macOS Security Compliance

https://github.com/usnistgov/macos_security
Using data to prioritize cybersecurity investments, automated hardening techniques were found, by a wide margin, to have the greatest ability of any control studied to decrease the likelihood of a successful cyberattack. Organizations with such techniques in place, which apply baseline security configurations to system components like servers and operating systems, are nearly six times less likely to have a cyber incident than those that do not.
Solving a Problem

- Yearly major release from Apple
- New hardware
- Out of date guidance
If we work together, we can accomplish anything.
Apple Platform Certifications

December 2022

Table of Contents

macOS Security Compliance

The macOS Security Compliance Project is a programmatic approach to generating a compliance strategy, output customized documentation, and an audit checklist based on a Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 5.

This is a joint project of federal agencies and organizations. The project uses a set of federal and state guidelines and controls to generate a strategy and supporting controls against any security guide supported by NIST or the ICH. The project supports the following guidance:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations, Revision 5
- Organization

Mac Security Compliance

Developing Your Mac Compliance Strategy

Chapter 1

- Developing Your Mac Compliance Strategy
- Identifying Security Gaps
- Generating Baselines and Guidance
- Using the macOS Security Compliance Project
- Preparing to Use the macOS Security Compliance Project
- Implementing a Security Strategy
Automated Secure Configuration
Guidance from the macOS Security Compliance Project (mSCP)

Mark Trappe
Eric Trappe
Munirah Souppaya
Computer Security Division
Information Technology Laboratory

Bob Gendler
Customer Access and Support Division
Office of Information Systems Management

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-219

June 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laura E. Lucas, NIST Director and Undersecretary of Commerce for Standards and Technology
macOS Security Compliance Project (mSCP)

• Ships alongside OS
• Tested Controls
• Fully Documented
• Scripts, Profiles, plists, and more
• Interagency tested, NIST approved
• Massive yearly effort reduction
### SP 800-53 Rev. 5.1 and SP 800-53B Latest Version

**Controls Contain:**
Moderate Security Baseline

**Showing 177 Controls**

<table>
<thead>
<tr>
<th>No.</th>
<th>Control Name</th>
<th>Low-Impact</th>
<th>Moderate-Impact</th>
<th>High-Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>POLICY AND PROCEDURES</td>
<td>AC-1</td>
<td>AC-1</td>
<td>AC-1</td>
</tr>
<tr>
<td>AC-2</td>
<td>ACCOUNT MANAGEMENT</td>
<td>AC-2</td>
<td>AC-2</td>
<td>AC-2</td>
</tr>
<tr>
<td>AC-3</td>
<td>ACCESS ENFORCEMENT</td>
<td>AC-3</td>
<td>AC-3</td>
<td>AC-3</td>
</tr>
<tr>
<td>AC-4</td>
<td>INFORMATION FLOW ENFORCEMENT</td>
<td>AC-4</td>
<td>AC-4</td>
<td>AC-4</td>
</tr>
<tr>
<td>AC-5</td>
<td>SEPARATION OF DUTIES</td>
<td>AC-5</td>
<td>AC-5</td>
<td>AC-5</td>
</tr>
<tr>
<td>AC-6</td>
<td>LEAST PRIVILEGE</td>
<td>AC-6</td>
<td>AC-6</td>
<td>AC-6</td>
</tr>
<tr>
<td>AC-7</td>
<td>UNSUCCESSFUL LOGON ATTEMPTS</td>
<td>AC-7</td>
<td>AC-7</td>
<td>AC-7</td>
</tr>
<tr>
<td>AC-8</td>
<td>SYSTEM USE NOTIFICATION</td>
<td>AC-8</td>
<td>AC-8</td>
<td>AC-8</td>
</tr>
<tr>
<td>AC-9</td>
<td>DEVICE LOCK</td>
<td>AC-11</td>
<td>AC-11</td>
<td>AC-11</td>
</tr>
<tr>
<td>AC-10</td>
<td>SESSION TERMINATION</td>
<td>AC-12</td>
<td>AC-12</td>
<td>AC-12</td>
</tr>
<tr>
<td>AC-11</td>
<td>PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION</td>
<td>AC-14</td>
<td>AC-14</td>
<td>AC-14</td>
</tr>
<tr>
<td>AC-12</td>
<td>REMOTE ACCESS</td>
<td>AC-17</td>
<td>AC-17</td>
<td>AC-17</td>
</tr>
<tr>
<td>AC-13</td>
<td>WIRELESS ACCESS</td>
<td>AC-18</td>
<td>AC-18</td>
<td>AC-18</td>
</tr>
<tr>
<td>AC-14</td>
<td>ACCESS CONTROL FOR MOBILE DEVICES</td>
<td>AC-19</td>
<td>AC-19</td>
<td>AC-19</td>
</tr>
<tr>
<td>AC-15</td>
<td>USE OF EXTERNAL SYSTEMS</td>
<td>AC-20</td>
<td>AC-20</td>
<td>AC-20</td>
</tr>
<tr>
<td>AC-16</td>
<td>INFORMATION SHARING</td>
<td>AC-21</td>
<td>AC-21</td>
<td>AC-21</td>
</tr>
<tr>
<td>AC-17</td>
<td>PUBLICLY ACCESSIBLE CONTENT</td>
<td>AC-22</td>
<td>AC-22</td>
<td>AC-22</td>
</tr>
<tr>
<td>AT-1</td>
<td>POLICY AND PROCEDURES</td>
<td>AT-1</td>
<td>AT-1</td>
<td>AT-1</td>
</tr>
</tbody>
</table>

---

**id:** os_airdrop_disable  
**title:** "Disable AirDrop"  
**discussion:**

AirDrop _MUST_ be disabled to prevent file transfers to or from unauthorized devices.

AirDrop allows users to share and receive files from other nearby Apple devices.

check:

```bash
/usr/bin/profiles -p -o stdout | /usr/bin/grep -c 'allowAirDrop = 0'
```

derived integer: 1

discovery:

- This is implemented by a Configuration Profile.

**references:**

- cce:  
  - CCE-99098-8  
  - CCE-80038-1
- srg:  
  - N/A
- disa_stig:  
  - N/A
- stig:  
  - 1.1.1  
  - 1.1.2  
  - 1.1.16  
  - 3.1.20  
  - 3.4.6
Release Ready

New Release/Guidance

New Hardware
Lifecycle

- WWDC
- Public Beta
- Release
- Maintenance
<table>
<thead>
<tr>
<th>Why does all this matter?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CISA</strong></td>
</tr>
<tr>
<td>• BOD 22-01</td>
</tr>
<tr>
<td>• BOD 23-01</td>
</tr>
<tr>
<td><strong>Executive Order</strong></td>
</tr>
<tr>
<td>• EO 14028</td>
</tr>
<tr>
<td><strong>OMB Memorandum</strong></td>
</tr>
<tr>
<td>• M-21-31</td>
</tr>
</tbody>
</table>
Why does all this matter?
“We’re required to use the DISA STIG for compliance, the mSCP has taken that from a nearly impossible task to one that is very easy to do.”

John Daly - Naval Air Warfare Center
“The mSCP makes a daunting task approachable for Mac Admins of all skill levels, creating easy to comprehend reports for InfoSec and Auditors.”

Jordan Burnette - Virginia Commonwealth University
“We’re a small team of two supporting a few hundred Macs, without mSCP, we likely would have fallen behind on many other projects or had to hire additional team members to support us.”

Niko Torres - New Teacher Center
“The mSCP has saved countless man hours creating and auditing security policies on our Macs. InfoSec thinks I’m a super hero!”

Lee Stanford - Workhuman
mSCP Requirements

The “xcode-select” command requires the command line developer tools. Would you like to install the tools now?
Choose Install to download and install the command line developer tools now.

Cancel  Install
Rules
Baselines
Scripts
Project Outputs
DEMO
Security Compliance Project

One More Thing...