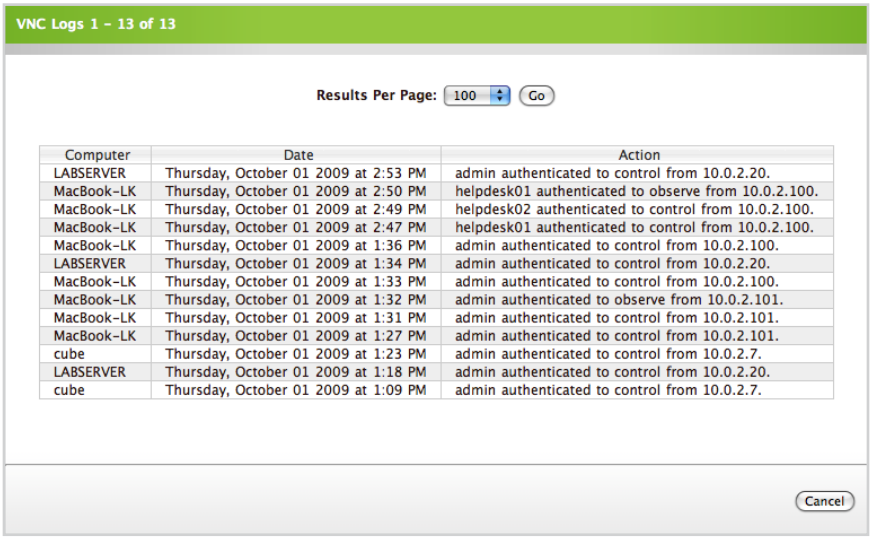


fig. 3

Software Restriction

Control Objectives

- Ensure that no illegal or unauthorized software can be run on corporate assets by blacklisting applications.

Ensuring that software that violates computer usage polices, such as Peer to Peer file sharing applications, are controlled requires the identification and removal of software that is out of scope, and notification about these activities to end user and management. In the case of software restriction (see fig. 4), the Casper Suite offers the following:

- Detection of software by the process that loads into Random Access Memory (RAM), which is a Detective Control.

- Quitting and removing the offending Application, which is a Preventative Control

- Notification to end user and system administrators allows for a Procedure that enforces the Control.

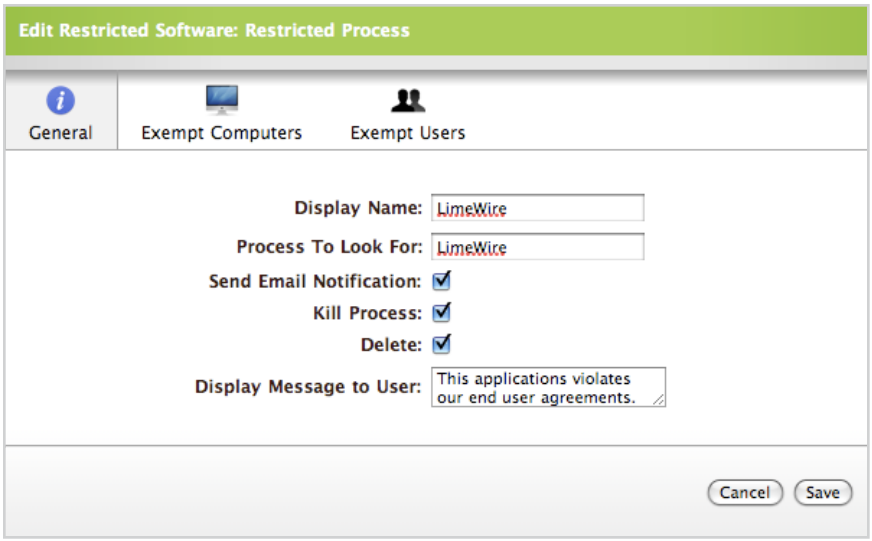


fig. 4

CasperVNC Security

Control Objectives

- Allow remote administrators to observe or control a computer in a way that is secure and audited.

Casper VNC tunnels connections through SSL, which is an Access Control on data transmission from source to host. The VNC server is launched on demand when trying to control or observe a remote client, then quit when the administrator quits the Application. This Preventative Control ensures that only authorized Administrators can access machines during an active session and eliminates concerns about passive reception from intrusion.

Every connection and all remote control, including VNC, are logged centrally in a database as illustrated in fig. 3 above.

With the introduction of Version 6 of the Casper Suite, there is now the additional capability of sending all administrator actions to a CMDB/ syslog server by specifying the directory, hostname and port of the server (see fig. 5).

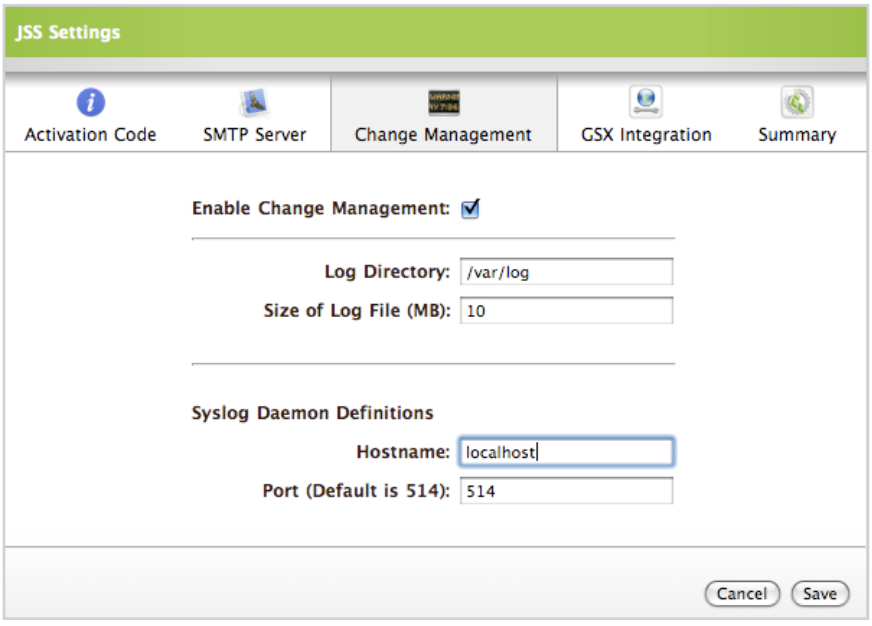


fig. 5

Change Local Administrator Account Password

Control Objectives

- Rapidly change Administrator account access on all computers.

Utilizing the remote features in either the Casper Remote application (see fig. 6) or via a policy (see fig. 7,8,9) the password used to access the remote computers can be updated immediately for the computers that are online and will poll for missing computers until they are found. This Access Control ensures that any security breach involving a compromised administrator can be resolved within minutes.

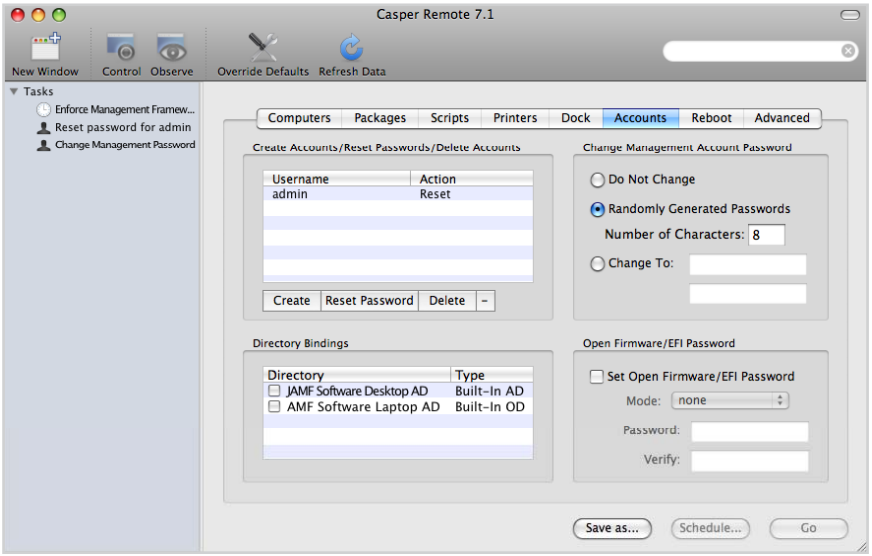


fig. 6

Change Local Administrator Account Password

To change local administrator accounts via a policy, first determine the trigger (start up, login, logout, shut down, time of day, timed frequency, etc.), activation date and execution frequency.

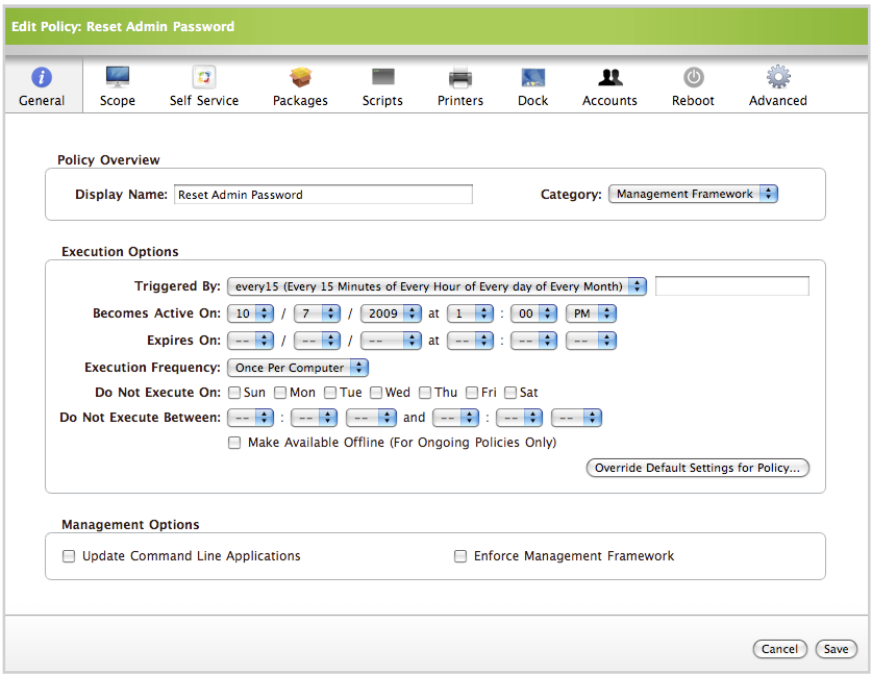


fig. 7

Change Local Administrator Account Password

The next step is to assign computers or groups, in this case we are applying the policy to all computers.

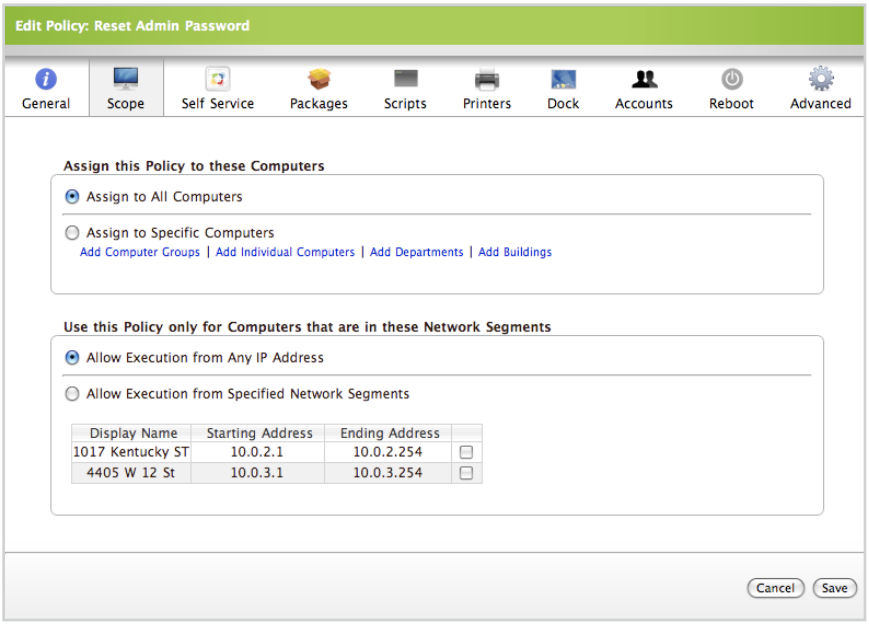


fig. 8

Change Local Administrator Account Password

The last step is to set the command to reset the admin password. In this case we are resetting both the local admin account as well as the account used by the Casper Suite.

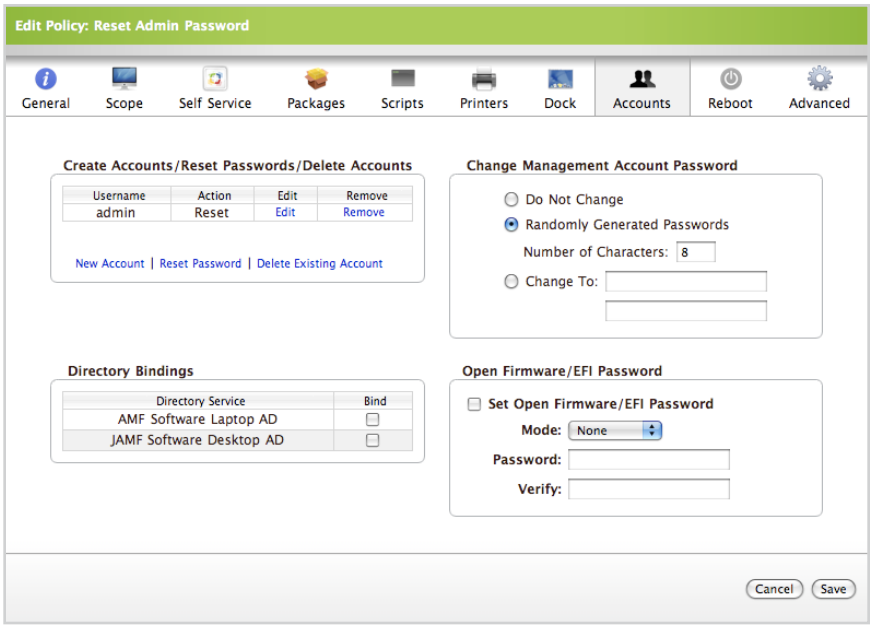


fig. 9

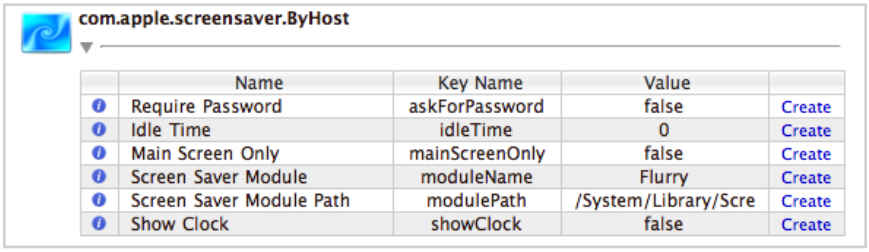
Enforce Screen Saver Settings

Control Objectives

- Ensure that desktop screen saver activates after a set amount of time, and requires a password to be unlocked.

The JAMF Software Server (JSS) can be used to create a Managed Preference that specifies (see fig. 10):

- Screen saver activation
- Idle time until activation
- The screen saver that is displayed



	Name	Key Name	Value	
ⓘ	Require Password	askForPassword	false	Create
ⓘ	Idle Time	idleTime	0	Create
ⓘ	Main Screen Only	mainScreenOnly	false	Create
ⓘ	Screen Saver Module	moduleName	Flurry	Create
ⓘ	Screen Saver Module Path	modulePath	/System/Library/Scre	Create
ⓘ	Show Clock	showClock	false	Create

fig. 10

Enforce Screen Saver Settings

These settings can be applied to target machines at the one of the following levels of enforcement (fig.11):

- User Level Enforced
- User Level at Every Login
- User Level at Next Login Only
- System Level Enforced

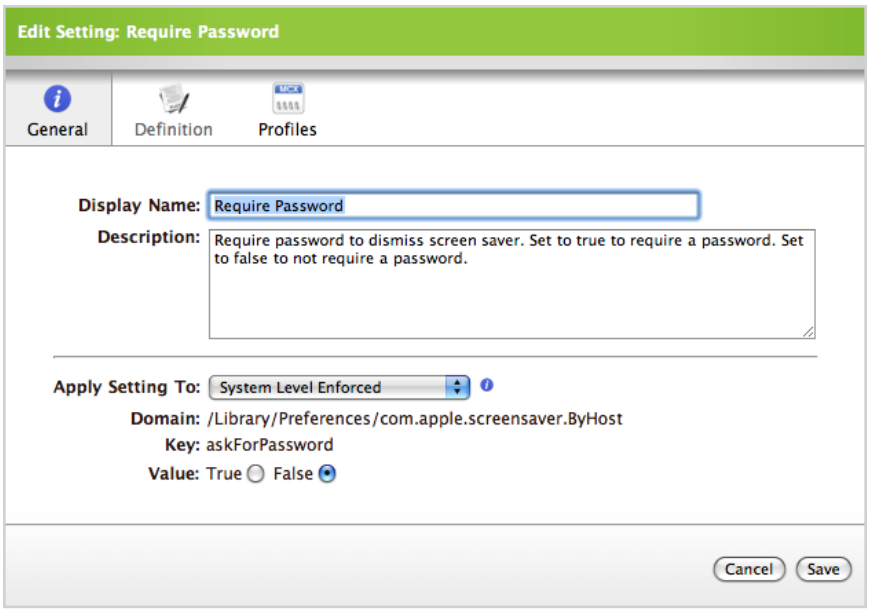


fig. 11

Protocol Security

Control Objectives

- Ensure that data transmission is encrypted.

The central component of the Casper Suite, the JAMF Software Server (JSS), communicates with the other applications using industry standard SSL encryption that allows for a single point of management.

While this list addresses many of the primary Controls that Sarbanes-Oxley governs concerning Desktop Management, it is by no means exhaustive. In the absence of clear definitions or standards of conduct, the above solutions meet specific objectives that demonstrate a company's willingness to abide by the spirit of the law.

The Increasing Importance of IT 'Controls'
http://itmanagement.earthweb.com/netsys/article.php/3402561
September 1, 2004
By George Spafford

IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition
IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA