Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date June 24, 2022

Original Release Date February 17, 2022

Superseding Document

Status Final

Series/Number NIST SP 800-219

Title Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP)

Publication Date June 2022

DOI https://doi.org/10.6028/NIST.SP.800-219

CSRC URL https://csrc.nist.gov/publications/detail/sp/800-219/final

Additional Information

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Draft NIST Special Publication 800-219

Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP)

Mark Trapnell
Eric Trapnell
Murugiah Souppaya
Bob Gendler
Karen Scarfone

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

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-219

Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP)

Mark Trapnell
Eric Trapnell
Murugiah 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-draft

February 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-219
Natl. Inst. Stand. Technol. Spec. Publ. 800-219, 30 pages (February 2022)
CODEN: NSPUE2

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

Public comment period: February 17, 2022 – March 23, 2022

Submit comments on this publication to: applesec@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

The macOS Security Compliance Project (mSCP) provides resources that system administrators, security professionals, security policy authors, information security officers, and auditors can leverage to secure and assess macOS desktop and laptop system security in an automated way. This publication introduces the mSCP and gives an overview of the resources available from the project's GitHub site, which is continuously curated and updated to support each new release of macOS. The GitHub site provides practical, actionable recommendations in the form of secure baselines and associated rules. This publication also describes use cases for leveraging the mSCP content.

Keywords

Apple; baseline; configuration management; endpoint device security; macOS; macOS Security Compliance Project (mSCP); operating system security; security compliance.

Supplemental Content

The mSCP's GitHub site is at https://github.com/usnistgov/macos_security#readme, and the project documentation Wiki is at https://github.com/usnistgov/macos_security/wiki.

Acknowledgments

The authors wish to thank Jason Blake and Blair Heiserman from NIST, Allen Golbig from Jamf, Dan Brodjieski, Gary Gapinski, and Elyse Anderson from NASA, and Jamie Richardson and Chris Stone from Apple for their contributions to the mSCP. The authors also wish to thank Stephanie Roberts from NIST for contributions to this publication. The authors appreciate Bob McSulla and Ryan Jaynes from Tenable for developing audit files based on the mSCP, testing the baselines for different macOS versions, and contributing to Appendix C. The authors also thank Isabel Van Wyk from NIST for editing the document. Finally, portions of this document are based on content from the mSCP Wiki, so the work of all Wiki contributors is appreciated.

Trademark Information

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

- assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or
- assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:
    - under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    - without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to applesec@nist.gov, with the subject: “SP 800-219 Call for Patent Claims.”

Executive Summary

The National Institute of Standards and Technology (NIST) has traditionally published secure configuration guides for Apple desktop/laptop operating system versions as prose-based Special Publications (SPs), such as NIST SP 800-179 Revision 1, *Guide to Securing Apple macOS 10.12 Systems for IT Professionals: A NIST Security Configuration Checklist*. In order to provide security configuration guidance to organizations more quickly and in a machine-consumable format, NIST has established the open-source macOS Security Compliance Project (mSCP). Instead of NIST producing a prose SP guidance document for each macOS release, the mSCP will continuously curate and update machine-consumable macOS guidance.

The mSCP seeks to simplify the macOS security development cycle by reducing the amount of effort required to implement security baselines. *Security baselines* are groups of settings used to configure a system to meet a target level or set of requirements, or to verify that a system complies with requirements. The mSCP, a collaboration among federal agencies, minimizes duplicate effort that would otherwise be needed for these agencies to administer individual security baselines. Additionally, the secure baseline content provided is easily extensible by other parties to implement their own security requirements.

This document provides a high-level overview of the mSCP, its components, and some common use cases. Readers seeking more detailed information on mSCP content or the content itself should visit the mSCP GitHub page (https://github.com/usnistgov/macos_security) and wiki (https://github.com/usnistgov/macos_security/wiki).

Organizations using mSCP content, particularly security baseline examples, should take a risk-based approach for selecting the appropriate settings and defining setting values that takes into account the context under which the baseline will be utilized.

Table of Contents

1 Introduction

The National Institute of Standards and Technology (NIST) has traditionally published secure configuration guides for Apple desktop/laptop operating system versions as prose-based Special Publications (SPs), such as NIST SP 800-179 Revision 1, *Guide to Securing Apple macOS 10.12 Systems for IT Professionals: A NIST Security Configuration Checklist*. NIST will no longer produce SP guidance documents for each macOS release, but instead will continuously curate and update machine-consumable guidance as part of NIST's macOS Security Compliance Project (mSCP) to keep up with each macOS release version.

The latest macOS security baseline content is maintained and updated on the mSCP GitHub page, https://github.com/usnistgov/macos_security [1]. *Security baselines* are groups of settings used to configure a system to meet a target level or set of requirements, or to verify that a system complies with requirements. The mSCP seeks to simplify the macOS security development cycle by reducing the amount of effort required to implement security baselines. This collaboration between federal agencies minimizes duplicate effort that would otherwise be needed for these agencies to administer individual security baselines. Additionally, the secure baseline content provided is easily extensible by other parties to implement their own security requirements.

1.1 Purpose and Scope

The purpose of this document is to introduce the mSCP to broader audiences. This document provides a high-level overview of the mSCP, its components, and some common use cases. It refers readers to the online project documentation for in-depth technical information and use instructions. This document is intended to be independent of macOS version releases; updates will be released as needed when there are substantial changes to the mSCP.

The information in this document regarding the details of the mSCP GitHub site is accurate at the time of publication. Check the project wiki (https://github.com/usnistgov/macos_security/wiki) for the latest information.

The release of SP 800-219 formally deprecates NIST SP 800-179 [2] and SP 800-179 Revision 1 [3]; their applicable recommendations have already been added to corresponding mSCP baselines. Organizations needing to reference a NIST SP to demonstrate how they are complying with United States Government mandates for adopting secure configurations for their macOS devices may reference this SP instead of SP 800-179 or SP 800-179 Revision 1.

1.2 Audience

This document—and the mSCP GitHub site—are intended for system administrators, security professionals, policy authors, privacy officers, and auditors who have responsibilities involving macOS security. Additionally, vendors of device management, security, configuration assessment, and compliance tools supporting macOS may find this document and the GitHub site to be helpful.

1.3 Document Structure

The remaining sections and appendices of this document are as follows:

- Section 2 provides an overview of the project, including what its goals are and how its content can be used.
- Section 3 explains the major components of the mSCP and provides pointers to additional information on component usage.
- The References section lists the references for the document.
- Appendix A briefly discusses how mSCP can help meet the needs of people in several roles.
- Appendix B provides examples of how a security professional might use mSCP content.
- Appendix C contains an example of how an assessment tool vendor could leverage mSCP content.
- Appendix D lists the acronyms and abbreviations used in this document.

2 Project Description

The mSCP is an open-source project providing a programmatic approach to generating and using macOS security configuration baselines. The project's content can be used to create customized security baselines of technical security controls by leveraging a library of rules, with each rule mapped to requirements in one or more existing security standards, regulations, frameworks, etc. This approach provides versioning and consistency of the content. Unifying and standardizing macOS baseline efforts via the mSCP means that updating security guidance is simplified and radically accelerated, even as new versions of macOS are introduced annually.

The mSCP started in August 2019 as a collaboration among operational IT security staff from NIST, the National Aeronautics and Space Administration (NASA), the Defense Information Systems Agency (DISA), and the Department of Energy's (DOE) Los Alamos National Laboratory (LANL).[1] The mSCP sought to map macOS settings to the NIST SP 800-53 Revision 4 [4] document with an extensible, modern approach to security guidance that could be used by any organization (e.g., government, enterprise, education) that needs to adhere to security compliance frameworks and policy.

As of this writing, the configuration settings represent guidance and best practices from NIST SP 800-53 Revision 5 [5], NIST SP 800-171 Revision 2 [6], the macOS DISA Security Technical Implementation Guide (STIG) [7], the Committee on National Security Systems (CNSS) Instruction (CNSSI) Number 1253 [8], and the Center for Internet Security (CIS) Critical Security Controls Version 8 [9], as well as internal organizational security guidance from NIST, NASA, and LANL.

2.1 Project Goals

Apple releases a new macOS version every year, and generally, agencies and organizations must wait for guidance or accept risk before deploying the new macOS version. Most agencies or organizations must create their own internal security configuration, which delays deploying the new macOS version or new hardware that only supports the new macOS version. The mSCP assists organizations in upgrading sooner. The technical security settings in macOS generally do not drastically change from release to release, with only a handful of new settings being introduced. By pursuing a rules-based approach, mSCP rules that remain applicable can be reused and incorporated into guidance for the latest macOS version. This enables quicker adoption of new security features that are not offered in prior versions of macOS.

The goals of the mSCP are:

- Develop recommended security baselines using a risk-based approach based on the impact of the data
- Normalize and accelerate annual adoption of the new operating system and hardware that is specific to it by providing guidance to meet the security needs of new operating systems at the earliest availability

[1] See https://github.com/usnistgov/macos_security#authors for a current list of project contributors.

- Reduce worldwide effort in creating annual guidance by unifying and consolidating compliance efforts into a single project
- Develop a methodology to foster collaboration between baseline authors, reducing overhead and redundancy
- Establish a unified approach for configuration and assessment of controls across multiple sources and tools
- Enable the customization of existing content and the creation of new content, including creating custom baselines in order to meet organization-specific security requirements
- Provide device management and security tool vendors, auditors, and Apple insight into customer security configuration needs

2.2 mSCP Content Use

mSCP content can be used by any organization to assist in setting and assessing the security configuration of macOS systems. Security baselines can be made to map to existing guidance or controls, such as those in NIST SP 800-53 Revision 5 [5], or they can be customized to meet an organization's specific needs. In mSCP terminology, a security baseline is represented as a *baseline file* designating rules required to meet a specific set of requirements. The mSCP provides a library of *rules* that are macOS settings. Each rule is mapped to a requirement within a security standard, framework, etc. Baseline files and rules comprise much of the mSCP's content.

The mSCP offers several example baselines, including the following, with descriptions adapted from FIPS 199 [10]:

- The ***SP 800-53 Revision 5 low baseline*** is a defined map of controls to secure a system defined as a low-impact information system. The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.
- The ***SP 800-53 Revision 5 moderate baseline*** is a defined map of controls to secure a system defined as a moderate-impact information system. The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
- The ***SP 800-53 Revision 5 high baseline*** is a defined map of controls to secure a system defined as a high-impact information system. The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Organizations using any baseline example should take a risk-based approach for selecting the appropriate settings and organizationally defined values depending on the context under which the baseline will be applied. Organizations can tailor any of the baselines to include controls specific to their needs and to produce evidence of control enforcement.

The mSCP provides scripts that can be used with baselines for several purposes, including the following:

- Creating scripts and profiles for configuring macOS
- Generating a mapping between two security standards, regulations, frameworks, etc.
- Producing human-readable documentation in a variety of formats
- Customizing existing baselines

mSCP content can also be used to generate Security Content Automation Protocol (SCAP) content for automated security compliance scans. The SCAP generated follows the SCAP 1.3 specification [11]. Generation of SCAP content uses an Extensible Stylesheet Language Transformations (XSLT) file to create an Extensible Configuration Checklist Description Format (XCCDF) checklist document with an accompanying Open Vulnerability and Assessment Language (OVAL) document.

The XCCDF and OVAL documents are bundled into an SCAP data stream collection document with accompanying files that include Common Platform Enumeration (CPE) dictionary [12] information and an Open Checklist Interactive Language (OCIL) document. This creates an SCAP 1.3 document that validates using the NIST SCAP Content Validation Tool[2] and can be used by SCAP tools on macOS. More information on SCAP content generation is available at https://github.com/usnistgov/macos_security/wiki/SCAP-Content-Generation.

[2] https://csrc.nist.gov/projects/security-content-automation-protocol/scap-releases/scap-1-3

3 mSCP Components

This section provides an overview of several components of the mSCP: security baseline files, configuration profiles and scripts, content generation scripts, customization capabilities, and directories. More information about all of these is available from the GitHub wiki at https://github.com/usnistgov/macos_security/wiki.

3.1 Security Baseline Files

In the mSCP, a security baseline is defined in a Yet Another Markup Language (YAML) file. A YAML file is a human-readable file format commonly used by configuration files where data is stored and/or transmitted. A baseline YAML file consists of the following required fields. The code immediately below this list provides a partial example of a YAML file that illustrates the use of these fields (with field names bolded).

- **title** – a human-readable name for the baseline
- **description** – a short description of the baseline, including its use case and target operating system (OS) version
- **authors** – developers of the baseline
- **profile** – the security content portion of the baseline
    - **section** – a keyword for organizing settings
    - **rules** – the names of the rule files that are a part of this baseline

```
title: "Apple macOS 11 (Big Sur) Test Baseline"
description: |
  This guide describes the prudent actions to take when securing a macOS 11
system against the Test Baseline.
authors: |
  |===
  |Joe Doe|NIST
  |===
profile:
  - section: "Authentication"
    rules:
      - auth_pam_login_smartcard_enforce
      - auth_pam_su_smartcard_enforce
      - auth_pam_sudo_smartcard_enforce
      - auth_smartcard_allow
  - section: "Auditing"
    rules:
      - audit_acls_files_configure
      - audit_acls_files_mode_configure
      - audit_acls_folder_wheel_configure
```

3.1.1 Rule File Composition

A YAML rule file is broken down into the following subsections. The code immediately below this list provides a notional example of a YAML rule file (with field names bolded). This example is from the Rules section of the mSCP wiki (https://github.com/usnistgov/macos_security/wiki/Rules).

- `id` – the name of the rule file, excluding the `.yaml` file extension
- `title` – a human-readable rule title
- `discussion` – a short description of the rule and its use case
- `check` – the check to assess the system for the specified rule; typically this is shell code
- `result` – the expected result of running the check
- `fix` – the necessary fix in case the check fails; if `[source,bash]` is included, the fix will be included in the configuration script
- `references` – references, including identifiers and mappings such as security frameworks, guidance, and controls; the references always include a Common Configuration Enumeration (CCE) identifier, which is assigned to this rule file and can be found in the official repository of NIST CCEs [13]
- `macOS` – the validated macOS version for this rule
- `tags` – modifiable keywords for categorizing and identifying related rules
- `severity` – the severity level specified in the DISA STIG, if applicable
- `mobileconfig` – if `true`, this rule will be used to generate configuration profile content
- `mobileconfig_info` – if `mobileconfig` is set to `true`, this field specifies the information required to produce configuration profile content

```
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: |
  /usr/bin/profiles -P -o stdout | /usr/bin/grep -c 'allowAirDrop = 0'
result:
  integer: 1
fix: |
  This is implemented by a Configuration Profile.
references:
  cce:
    - CCE-85293-9
  cci:
    - CCI-000381
  800-53r5:
    - AC-3
    - AC-20
    - CM-7
    - CM-7(1)
  800-53r4:
    - CM-7
    - CM-7(1)
    - AC-3
    - AC-20
  srg:
    - SRG-OS-000095-GPOS-00049
  disa_stig:
    - APPL-11-002009
  800-171r2:
    - 3.1.1
    - 3.1.2
    - 3.1.16
    - 3.1.20
    - 3.4.6
macOS:
  - "11.0"
tags:
  - 800-53r5_low
  - 800-53r5_moderate
  - 800-53r5_high
  - 800-53r4_low
  - 800-53r4_moderate
  - 800-53r4_high
  - 800-171
  - cnssi-1253
  - stig
severity: "medium"
mobileconfig: true
mobileconfig_info:
  com.apple.applicationaccess:
    allowAirDrop: false
```

3.1.2 Rule File Categories

The mSCP organizes YAML files in the `rules` directory into the following subdirectories, each corresponding to a category of settings:

- **audit** – OpenBSM
- **auth** – smartcard authentication
- **icloud** – Apple's iCloud/Apple ID service
- **os** – settings that do not fit into the other categories
- **pwpolicy** – password policy
- **sysprefs** – settings controlled within the System Preferences application

The `rules` directory also includes a **supplemental** subdirectory, which contains additional information that supports the guidance provided by the baselines. Supplemental content contains information for rules that are not part of an existing baseline but could be beneficial for certain use cases. Supplemental content may not have mappings and may or may not contain the YAML rule file check and fix sections mentioned in Section 3.1.1. Supplemental content can be added to enhance baselines where organizational requirements are different than the system baseline requirements.

3.2 Configuration Profiles and Scripts

When an mSCP YAML file is processed, it yields a configuration script and/or configuration profile (`mobileconfig` file) as outputs. Both are used to apply configuration settings to a system.

A *configuration profile* is an Extensible Markup Language (XML) formatted file with a `mobileconfig` extension containing a configuration payload. macOS can automatically configure itself based on a `mobileconfig` file's contents upon execution. Configuration profiles offer a convenient, Apple-supported mechanism for applying security settings to a macOS environment. Additionally, they can be cryptographically signed to ensure integrity and authenticity. These factors make configuration profiles the preferred vehicle for configuration delivery. However, mobileconfig files cannot modify all macOS settings, so a configuration script is needed for those that are not supported.

A *configuration script* is a shell script that manipulates operating system files directly. The script content is derived from all YAML rule files that have a `mobileconfig` value of `false` and belong to the specified baseline. The YAML rule file must contain the `fix` section in order to generate its corresponding configuration script entry.

3.3 Content Generation Scripts

The mSCP provides several types of scripts for generating baselines, human-readable guidance, baseline compliance checkers, and other types of content. Each script is described below.

3.3.1 Generate Baseline Script

The `generate_baseline.py` script compiles a list of security rules into a single baseline YAML file. It can be used to modify an existing security baseline or create a new one. See https://github.com/usnistgov/macos_security/wiki/Scripts#generate_baselinepy for additional information.

3.3.2 Generate Guidance Script

The `generate_guidance.py` script can produce human-readable guidance as well as generate the macOS Security Compliance Tool in the form of a Z shell script.

The `generate_guidance.py` script takes a baseline file and produces a human-readable guide in the format of documentation from information available in the YAML rules files. The documentation can be in any of several formats. The script always generates an Asciidoc file. AsciiDoc (`.adoc`) is a plain text format that uses markup conventions for traditional document formatting and organization. AsciiDoc files are easily transformable into many other formats via the `generate_guidance.py` script, including Hypertext Markup Language (HTML), PDF, and Excel. The Excel format is particularly useful for quickly viewing all the rules of a baseline, and it contains all the data in the YAML rules files.

The `generate_guidance.py` script can also create configuration profiles (`mobileconfig` files) and a compliance script. Using the `-s` argument, the `generate_guidance.py` script will generate an `org.{baseline}.audit.plist` file and another script, the macOS Security Compliance Tool that can check and remediate compliance settings. The `audit.plist` file can be used to set an exemption to organizational rules for approved users so that compliance checks can succeed without findings. To create an exemption for a rule, the `exempt` field should be set to `true` and an `exempt_reason` should be added.

See https://github.com/usnistgov/macos_security/wiki/Scripts#generate_guidancepy-script for more information on the `generate_guidance.py` script.

3.3.3 macOS Security Compliance Tool

The `{baseline}_compliance.sh` script runs interactively by default. It can evaluate a system's conformance to a baseline or remediate any incorrectly configured settings. Alternatively, the script can autonomously assess a system with the `-check` argument or automatically remediate any possible settings with `-fix`.

The lines below provide an example of the results of running the script.

```
Thu Jan 21 15:09:41 UTC 2021 auth_pam_login_smartcard_enforce passed (Result:
2, Expected: {integer: 2})
Thu Jan 21 15:09:41 UTC 2021 auth_smartcard_allow passed (Result: 1,
Expected: {integer: 1})
Thu Jan 21 15:09:41 UTC 2021 auth_pam_sudo_smartcard_enforce passed (Result:
2, Expected: {integer: 2})
Thu Jan 21 15:09:41 UTC 2021
auth_smartcard_certificate_trust_enforce_moderate passed (Result: 2,
Expected: {integer: 2})
Thu Jan 21 15:09:41 UTC 2021 auth_smartcard_enforce has an exemption (Reason:
Broken Reader)
```

For more information on the macOS Security Compliance Tool script, see https://github.com/usnistgov/macos_security/wiki/Compliance-Script.

3.3.4 OVAL Generation Script

The OVAL generation script, `yaml-to-oval.py`, takes a baseline YAML file and generates OVAL checks for any rule file where possible. Note that this script does not recognize any custom settings. For more information, see https://github.com/usnistgov/macos_security/wiki/Scripts#yaml-to-ovalpy.

3.3.5 Generate Mapping Script

The `generate_mapping.py` script allows for the quick creation of custom rules and baselines for a compliance framework not published by the mSCP. The script requires a user-created comma-separated values (CSV) file containing control identifiers that maps to a new framework (CSV column 1) from another already defined by the project (CSV column 2). By default, the script is designed to map a framework to the NIST SP 800-53r5 [5] set of controls. Adding the `-f` argument allows for mapping to another supported framework. See https://github.com/usnistgov/macos_security/wiki/Generate-Mapping for more information on the `generate_mapping.py` script.

3.4 Customization

Customization allows organizations to generate their own customized content outside of that provided by the project. Additionally, it allows them to add content for internal-only controls, which are not suitable for inclusion in a global baseline. Customization primarily takes place within the `custom` folder. Here are examples of customization supported by mSCP:

- **Baselines**: A `baseline` folder can be included within the `custom` folder to create customized baselines that fit an organization's needs. These baseline files may include rule, section, and template customization (discussed below).
- **Rules**: Existing rules can have their setting values overridden via the `custom` folder instead of modifying the mSCP-supplied rule file. New rules can be created and added to existing baselines or to user-defined baselines. Organizations can create their own discussions, checks, results, fixes, and mappings of rules to security frameworks not included in the project. In order to override an existing rule, the custom rule file name must match an existing rule so the `generate_guidance.py` script will pick up the new values. New rules not included in mSCP must be listed in the baseline YAML file specified when running `generate_guidance.py`. Additional information on custom rules can be found in an article written by mSCP contributor Allen Golbig [14].
- **Sections**: Custom sections can be used to organize existing or custom YAML rule files. Sections defined in the `custom` folder must be included in a baseline YAML file in order to be used by `generate_guidance.py`.
- **Templates**: Custom templates can be used to define new template structures for the project and affect the organization and appearance of generated documentation. The template files must match the name of an existing template and will override that template when running `generate_guidance.py`.
- **Logos**: An organization can include a custom logo when running the `generate_guidance.py` script by using the `-l` argument to point to an image file.

3.5 Directories

mSCP releases available at https://github.com/usnistgov/macos_security/releases include the following directories:

- `baselines` – contains the defined YAML baseline files
- `build` – holds scripts, documents, and configuration profiles generated by running scripts
- `custom` – used for creating customized baselines, rules, sections, or templates to meet an organization's requirements
- `includes` – contains YAML-based libraries required for running the scripts
- `rules` – contains YAML rule files, with one rule per file
- `SCAP` – contains the required files for generating SCAP content
- `scripts` – contains the content generation scripts, along with their required files
- `sections` – defines the sections that correlate to the directories in the `rules` folder; each section has its own YAML file containing the section name and description as it will appear in the generated guide, which is human-readable documentation
- `templates` – includes AsciiDoc templates for generating an AsciiDoc guide

602 # References

[1] macOS Security Compliance Project (2022) *macOS Security Compliance Project*. Available at https://github.com/usnistgov/macos_security

[2] Trapnell M, Scarfone KA, Trapnell E, Badger ML, Souppaya MP, Yaga DJ (2016) Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-179. https://doi.org/10.6028/NIST.SP.800-179

[3] Trapnell M, Scarfone KA, Trapnell E, Badger ML, Souppaya MP, Yaga DJ (2018) Guide to Securing Apple macOS 10.12 Systems for IT Professionals: A NIST Security Configuration Checklist. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-179, Rev. 1. Available at https://csrc.nist.gov/publications/detail/sp/800-179/rev-1/draft

[4] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[6] Ross R, Pillitteri V, Dempsey K, Riddle M, Guissanie G (2020) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-171, Rev. 2, Includes updates as of January 28, 2021. https://doi.org/10.6028/NIST.SP.800-171r2

[7] Department of Defense (2021) *DISA STIG for macOS*. Available at https://public.cyber.mil/stigs/

[8] Committee on National Security Systems (2014) Security Categorization and Control Selection for National Security Systems. (National Security Agency, Ft. Meade, MD), Committee on National Security Systems Instruction (CNSSI) No. 1253. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[9] Center for Internet Security (2021) *CIS Critical Security Controls Version 8*. Available at https://www.cisecurity.org/controls/v8/

[10] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199

[11] Waltermire DA, Quinn SD, Booth H, III, Scarfone KA, Prisaca D (2018) The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.3. (National Institute of Standards and Technology, Gaithersburg, MD),

NIST Special Publication (SP) 800-126, Rev. 3. https://doi.org/10.6028/NIST.SP.800-126r3

[12] National Institute of Standards and Technology (2021). *Official Common Platform Enumeration (CPE) dictionary*. Available at https://nvd.nist.gov/products/cpe

[13] National Institute of Standards and Technology (2021) *CCE Platform Listing*. Available at https://ncp.nist.gov/cce

[14] Golbig A (2021) *Getting to Know: macOS Security Compliance Project – Part 2*. Available at https://golbiga.medium.com/getting-to-know-macos-security-compliance-project-part-2-24131b60cdfb

Appendix A—mSCP User Roles

The mSCP was designed to meet the needs of different security roles. These perspectives are briefly examined below.

Security policy authors define the policies for their organizations. The customization and ease of extensibility offered by the mSCP facilitate new content creation. Policy authors will need to familiarize themselves with the YAML rule file format described in Section 3.1.1. Of particular interest is the ability to map rules directly to references. Additionally, the generate mapping script (Section 3.3.5) enhances portability between compliance frameworks.

System administrators and security professionals are responsible for configuring the systems under their purview. They implement the guidance issued by security policy authors. As such, configuration tools such as the macOS Security Compliance Tool's (Section 3.3.3) automatic remediation mode are of interest. Additionally, security professionals may wish to generate baselines (Section 3.3.1), guidance (Section 3.3.2), and the macOS Security Compliance Tool (Section 3.3.3).

Auditors approach macOS security compliance from a validator perspective, seeking proof that a system is configured in the required way. They are more interested in system setting documentation and compliance evidence than technical tools such as configuration scripts. Both of these needs can be met by mSCP tools. The generate guidance script (Section 3.3.2) provides the necessary documentation in a variety of formats including HTML, PDF, and Excel. The macOS Security Compliance Tool (Section 3.3.3) assesses a system and produces a log of the results. Additionally, some auditors may be interested in examining YAML rule content directly (Section 3.1.1).

Information security officers have a variety of goals but are ultimately responsible for ensuring that systems are configured according to their organizational requirements. To accomplish this, they need policy documentation (Section 3.3.2) and the results of compliance scans (Section 3.3.3). Information security officers may also be responsible for reviewing the security rules proposed by the policy authors. If this is the case, they may be interested in YAML rule file components (Section 3.1.1).

Vendors of device management, security, configuration assessment, and compliance tools can produce a series of audit files based on mSCP content to support different macOS versions and associated security baselines. These audit files are maintained, tested, published, and supported by the tool vendors. Tool customers can download and import the content into the tool to assess the state of their system against a particular baseline in an automated way.

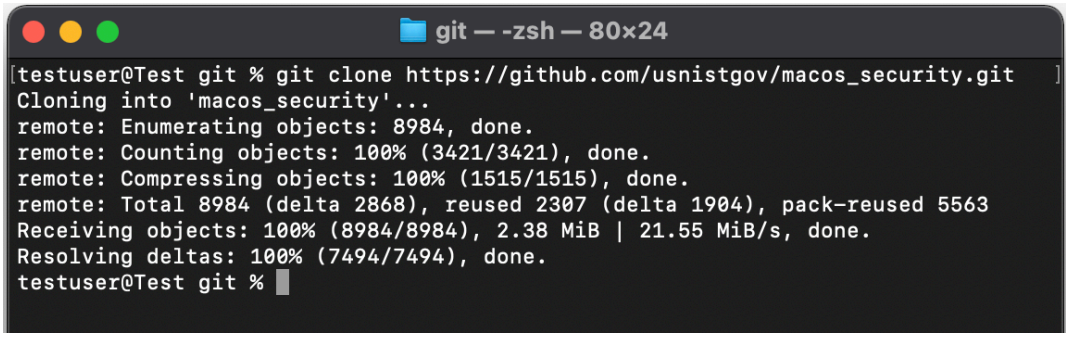
Specific audit files of the mSCP by tool vendors are described on the project wiki page. This content will be updated as contributing tool vendors develop new audit content.

Appendix B—Example of mSCP Usage by a Security Professional

This appendix provides examples of how a security professional might use mSCP content. People in other roles might perform some of the same actions. The examples illustrated below were accurate at the time of publication, but please see the mSCP wiki at https://github.com/usnistgov/macos_security/wiki for up-to-date usage guidance. Note that the mSCP scripts are not meant to replace enterprise-class configuration and management tools. Configurations should be tested on development systems before being deployed on end users' systems.

Preparing to use mSCP

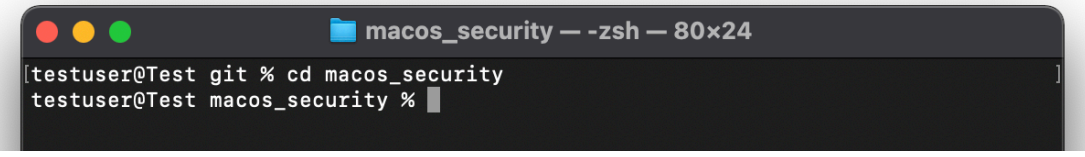
All project components are available from the mSCP GitHub page [1] by navigating to `Releases` and downloading the latest source code revision for the desired macOS version. Alternatively, the project source code can be downloaded via git, as the example below illustrates.



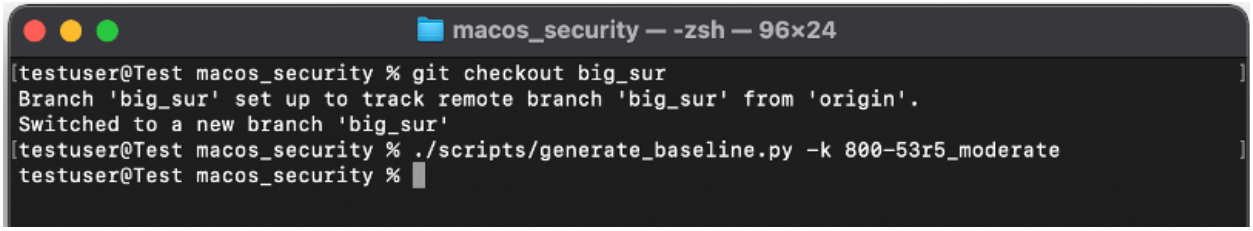
mSCP components rely on prerequisite software listed at https://github.com/usnistgov/macos_security/wiki/Getting-Started, so any missing software will need to be installed.

Changing code branches and generating a baseline

After obtaining a copy of the source code, change directory to the mSCP git folder, `macos_security`.



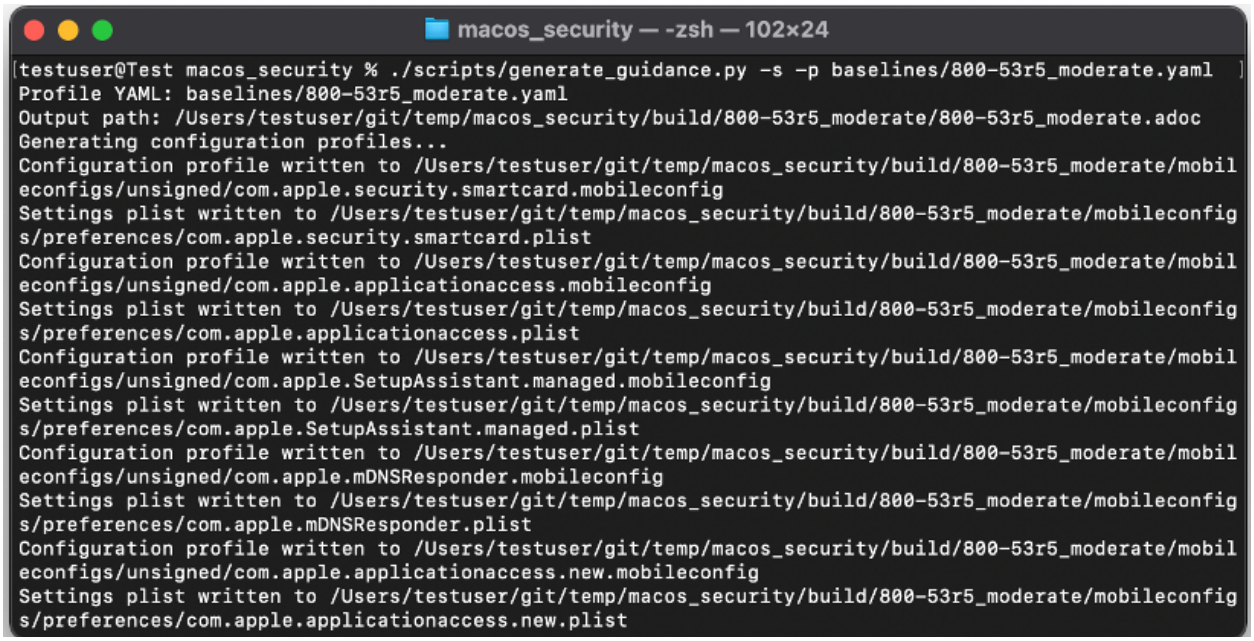
Next, select the appropriate code branch that corresponds to the target OS version. Then choose a baseline and use the `generate_baseline.py` script to create a baseline YAML file. The example below illustrates these steps for the NIST SP 800-53 Revision 5 moderate baseline for macOS Big Sur.



663

664 **Creating the macOS Security Compliance Tool and configuration profiles**

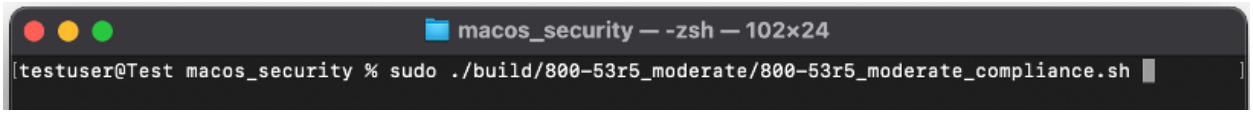
665 Using the `generate_guidance.py` script, create the macOS Security Compliance Tool and
666 configuration profiles. The example below illustrates this, continuing from the previous example.



667

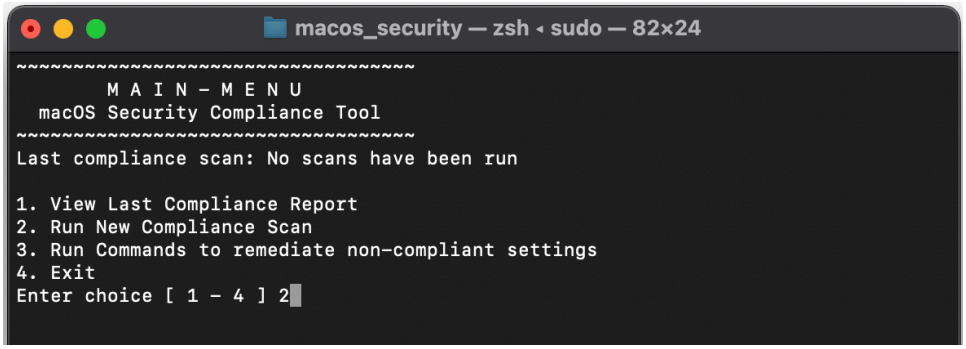
668 **Running a compliance scan**

669 As the example below shows, the macOS Security Compliance Tool is typically run with
670 administrator privileges so that it can access all the settings.



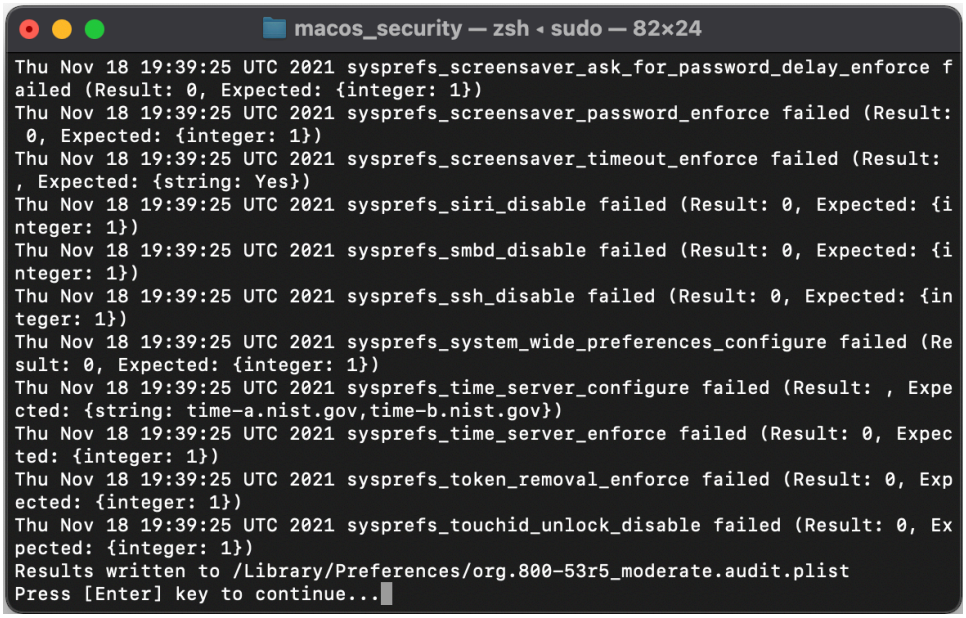
671

672 The example below shows the main menu presented by the macOS Security Compliance Tool.



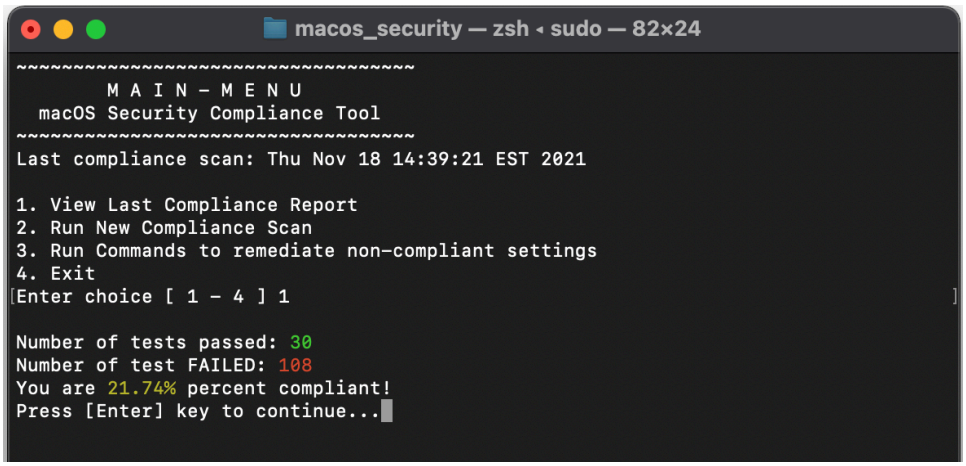
673

674 Selecting option 2, "Run New Compliance Scan," from the main menu launches the scan. The
675 example below shows output from the scan, which in this case reflects numerous rule failures,
676 each indicating a deviation from the expected configuration.



677

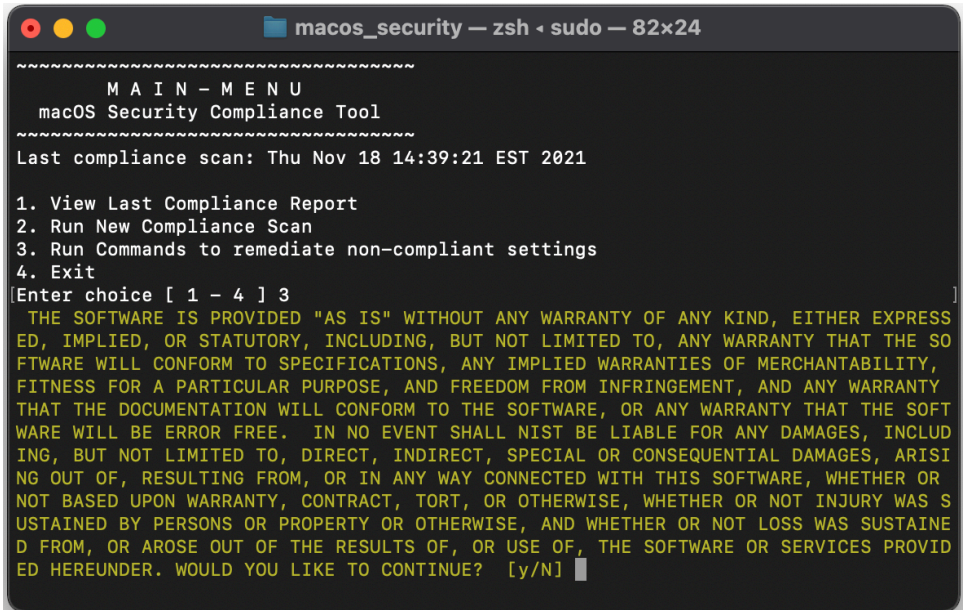
678 Selecting option 1, "View Last Compliance Report," from the main menu displays a summary of
679 the compliance report results. The example below depicts results indicating that 30 tests passed
680 and 108 tests failed, for an overall score of 21.74% compliant.



681

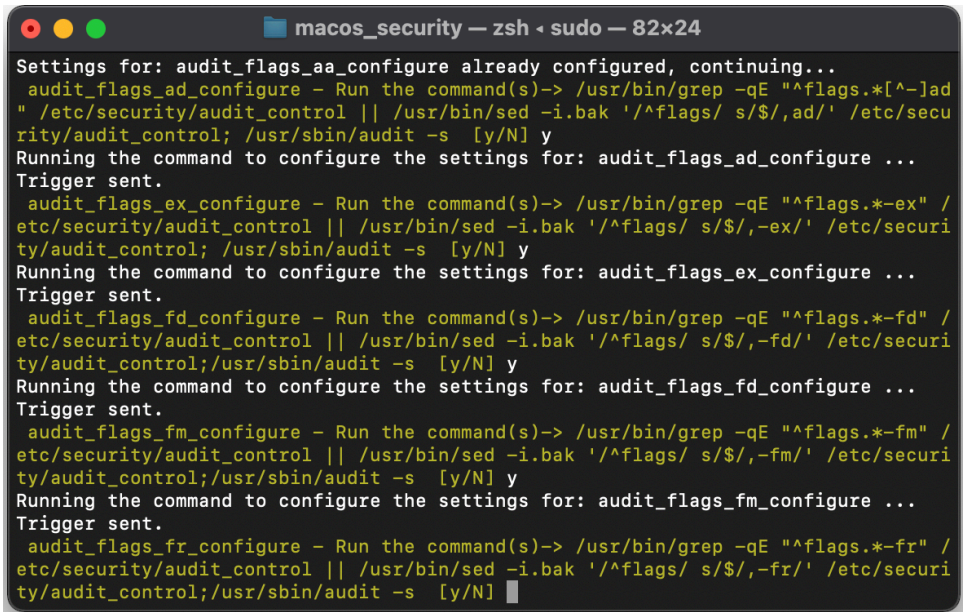
682 **Fixing non-compliant settings**

683 Selecting option 3, "Run Commands to remediate non-compliant settings," begins the process of
684 fixing non-compliant settings discovered during a previous compliance scan. The example below
685 illustrates the disclaimer to be reviewed and accepted before fixes are initiated. This disclaimer
686 indicates the potential risk in applying fixes.



687

688 After the disclaimer statement is accepted, the fixes are applied to the system, as the example
689 below illustrates.


macos_security — zsh ◂ sudo — 82×24
Settings for: audit_flags_aa_configure already configured, continuing...
audit_flags_ad_configure - Run the command(s)-> /usr/bin/grep -qE "^flags.*[^-]ad " /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,ad/' /etc/security/audit_control; /usr/sbin/audit -s [y/N] y
Running the command to configure the settings for: audit_flags_ad_configure ...
Trigger sent.
audit_flags_ex_configure - Run the command(s)-> /usr/bin/grep -qE "^flags.*-ex" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,-ex/' /etc/security/audit_control; /usr/sbin/audit -s [y/N] y
Running the command to configure the settings for: audit_flags_ex_configure ...
Trigger sent.
audit_flags_fd_configure - Run the command(s)-> /usr/bin/grep -qE "^flags.*-fd" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,-fd/' /etc/security/audit_control;/usr/sbin/audit -s [y/N] y
Running the command to configure the settings for: audit_flags_fd_configure ...
Trigger sent.
audit_flags_fm_configure - Run the command(s)-> /usr/bin/grep -qE "^flags.*-fm" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,-fm/' /etc/security/audit_control;/usr/sbin/audit -s [y/N] y
Running the command to configure the settings for: audit_flags_fm_configure ...
Trigger sent.
audit_flags_fr_configure - Run the command(s)-> /usr/bin/grep -qE "^flags.*-fr" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/ s/$/,-fr/' /etc/security/audit_control;/usr/sbin/audit -s [y/N]

690

Appendix C—Example of mSCP Usage by an Assessment Tool Vendor

This appendix provides an example of how an assessment tool vendor converted mSCP content to their tool's proprietary format so their tool could perform compliance checks against mSCP baselines and rules. Refer to the mSCP GitHub wiki page for the most current list of tool vendors and associated content that will support the mSCP baselines.

This example is for Tenable, Inc. They automated the conversion of mSCP YAML rules into their `.audit` format using Python and YAML libraries. Programmatically approaching this conversion allows for faster future releases and greater consistency, and it also maintains the integrity of the source content. Because the YAML content is all command-driven, it is converted to Tenable's `CMD_EXEC` check type for use with the Unix plugin. The YAML rules have a "tags" section that was used to create unique audit profiles related to common frameworks. An example of these profiles can be seen in the audit file naming convention:

- `NIST_macOS_Big_Sur_800-171_v1.4.0.audit`
- `NIST_macOS_Catalina_800-53r5_high_v1.5.0.audit`

See Tenable's research highlight at https://community.tenable.com/s/feed/0D53a00008E0hgYCAR for more details.

The following example shows a YAML-to-audit-check conversion. The content has been condensed and abbreviated for the purposes of comparison:

mSCP YAML

```
title: "Limit SSHD to FIPS 140 Validated Ciphers"

discussion: |
  If SSHD is enabled then it _MUST_ be configured to limit the ciphers to
algorithms that are FIPS 140 validated.
FIPS 140-2 is the current standard for validating that mechanisms used to
access cryptographic modules utilize authentication that meet federal
requirements.
Operating systems utilizing encryption _MUST_ use FIPS validated mechanisms
for authenticating to cryptographic modules.
  NOTE: /etc/ssh/sshd_config will be automatically modified to its original
state following any update or major upgrade to the operating system.

check: |
  /usr/bin/grep -c "^Ciphers aes256-ctr,aes192-ctr,aes128-ctr"
/etc/ssh/sshd_config

result:
  integer: 1
```

Tenable Audit Check

```
<custom_item>
  system      : "Darwin"
  type        : CMD_EXEC
  description : "Big Sur - Limit SSHD to FIPS 140 Validated Ciphers"
  info        : "If SSHD is enabled then it _MUST_ be configured to limit the
ciphers to algorithms that are FIPS 140 validated.
FIPS 140-2 is the current standard for validating that mechanisms used to
access cryptographic modules utilize authentication that meet federal
requirements.
```

```
739
740   Operating systems utilizing encryption _MUST_ use FIPS validated mechanisms
741   for authenticating to cryptographic modules.
742   NOTE: /etc/ssh/sshd_config will be automatically modified to its original
743   state following any update or major upgrade to the operating system."
744     cmd         : "/usr/bin/grep -c \"^Ciphers aes256-ctr,aes192-ctr,aes128-
745   ctr\" /etc/ssh/sshd_config"
746     expect      : "1"
747   </custom_item>
```

Appendix D—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CCE	Common Configuration Enumeration
CIS	Center for Internet Security
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CSV	Comma-Separated Values
DISA	Defense Information Systems Agency
DOE	Department of Energy
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GUI	Graphical User Interface
HTML	Hypertext Markup Language
IT	Information Technology
ITL	Information Technology Laboratory
LANL	Los Alamos National Laboratory
mSCP	macOS Security Compliance Project
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OCIL	Open Checklist Interactive Language
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
SCAP	Security Content Automation Protocol
SP	Special Publication
STIG	Security Technical Implementation Guide
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations
YAML	Yet Another Markup Language