

# CIS Apple macOS 14 (Sonoma) Security Technical Implementation Guide STIG Benchmark

v1.0.0 - 09-10-2025

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

For information on referencing and/or citing CIS Benchmarks in 3<sup>rd</sup> party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal ([legalnotices@cisecurity.org](mailto:legalnotices@cisecurity.org)) and request guidance on copyright usage.

**NOTE:** It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3<sup>rd</sup> party (non-CIS owned) site.

# Table of Contents

|                                                             |                                     |
|-------------------------------------------------------------|-------------------------------------|
| <b>Terms of Use .....</b>                                   | <b>1</b>                            |
| <b>Table of Contents.....</b>                               | <b>2</b>                            |
| <b>Overview .....</b>                                       | <b>7</b>                            |
| <b>Important Usage Information .....</b>                    | <b>Error! Bookmark not defined.</b> |
| Key Stakeholders .....                                      | Error! Bookmark not defined.        |
| Apply the Correct Version of a Benchmark .....              | Error! Bookmark not defined.        |
| Exceptions .....                                            | Error! Bookmark not defined.        |
| Remediation.....                                            | Error! Bookmark not defined.        |
| Summary .....                                               | Error! Bookmark not defined.        |
| <b>Target Technology Details.....</b>                       | <b>7</b>                            |
| <b>Intended Audience .....</b>                              | <b>7</b>                            |
| <b>Consensus Guidance .....</b>                             | <b>Error! Bookmark not defined.</b> |
| <b>Typographical Conventions .....</b>                      | <b>Error! Bookmark not defined.</b> |
| <b>Recommendation Definitions .....</b>                     | <b>8</b>                            |
| <b>Title .....</b>                                          | <b>8</b>                            |
| <b>Assessment Status .....</b>                              | <b>8</b>                            |
| Automated.....                                              | 8                                   |
| Manual .....                                                | 8                                   |
| <b>Profile .....</b>                                        | <b>8</b>                            |
| <b>Description .....</b>                                    | <b>8</b>                            |
| <b>Rationale Statement .....</b>                            | <b>8</b>                            |
| <b>Impact Statement.....</b>                                | <b>Error! Bookmark not defined.</b> |
| <b>Audit Procedure.....</b>                                 | <b>9</b>                            |
| <b>Remediation Procedure .....</b>                          | <b>9</b>                            |
| <b>Default Value.....</b>                                   | <b>Error! Bookmark not defined.</b> |
| <b>References .....</b>                                     | <b>Error! Bookmark not defined.</b> |
| <b>CIS Critical Security Controls® (CIS Controls®).....</b> | <b>Error! Bookmark not defined.</b> |
| <b>Additional Information .....</b>                         | <b>9</b>                            |
| <b>Profile Definitions .....</b>                            | <b>10</b>                           |
| <b>Acknowledgements.....</b>                                | <b>12</b>                           |
| <b>Recommendations.....</b>                                 | <b>13</b>                           |
| <b>1 STIG RULES .....</b>                                   | <b>13</b>                           |
| 1.1 APPL-14-000001 (Manual).....                            | 14                                  |
| 1.2 APPL-14-000002 (Manual).....                            | 15                                  |
| 1.3 APPL-14-000003 (Manual).....                            | 16                                  |

|                                                                                                                                                                                                                                                                                         |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1.4 APPL-14-000005 (Manual).....                                                                                                                                                                                                                                                        | 18  |
| 1.5 APPL-14-000009 (Manual).....                                                                                                                                                                                                                                                        | 20  |
| 1.6 APPL-14-000007 (Manual).....                                                                                                                                                                                                                                                        | 21  |
| 1.7 APPL-14-000012 (Manual).....                                                                                                                                                                                                                                                        | 22  |
| 1.8 APPL-14-000014 (Manual).....                                                                                                                                                                                                                                                        | 25  |
| 1.9 APPL-14-000022 (Manual).....                                                                                                                                                                                                                                                        | 27  |
| 1.10 APPL-14-000023 (Manual).....                                                                                                                                                                                                                                                       | 29  |
| 1.11 APPL-14-000024 (Manual).....                                                                                                                                                                                                                                                       | 32  |
| 1.12 APPL-14-000025 (Manual).....                                                                                                                                                                                                                                                       | 34  |
| 1.13 APPL-14-000030 (Manual).....                                                                                                                                                                                                                                                       | 38  |
| 1.14 APPL-14-000031 (Manual).....                                                                                                                                                                                                                                                       | 40  |
| 1.15 APPL-14-000033 (Manual).....                                                                                                                                                                                                                                                       | 42  |
| 1.16 APPL-14-000051 (Manual).....                                                                                                                                                                                                                                                       | 44  |
| 1.17 APPL-14-000052 (Manual).....                                                                                                                                                                                                                                                       | 46  |
| 1.18 APPL-14-000053 (Manual).....                                                                                                                                                                                                                                                       | 48  |
| 1.19 APPL-14-000054 (Manual).....                                                                                                                                                                                                                                                       | 50  |
| 1.20 APPL-14-000057 (Manual).....                                                                                                                                                                                                                                                       | 53  |
| 1.21 APPL-14-000060 (Manual).....                                                                                                                                                                                                                                                       | 56  |
| 1.22 APPL-14-000070 (Manual).....                                                                                                                                                                                                                                                       | 58  |
| 1.23 APPL-14-000090 (Manual).....                                                                                                                                                                                                                                                       | 60  |
| 1.24 APPL-14-000100 (Manual).....                                                                                                                                                                                                                                                       | 62  |
| 1.25 APPL-14-000110 (Manual).....                                                                                                                                                                                                                                                       | 64  |
| 1.26 APPL-14-000120 (Manual).....                                                                                                                                                                                                                                                       | 66  |
| 1.27 APPL-14-000130 (Manual).....                                                                                                                                                                                                                                                       | 68  |
| 1.28 APPL-14-000140 (Manual).....                                                                                                                                                                                                                                                       | 70  |
| 1.29 APPL-14-000160 (Manual).....                                                                                                                                                                                                                                                       | 72  |
| [IMPORTANT].....                                                                                                                                                                                                                                                                        | 72  |
| The automatic logout may cause disruptions to an organization's workflow and/or loss of data. Information system security officers (ISSOs) are advised to first fully weigh the potential risks posed to their organization before opting to disable the automatic logout setting. .... | 72  |
| 1.30 APPL-14-000170 (Manual).....                                                                                                                                                                                                                                                       | 74  |
| 1.31 APPL-14-000180 (Manual).....                                                                                                                                                                                                                                                       | 76  |
| 1.32 APPL-14-001001 (Manual).....                                                                                                                                                                                                                                                       | 78  |
| 1.33 APPL-14-001002 (Manual).....                                                                                                                                                                                                                                                       | 81  |
| 1.34 APPL-14-001003 (Manual).....                                                                                                                                                                                                                                                       | 83  |
| 1.35 APPL-14-001010 (Manual).....                                                                                                                                                                                                                                                       | 88  |
| 1.36 APPL-14-001012 (Manual).....                                                                                                                                                                                                                                                       | 90  |
| 1.37 APPL-14-001013 (Manual).....                                                                                                                                                                                                                                                       | 92  |
| 1.38 APPL-14-001014 (Manual).....                                                                                                                                                                                                                                                       | 94  |
| 1.39 APPL-14-001015 (Manual).....                                                                                                                                                                                                                                                       | 96  |
| 1.40 APPL-14-001016 (Manual).....                                                                                                                                                                                                                                                       | 98  |
| 1.41 APPL-14-001017 (Manual).....                                                                                                                                                                                                                                                       | 100 |
| 1.42 APPL-14-001020 (Manual).....                                                                                                                                                                                                                                                       | 102 |
| 1.43 APPL-14-001021 (Manual).....                                                                                                                                                                                                                                                       | 105 |
| 1.44 APPL-14-001022 (Manual).....                                                                                                                                                                                                                                                       | 108 |
| 1.45 APPL-14-001023 (Manual).....                                                                                                                                                                                                                                                       | 110 |
| 1.46 APPL-14-001024 (Manual).....                                                                                                                                                                                                                                                       | 112 |
| 1.47 APPL-14-001029 (Manual).....                                                                                                                                                                                                                                                       | 114 |
| 1.48 APPL-14-001030 (Manual).....                                                                                                                                                                                                                                                       | 115 |
| 1.49 APPL-14-001031 (Manual).....                                                                                                                                                                                                                                                       | 117 |
| 1.50 APPL-14-001044 (Manual).....                                                                                                                                                                                                                                                       | 119 |
| 1.51 APPL-14-001060 (Manual).....                                                                                                                                                                                                                                                       | 121 |
| 1.52 APPL-14-001100 (Manual).....                                                                                                                                                                                                                                                       | 123 |
| 1.53 APPL-14-001110 (Manual).....                                                                                                                                                                                                                                                       | 125 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                       |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1.54 APPL-14-001120 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 127 |
| 1.55 APPL-14-001130 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 129 |
| 1.56 APPL-14-001140 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 131 |
| 1.57 APPL-14-002001 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 133 |
| 1.58 APPL-14-002003 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 134 |
| 1.59 APPL-14-001150 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 135 |
| 1.60 APPL-14-002004 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 138 |
| 1.61 APPL-14-002005 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 139 |
| 1.62 APPL-14-002006 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 140 |
| 1.63 APPL-14-002007 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 141 |
| 1.64 APPL-14-002008 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 142 |
| 1.65 APPL-14-002009 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 143 |
| 1.66 APPL-14-002010 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 145 |
| [IMPORTANT].....                                                                                                                                                                                                                                                                                                                                                                                                                                      | 146 |
| Apple has deprecated the use of application restriction controls<br>( <a href="https://github.com/apple/device-management/blob/eb51fb0cb9626cac4717858556912c257a734ce0/mdm/profiles/com.apple.applicationaccess.new.yaml#L67-L70">https://github.com/apple/device-<br/>management/blob/eb51fb0cb9626cac4717858556912c257a734ce0/mdm/profiles/com.apple<br/>.applicationaccess.new.yaml#L67-L70</a> ). Using these controls may not work as expected. |     |
| Third-party software may be required to fulfill the compliance requirements. ....                                                                                                                                                                                                                                                                                                                                                                     | 146 |
| 1.67 APPL-14-002012 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 148 |
| 1.68 APPL-14-002013 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 149 |
| 1.69 APPL-14-002014 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 150 |
| 1.70 APPL-14-002015 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 151 |
| 1.71 APPL-14-002016 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 152 |
| 1.72 APPL-14-002017 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 153 |
| 1.73 APPL-14-002020 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 155 |
| 1.74 APPL-14-002021 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 156 |
| 1.75 APPL-14-002022 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 158 |
| 1.76 APPL-14-002035 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 160 |
| 1.77 APPL-14-002036 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 161 |
| 1.78 APPL-14-002037 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 162 |
| 1.79 APPL-14-002038 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 163 |
| 1.80 APPL-14-002039 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 165 |
| 1.81 APPL-14-002040 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 166 |
| 1.82 APPL-14-002041 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 167 |
| 1.83 APPL-14-002042 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 168 |
| 1.84 APPL-14-002043 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 169 |
| 1.85 APPL-14-002050 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 170 |
| 1.86 APPL-14-002051 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 171 |
| 1.87 APPL-14-002052 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 172 |
| 1.88 APPL-14-002053 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 173 |
| 1.89 APPL-14-002060 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 174 |
| 1.90 APPL-14-002062 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 176 |
| [IMPORTANT].....                                                                                                                                                                                                                                                                                                                                                                                                                                      | 176 |
| Information system security officers (ISSOs) may make the risk-based decision not to<br>disable Bluetooth to maintain necessary functionality, but they are advised to first fully weigh<br>the potential risks posed to their organization. ....                                                                                                                                                                                                     |     |
| 1.91 APPL-14-002063 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 178 |
| 1.92 APPL-14-002064 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 180 |
| 1.93 APPL-14-002066 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 181 |
| 1.94 APPL-14-002068 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 182 |
| 1.95 APPL-14-002069 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 183 |
| 1.96 APPL-14-002080 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 185 |
| 1.97 APPL-14-002090 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 187 |
| 1.98 APPL-14-002100 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                     | 188 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                             |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1.99 APPL-14-002110 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                           | 190 |
| [NOTE].....                                                                                                                                                                                                                                                                                                                                                                                                                                 | 190 |
| The check and fix are for the currently logged on user. To get the currently logged on user,<br>run the following. [source,bash] .....                                                                                                                                                                                                                                                                                                      | 190 |
| CURRENT_USER=\$( /usr/sbin/scutil <<< "show State:/Users/ConsoleUser"   /usr/bin/awk<br>'/Name :/ && ! /loginwindow/ { print \$3 }' ) .....                                                                                                                                                                                                                                                                                                 | 190 |
| 1.100 APPL-14-002120 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 192 |
| [IMPORTANT].....                                                                                                                                                                                                                                                                                                                                                                                                                            | 192 |
| Some organizations may allow the use and configuration of the built-in Mail.app,<br>Calendar.app, and Contacts.app for organizational communication. Information system<br>security officers (ISSOs) may make the risk-based decision not to disable the Internet<br>Accounts System Preference pane to avoid losing this functionality, but they are advised to<br>first fully weigh the potential risks posed to their organization. .... | 192 |
| 1.101 APPL-14-002130 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 194 |
| 1.102 APPL-14-002140 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 195 |
| 1.103 APPL-14-002150 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 196 |
| 1.104 APPL-14-002160 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 197 |
| 1.105 APPL-14-002170 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 198 |
| 1.106 APPL-14-002180 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 199 |
| 1.107 APPL-14-002190 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 201 |
| 1.108 APPL-14-002200 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 202 |
| 1.109 APPL-14-002210 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 203 |
| 1.110 APPL-14-002220 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 204 |
| 1.111 APPL-14-002230 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 205 |
| 1.112 APPL-14-002240 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 206 |
| 1.113 APPL-14-002250 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 207 |
| 1.114 APPL-14-002260 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 208 |
| 1.115 APPL-14-002270 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 209 |
| 1.116 APPL-14-003001 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 210 |
| 1.117 APPL-14-003007 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 211 |
| 1.118 APPL-14-003008 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 213 |
| 1.119 APPL-14-003010 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 215 |
| 1.120 APPL-14-003011 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 217 |
| 1.121 APPL-14-003012 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 219 |
| 1.122 APPL-14-003013 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 220 |
| [source,bash] .....                                                                                                                                                                                                                                                                                                                                                                                                                         | 220 |
| /usr/sbin/firmwarepasswd -setpasswd .....                                                                                                                                                                                                                                                                                                                                                                                                   | 220 |
| 1.123 APPL-14-003014 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 222 |
| 1.124 APPL-14-003020 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 223 |
| 1.125 APPL-14-003030 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 226 |
| 1.126 APPL-14-003050 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 228 |
| login: auth account password session .....                                                                                                                                                                                                                                                                                                                                                                                                  | 229 |
| 1.127 APPL-14-003051 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 231 |
| su: auth account password session .....                                                                                                                                                                                                                                                                                                                                                                                                     | 232 |
| Fix new file ownership and permissions .....                                                                                                                                                                                                                                                                                                                                                                                                | 232 |
| 1.128 APPL-14-003052 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 234 |
| sudo: auth account password session .....                                                                                                                                                                                                                                                                                                                                                                                                   | 235 |
| 1.129 APPL-14-003060 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 237 |
| 1.130 APPL-14-003070 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 239 |
| [source,xml] .....                                                                                                                                                                                                                                                                                                                                                                                                                          | 239 |
| [source,bash] .....                                                                                                                                                                                                                                                                                                                                                                                                                         | 239 |
| /usr/bin/pwpolicy setaccountpolicies \$pwpolicy_file .....                                                                                                                                                                                                                                                                                                                                                                                  | 240 |
| 1.131 APPL-14-003080 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                          | 241 |
| [source,xml] .....                                                                                                                                                                                                                                                                                                                                                                                                                          | 241 |
| [source,bash] .....                                                                                                                                                                                                                                                                                                                                                                                                                         | 241 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| /usr/bin/pwpolicy setaccountpolicies \$pwpolicy_file .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 241 |
| 1.132 APPL-14-004001 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 243 |
| 1.133 APPL-14-004002 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 245 |
| 1.134 APPL-14-004022 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 247 |
| 1.135 APPL-14-004030 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 249 |
| 1.136 APPL-14-004040 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 251 |
| 1.137 APPL-14-004050 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 253 |
| 1.138 APPL-14-004060 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 254 |
| 1.139 APPL-14-005001 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 256 |
| 1.140 APPL-14-005020 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 260 |
| 1.141 APPL-14-005050 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 262 |
| 1.142 APPL-14-005052 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 264 |
| 1.143 APPL-14-005054 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 265 |
| 1.144 APPL-14-005055 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 266 |
| 1.145 APPL-14-005056 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 267 |
| 1.146 APPL-14-005058 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 268 |
| 1.147 APPL-14-005060 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 270 |
| 1.148 APPL-14-005061 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 271 |
| 1.149 APPL-14-005070 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 272 |
| 1.150 APPL-14-005080 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 273 |
| [IMPORTANT].....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 274 |
| Apple has deprecated the use of application restriction controls<br>( <a href="https://github.com/apple/device-management/blob/eb51fb0cb9626cac4717858556912c257a734ce0/mdm/profiles/com.apple.applicationaccess.new.yaml#L67-L70">https://github.com/apple/device-management/blob/eb51fb0cb9626cac4717858556912c257a734ce0/mdm/profiles/com.apple.applicationaccess.new.yaml#L67-L70</a> ). Using these controls may not work as expected.<br>Third-party software may be required to fulfill the compliance requirements. .... | 274 |
| 1.151 APPL-14-005090 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 276 |
| [IMPORTANT].....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 276 |
| This feature is removed if a smart card is paired or smart card attribute mapping is<br>configured. ....                                                                                                                                                                                                                                                                                                                                                                                                                         | 276 |
| 1.152 APPL-14-005100 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 278 |
| 1.153 APPL-14-005110 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 280 |
| 1.154 APPL-14-005120 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 282 |
| 1.155 APPL-14-005130 (Manual).....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 283 |

## **Appendix: Summary Table..... 285**

## **Appendix: Change History..... 293**

# Overview

## Target Technology Details

Apple macOS 14 (Sonoma) Security Technical Implementation Guide Secure Technical Implementation Guide (STIG)  
Version: 2 Release: 3 Benchmark  
Date: 30 Jan 2025

## Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Apple macOS 14 (Sonoma) Security Technical Implementation Guide and are looking to comply with the STIG guidance

# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

## Description

The Rule Title from the STIG

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

## **Audit Procedure**

Systematic instructions for determining if the target system complies with the recommendation.

## **Remediation Procedure**

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## **Additional Information**

References from the STIG Rule if applicable.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

Items in this profile exhibit one or more of the following characteristics:

- are considered to be high severity
- are intended for environments or use cases where following STIG based security guidance is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

Items in this profile exhibit one or more of the following characteristics:

- are considered to be medium severity
- are intended for environments or use cases where following STIG based security guidance is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

Items in this profile exhibit one or more of the following characteristics:

- are considered to be low severity
- are intended for environments or use cases where following STIG based security guidance is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers and workstations.



## **Acknowledgements**

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Apple macOS 14 (Sonoma) Security Technical Implementation Guide.

# Recommendations

## 1 STIG RULES

Apple macOS 14.0

Apple macOS 14 (Sonoma) Security Technical Implementation Guide Secure Technical Implementation Guide (STIG)

Version: 2 Release: 3 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

## 1.1 APPL-14-000001 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must prevent Apple Watch from terminating a session lock.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259418<br>RULE ID: SV-259418r958400 |
|-------------------------------------------------|

### Rationale:

Disabling Apple watches is a necessary step to ensuring that the information system retains a session lock until the user reestablishes access using authorized identification and authentication procedures.

### Audit:

Verify the macOS system is configured to prevent Apple Watch from terminating a session lock with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowAutoUnlock').js
```

```
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to prevent Apple Watch from terminating a session lock by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

## 1.2 APPL-14-000002 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce screen saver password.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259419<br>RULE ID: SV-259419r958400 |
|-------------------------------------------------|

### Rationale:

Users must authenticate when unlocking the screen saver.

The screen saver acts as a session lock and prevents unauthorized users from accessing the current user's account.

### Audit:

Verify the macOS system is configured to prompt users to enter a password to unlock the screen saver with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')
```

```
.objectForKey('askForPassword').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to prompt users to enter a password to unlock the screen saver by installing the "com.apple.screensaver" configuration profile.

### Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

## 1.3 APPL-14-000003 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce session lock no more than five seconds after screen saver is started.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259420<br>RULE ID: SV-259420r958400 |
|-------------------------------------------------|

### Rationale:

A screen saver must be enabled and the system must be configured to require a password to unlock once the screensaver has been on for a maximum of five seconds.

An unattended system with an excessive grace period is vulnerable to a malicious user.

### Audit:

Verify the macOS system is configured to initiate a session lock within five seconds of the screen saver starting with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
function run() {
```

```
  let delay =
```

```
  ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')
```

```
    .objectForKey('askForPasswordDelay'))
```

```
    if ( delay <= 5 ) {
```

```
      return("true")
```

```
    } else {
```

```
      return("false")
```

```
    }
```

```
  }
```

```
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to initiate a session lock within five seconds of the screen saver starting by installing the "com.apple.screensaver" configuration profile.

### Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

## 1.4 APPL-14-000005 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure user session lock when a smart token is removed.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259421<br>RULE ID: SV-259421r1009577 |
|--------------------------------------------------|

### Rationale:

The screen lock must be configured to initiate automatically when the smart token is removed from the system.

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the information system but do not want to log out because of the temporary nature of their absence. While a session lock is not an acceptable substitute for logging out of an information system for longer periods of time, they prevent a malicious user from accessing the information system when a user has removed their smart token.

### Audit:

Verify the macOS system is configured to lock the user session when a smart token is removed with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')
```

```
.objectForKey('tokenRemovalAction').js  
EOS
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to lock the user session when a smart token is removed by installing the "com.apple.security.smartcard" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

### Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11
- NIST SP 800-53 Revision 4::AC-11 a

## 1.5 APPL-14-000009 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must prevent AdminHostInfo from being available at LoginWindow.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259423<br>RULE ID: SV-259423r958402 |
|-------------------------------------------------|

### Rationale:

The system must be configured to not display sensitive information at the LoginWindow. The key AdminHostInfo when configured will allow the HostName, IP Address, and operating system version and build to be displayed.

### Audit:

Verify the macOS system is configured to prevent AdminHostInfo from being available at LoginWindow with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')
```

```
.objectIsForcedForKey('AdminHostInfo')
```

```
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to prevent AdminHostInfo from being available at LoginWindow by installing the "com.apple.loginwindow" configuration profile.

### Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

## 1.6 APPL-14-000007 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable hot corners.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259422<br>RULE ID: SV-259422r958404 |
|-------------------------------------------------|

### Rationale:

Hot corners must be disabled.

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. Although hot corners can be used to initiate a session lock or to launch useful applications, they can also be configured to disable an automatic session lock from initiating. Such a configuration introduces the risk that a user might forget to manually lock the screen before stepping away from the computer.

### Audit:

Verify the macOS system is configured to disable hot corners with the following command:

```
/usr/bin/profiles -P -o stdout | /usr/bin/grep -Ec "'wvous-bl-corner' = 0|'wvous-br-corner' = 0|'wvous-tl-corner' = 0|'wvous-tr-corner' = 0'
```

If the result is not "4", this is a finding.

### Remediation:

Configure the macOS system to disable hot corners by installing the "com.apple.ManagedClient.preferences" configuration profile.

### Additional Information:

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

## 1.7 APPL-14-000012 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must automatically remove or disable temporary or emergency user accounts within 72 hours.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259424<br>RULE ID: SV-259424r958364 |
|-------------------------------------------------|

### Rationale:

The macOS is able to be configured to set an automated termination for 72 hours or less for all temporary or emergency accounts upon account creation.

Emergency administrator accounts are privileged accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Although the ability to create and use emergency administrator accounts is necessary for performing system maintenance during emergencies, these accounts present vulnerabilities to the system if they are not disabled and removed when they are no longer needed. Configuring the macOS to automatically remove or disable emergency accounts within 72 hours of creation mitigates the risks posed if one were to be created and accidentally left active once the crisis is resolved.

Emergency administrator accounts are different from infrequently used accounts (i.e., local logon accounts used by system administrators when network or normal logon is not available). Infrequently used accounts also remain available and are not subject to automatic termination dates. However, an emergency administrator account is normally a different account created for use by vendors or system maintainers.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

If temporary or emergency user accounts remain active when no longer needed or for an excessive period, these accounts may be targeted by attackers to gain unauthorized access. To mitigate this risk, automated termination of all temporary or emergency accounts must be set to 72 hours (or less) when the temporary or emergency account is created.

If no policy is enforced by a directory service, a password policy can be set with the "pwpolicy" utility. The variable names may vary depending on how the policy was set.

If there are no temporary or emergency accounts defined on the system, this is Not Applicable.

Satisfies: SRG-OS-000002-GPOS-00002,SRG-OS-000123-GPOS-00064

### **Audit:**

Verify if a password policy is enforced by a directory service by asking the system administrator (SA) or information system security officer (ISSO).

If no policy is enforced by a directory service, a password policy can be set with the "pwpolicy" utility. The variable names may vary depending on how the policy was set.

If there are no temporary or emergency accounts defined on the system, this is Not Applicable.

To check if the password policy is configured to disable a temporary or emergency account after 72 hours, run the following command to output the password policy to the screen, substituting the correct user name in place of username:

```
/usr/bin/pwpolicy -u username getaccountpolicies | tail -n +2
```

If there is no output, and password policy is not controlled by a directory service, this is a finding.

Otherwise, look for the line "policyCategoryAuthentication".

In the array that follows, there should be a section that contains a check that allows users to log in if "policyAttributeCurrentTime" is less than the result of adding "policyAttributeCreationTime" to 72 hours (259200 seconds). The check might use a variable defined in its "policyParameters" section.

If the check does not exist or if the check adds too great an amount of time to "policyAttributeCreationTime", this is a finding.

### **Remediation:**

This setting may be enforced using local policy or by a directory service.

To set local policy to disable a temporary or emergency user, create a plain text file containing the following:

After saving the file and exiting to the command prompt, run the following command to load the new policy file, substituting the correct user name in place of "username" and the path to the file in place of "/path/to/file".

```
/usr/bin/pwpolicy -u username setaccountpolicies /path/to/file
```

### **Additional Information:**

CCI-000016 Automatically remove or disable temporary and emergency accounts after an organization-defined time-period for each type of account.

- NIST SP 800-53::AC-2 (2)
- NIST SP 800-53A::AC-2 (2).1 (ii)
- NIST SP 800-53 Revision 4::AC-2 (2)
- NIST SP 800-53 Revision 5::AC-2 (2)

CCI-001682 Automatically remove or disable emergency accounts after an organization-defined time period for each type of account.

- NIST SP 800-53 Revision 5::AC-2 (2)
- NIST SP 800-53::AC-2 (2)
- NIST SP 800-53 Revision 4::AC-2 (2)
- NIST SP 800-53A::AC-2 (2).1 (ii)

## 1.8 APPL-14-000014 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce time synchronization.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259425<br>RULE ID: SV-259425r1038944 |
|--------------------------------------------------|

### Rationale:

Time synchronization must be enforced on all networked systems.

This rule ensures the uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Satisfies: SRG-OS-000355-GPOS-00143,SRG-OS-000356-GPOS-00144

### Audit:

Verify the macOS system is configured to enforce time synchronization with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.timed')
```

```
.objectForKey('TMAutomaticTimeOnlyEnabled').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to enforce time synchronization by installing the "com.apple.timed" configuration profile.

### Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

CCI-004922 Synchronize system clocks within and between systems or system components.

- NIST SP 800-53 Revision 5::SC-45

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (1) (a)

CCI-002046 The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

- NIST SP 800-53 Revision 4::AU-8 (1) (b)

## 1.9 APPL-14-000022 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must limit consecutive failed log on attempts to three.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259428<br>RULE ID: SV-259428r958388 |
|-------------------------------------------------|

### Rationale:

The macOS must be configured to limit the number of failed log on attempts to a maximum of three. When the maximum number of failed attempts is reached, the account must be locked for a period of time after.

This rule protects against malicious users attempting to gain access to the system via brute-force hacking methods.

Satisfies: SRG-OS-000021-GPOS-00005,SRG-OS-000329-GPOS-00128

### Audit:

Verify the macOS system is configured to limit consecutive failed log on attempts to three with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --  
xpath '//dict/key[text()="policyAttributeMaximumFailedAuthentications"]/following-  
sibling::integer[1]/text()' - | /usr/bin/awk '{ if ($1 <= 3) {print "yes"} else {print "no"}}'
```

If the result is not "yes", this is a finding.

### Remediation:

Configure the macOS system to limit consecutive failed log on attempts to three by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile or by a directory service.

### Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

## 1.10 APPL-14-000023 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must display the Standard Mandatory DOD Notice and Consent Banner at remote log on.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259429<br>RULE ID: SV-259429r958390 |
|-------------------------------------------------|

### Rationale:

Displaying a standardized and approved use notification before granting access to the operating system ensures that users are provided with privacy and security notification verbiage that is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060.

Satisfies: SRG-OS-000023-GPOS-00006,SRG-OS-000024-GPOS-00007

**Audit:**

Verify the macOS system is configured to display the Standard Mandatory DOD Notice and Consent Banner before granting remote access to the operating system.

Verify the operating system has the correct text listed in the "/etc/banner" file with the following command:

```
/usr/bin/more /etc/banner
```

The command must return the following text:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

If the operating system does not display a logon banner before granting remote access or the banner does not match the Standard Mandatory DOD Notice and Consent Banner, this is a finding.

If the text in the "/etc/banner" file does not match the Standard Mandatory DOD Notice and Consent Banner, this is a finding.

**Remediation:**

Configure the macOS system to display the Standard Mandatory DOD Notice and Consent Banner before granting remote access to the operating system by creating a text file containing the required DOD text.

Name the file "banner" and place it in "/etc/".

**Additional Information:**

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

## 1.11 APPL-14-000024 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce SSH to display the Standard Mandatory DOD Notice and Consent Banner.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259430<br>RULE ID: SV-259430r958390 |
|-------------------------------------------------|

### Rationale:

Displaying a standardized and approved use notification before granting access to the operating system ensures that users are provided with privacy and security notification verbiage that is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060.

Note: /etc/ssh/sshd\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000023-GPOS-00006,SRG-OS-000024-GPOS-00007

### Audit:

Verify the macOS system is configured to display the contents of "/etc/banner" before granting access to the system with the following command:

```
/usr/sbin/sshd -G | /usr/bin/grep -c "^banner /etc/banner"
```

If the command does not return "1", this is a finding.

### Remediation:

Configure the macOS system to display the contents of "/etc/banner" before granting access to the system by creating a plain text file in the /private/etc/ssh/sshd\_config.d/ directory containing the following:

```
banner /etc/banner
```

### Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

## 1.12 APPL-14-000025 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must display the Standard Mandatory DOD Notice and Consent Banner at the login window.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259431<br>RULE ID: SV-259431r958390 |
|-------------------------------------------------|

### Rationale:

Displaying a standardized and approved use notification before granting access to the operating system ensures that users are provided with privacy and security notification verbiage that is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The policy banner will show if a "PolicyBanner.rtf" or "PolicyBanner.rtf.d" exists in the "/Library/Security" folder.

The banner must be formatted in accordance with DTM-08-060.

Satisfies: SRG-OS-000023-GPOS-00006,SRG-OS-000024-GPOS-00007,SRG-OS-000228-GPOS-00088

## Audit:

Verify the macOS system is configured to display a policy banner with the following command:

```
/bin/ls -ld /Library/Security/PolicyBanner.rtf* | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If "PolicyBanner.rtf" does not exist, this is a finding.

If the permissions for "PolicyBanner.rtf" are not "644", this is a finding.

The banner text of the document must read:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

If the text is not worded exactly this way, this is a finding.

## Remediation:

Configure the macOS system to display a policy banner by creating an RTF file containing the required text. Name the file "PolicyBanner.rtf" and place it in "/Library/Security/".

Update the permissions of the "/Library/Security/PolicyBanner.rtf" file with the following command:

```
/usr/bin/sudo /bin/chmod 644 /Library/Security/PolicyBanner.rtf
```

## Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a

- NIST SP 800-53 Revision 5::AC-8 a

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2

- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (iii)
- NIST SP 800-53 Revision 4::AC-8 c 3
- NIST SP 800-53 Revision 5::AC-8 c 3

## 1.13 APPL-14-000030 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit log files to not contain access control lists.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259432<br>RULE ID: SV-259432r958434 |
|-------------------------------------------------|

### Rationale:

The audit log files must not contain access control lists (ACLs).

This rule ensures that audit information and audit files are configured to be readable and writable only by system administrators, thereby preventing unauthorized access, modification, and deletion of files.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured without ACLs applied to log files with the following command:

```
/bin/ls -le $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') | /usr/bin/awk '{print $1}' | /usr/bin/grep -c ":"
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system without ACLs applied to log files with the following command:

```
/bin/chmod -RN /var/audit
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.14 APPL-14-000031 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit log folders to not contain access control lists.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259433<br>RULE ID: SV-259433r958434 |
|-------------------------------------------------|

### Rationale:

The audit log folder must not contain access control lists (ACLs).

Audit logs contain sensitive data about the system and users. This rule ensures that the audit service is configured to create log folders that are readable and writable only by system administrators in order to prevent normal users from reading audit logs.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured without ACLs applied to log folders with the following command:

```
/bin/ls -lde /var/audit | /usr/bin/awk '{print $1}' | /usr/bin/grep -c ":",
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system without ACLs applied to log folders with the following command:

```
/bin/chmod -N /var/audit
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9

- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.15 APPL-14-000033 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable FileVault automatic log on.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259434<br>RULE ID: SV-259434r958472 |
|-------------------------------------------------|

### Rationale:

If FileVault is enabled, automatic log on must be disabled, so that both FileVault and login window authentication are required.

The default behavior of macOS when FileVault is enabled is to automatically log on to the computer once successfully passing user's FileVault credentials.

Note: DisableFDEAutoLogin does not have to be set on Apple Silicon-based macOS systems that are smartcard enforced, as smartcards are available at preboot.

### Audit:

Verify the macOS system is configured to disable filevault automatic login with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')
```

```
.objectForKey('DisableFDEAutoLogin').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable filevault automatic login by installing the "com.apple.loginwindow" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3

- NIST SP 800-53 Revision 5::AC-3

## 1.16 APPL-14-000051 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure SSHD ClientAliveInterval to 900.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259435<br>RULE ID: SV-259435r970703 |
|-------------------------------------------------|

### Rationale:

If SSHD is enabled, then it must be configured with the Client Alive Interval set to 900.

Sets a timeout interval in seconds after which if no data has been received from the client, sshd(8) will send a message through the encrypted channel to request a response from the client.

This setting works in conjunction with ClientAliveCountMax to determine the termination of the connection after the threshold has been reached.

Note: This setting is not intended to manage idle user sessions where there is no input from the client. Its purpose is to monitor for interruptions in network connectivity and force the session to terminate after the connection appears to be broken.

Note: /etc/ssh/sshd\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

### Audit:

Verify the macOS system is configured to set the SSHD ClientAliveInterval to 900 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/clientaliveinterval/{print $2}'
```

If the result is not "900", this is a finding.

## Remediation:

Configure the macOS system to set the SSHD ClientAliveInterval to 900 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '\n')
if [[ -z $include_dir ]]; then
/usr/bin/sed -i.bk "1s/.*/Include /etc/ssh/sshd_config.d/*/ /etc/ssh/sshd_config
fi
/usr/bin/grep -qxF 'clientaliveinterval 900' "${include_dir}01-mscp-sshd.conf" 2>/dev/null
|| echo "clientaliveinterval 900" >> "${include_dir}01-mscp-sshd.conf"
for file in $(ls ${include_dir}); do
if [[ "$file" == "100-macos.conf" ]]; then
continue
fi
if [[ "$file" == "01-mscp-sshd.conf" ]]; then
break
fi
/bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

## Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

## 1.17 APPL-14-000052 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure SSHD ClientAliveCountMax to 1.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259436<br>RULE ID: SV-259436r970703 |
|-------------------------------------------------|

### Rationale:

If SSHD is enabled it must be configured with the Client Alive Maximum Count set to 1.

This will set the number of client alive messages which may be sent without the SSH server receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, the SSH server will disconnect the client, terminating the session. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive.

Note: This setting is not intended to manage idle user sessions where there is no input from the client. Its purpose is to monitor for interruptions in network connectivity and force the session to terminate after the connection appears to be broken.

Note: /etc/ssh/sshd\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

### Audit:

Verify the macOS system is configured to set the SSHD ClientAliveCountMax to 1 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/clientalivecountmax/{print $2}'
```

If the result is not "1", this is a finding.

## Remediation:

Configure the macOS system to set the SSHD ClientAliveCountMax to 1 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '\n')
if [[ -z $include_dir ]]; then
/usr/bin/sed -i.bk "1s/.*/Include /etc/ssh/sshd_config.d/*/ /etc/ssh/sshd_config
fi
/usr/bin/grep -qxF 'clientalivecountmax 1' "${include_dir}01-mscp-sshd.conf" 2>/dev/null
|| echo "clientalivecountmax 1" >> "${include_dir}01-mscp-sshd.conf"
for file in $(ls ${include_dir}); do
if [[ "$file" == "100-macos.conf" ]]; then
continue
fi
if [[ "$file" == "01-mscp-sshd.conf" ]]; then
break
fi
/bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

## Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

## 1.18 APPL-14-000053 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must set Login Grace Time to 30.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259437<br>RULE ID: SV-259437r970703 |
|-------------------------------------------------|

### Rationale:

If SSHD is enabled, then it must be configured to wait only 30 seconds before timing out logon attempts.

Note: /etc/ssh/sshd\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

### Audit:

Verify the macOS system is configured to set Login Grace Time to 30 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/logingracetime/{print $2}'
```

If the result is not "30", this is a finding.

### Remediation:

Configure the macOS system to set Login Grace Time to 30 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d ' ')
if [[ -z $include_dir ]]; then
  /usr/bin/sed -i.bk "1s/.*/Include /etc/ssh/sshd_config.d/*/\" /etc/ssh/sshd_config
fi
/usr/bin/grep -qxF 'logingracetime 30' "${include_dir}01-mscp-sshd.conf" 2>/dev/null ||
echo "logingracetime 30" >> "${include_dir}01-mscp-sshd.conf"
for file in $(ls ${include_dir}); do
  if [[ "$file" == "100-macos.conf" ]]; then
    continue
  fi
  if [[ "$file" == "01-mscp-sshd.conf" ]]; then
    break
  fi
  /bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

**Additional Information:**

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

## 1.19 APPL-14-000054 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must limit SSHD to FIPS-compliant connections.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259438<br>RULE ID: SV-259438r958408 |
|-------------------------------------------------|

### Rationale:

If SSHD is enabled then it must be configured to limit the Ciphers, HostbasedAcceptedAlgorithms, HostKeyAlgorithms, KexAlgorithms, MACs, PubkeyAcceptedAlgorithms, CASignatureAlgorithms 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: For more information on FIPS compliance with the version of SSHD included in the macOS, the manual page `apple_ssh_and_fips` has additional information.

Satisfies: SRG-OS-000033-GPOS-00014,SRG-OS-000120-GPOS-00061,SRG-OS-000250-GPOS-00093,SRG-OS-000393-GPOS-00173,SRG-OS-000394-GPOS-00174,SRG-OS-000396-GPOS-00176,SRG-OS-000424-GPOS-00188,SRG-OS-000478-GPOS-00223

## Audit:

Verify the macOS system is configured to limit SSHD to FIPS-compliant connections with the following command:

```
fips_sshd_config=("Ciphers aes128-gcm@openssh.com"  
"HostbasedAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com" "HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com" "KexAlgorithms ecdh-sha2-nistp256" "MACs hmac-sha2-256"  
"PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com" "CASignatureAlgorithms ecdsa-sha2-nistp256")  
total=0  
for config in $fips_sshd_config; do  
total=$((expr $(/usr/sbin/sshd -G | /usr/bin/grep -i -c "$config") + $total))  
done  
echo $total  
If the result is not "7", this is a finding.
```

## Remediation:

Configure the macOS system to limit SSHD to FIPS-compliant connections with the following command:

```
fips_sshd_config="Ciphers aes128-gcm@openssh.com  
HostbasedAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com  
HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com  
KexAlgorithms ecdh-sha2-nistp256  
MACs hmac-sha2-256  
PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com  
CASignatureAlgorithms ecdsa-sha2-nistp256"  
/bin/echo "${fips_sshd_config}" > /etc/ssh/sshd_config.d/fips_sshd_config
```

## Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7

- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

## 1.20 APPL-14-000057 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must limit SSH to FIPS-compliant connections.

GROUP ID: V-259439  
RULE ID: SV-259439r958408

### Rationale:

SSH must be configured to limit the Ciphers, HostbasedAcceptedAlgorithms, HostKeyAlgorithms, KexAlgorithms, MACs, PubkeyAcceptedAlgorithms, CASignatureAlgorithms 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: For more information on FIPS compliance with the version of SSH included in the macOS, the manual page `apple_ssh_and_fips` has additional information.

Satisfies: SRG-OS-000033-GPOS-00014,SRG-OS-000120-GPOS-00061,SRG-OS-000250-GPOS-00093,SRG-OS-000396-GPOS-00176,SRG-OS-000424-GPOS-00188,SRG-OS-000478-GPOS-00223

### Audit:

Verify the macOS system is configured to limit SSH to FIPS-compliant connections with the following command:

```
fips_ssh_config="Host *
```

```
Ciphers aes128-gcm@openssh.com
```

```
HostbasedAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
```

```
HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
```

```
KexAlgorithms ecdh-sha2-nistp256
```

```
MACs hmac-sha2-256
```

```
PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
```

```
CASignatureAlgorithms ecdsa-sha2-nistp256"
```

```
/usr/bin/grep -c "$fips_ssh_config" /etc/ssh/ssh_config.d/fips_ssh_config
```

If the result is not "8", this is a finding.

## Remediation:

Configure the macOS system to limit SSH to FIPS-compliant connections with the following command:

```
fips_ssh_config="Host *
```

```
Ciphers aes128-gcm@openssh.com
```

```
HostbasedAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
```

```
HostKeyAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
```

```
KexAlgorithms ecdh-sha2-nistp256
```

```
MACs hmac-sha2-256
```

```
PubkeyAcceptedAlgorithms ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com
```

```
CASignatureAlgorithms ecdsa-sha2-nistp256"
```

```
/bin/echo "${fips_ssh_config}" > /etc/ssh/ssh_config.d/fips_ssh_config
```

## Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

## 1.21 APPL-14-000060 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must set account lockout time to 15 minutes.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259440<br>RULE ID: SV-259440r958388 |
|-------------------------------------------------|

### Rationale:

The macOS must be configured to enforce a lockout time period of at least 15 minutes when the maximum number of failed logon attempts is reached.

This rule protects against malicious users attempting to gain access to the system via brute-force hacking methods.

Satisfies: SRG-OS-000021-GPOS-00005,SRG-OS-000329-GPOS-00128

### Audit:

Verify the macOS system is configured to set account lockout time to 15 minutes with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --  
xpath '//dict/key[text()="autoEnableInSeconds"]/following-sibling::integer[1]/text()' - |  
/usr/bin/awk '{ if ($1/60 >= 15 ) {print "yes"} else {print "no"}}'
```

If the result is not "yes", this is a finding.

### Remediation:

Configure the macOS system to set account lockout time to 15 minutes by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile or by a directory service.

### Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

## 1.22 APPL-14-000070 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce screen saver timeout.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259441<br>RULE ID: SV-259441r958402 |
|-------------------------------------------------|

### Rationale:

The screen saver timeout must be set to 900 seconds or a shorter length of time.

This rule ensures that a full session lock is triggered within no more than 900 seconds of inactivity.

### Audit:

Verify the macOS system is configured to initiate the screen saver timeout after 15 minutes of inactivity with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
let timeout =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.screensaver')
.objectForKey('idleTime'))
if ( timeout <= 900 ) {
return("true")
} else {
return("false")
}
}
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to initiate the screen saver after 15 minutes of inactivity by installing the "com.apple.screensaver" configuration profile.

### Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

## 1.23 APPL-14-000090 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable login to other user's active and locked sessions.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259443<br>RULE ID: SV-259443r1009579 |
|--------------------------------------------------|

### Rationale:

The ability to log in to another user's active or locked session must be disabled.

macOS has a privilege that can be granted to any user that will allow that user to unlock active user's sessions. Disabling the admins and/or user's ability to log into another user's active and locked session prevents unauthorized persons from viewing potentially sensitive and/or personal information.

Note: Configuring this setting will disable TouchID from unlocking the screensaver.

### Audit:

Verify the macOS system is configured to disable login to other user's active and locked sessions with the following command:

```
/usr/bin/security authorizationdb read system.login.screensaver 2>&1 | /usr/bin/grep -c 'authenticate-session-owner'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable login to other user's active and locked sessions with the following command:

```
/usr/bin/security authorizationdb write system.login.screensaver "authenticate-session-owner"
```

### Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5::IA-2 (5)

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

- NIST SP 800-53::IA-2 (5) (b)
- NIST SP 800-53A::IA-2 (5).2 (ii)
- NIST SP 800-53 Revision 4::IA-2 (5)

## 1.24 APPL-14-000100 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable root login.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259444<br>RULE ID: SV-259444r1009580 |
|--------------------------------------------------|

### Rationale:

To ensure individual accountability and prevent unauthorized access, logging in as root at the login window must be disabled.

The macOS system must require individuals to be authenticated with an individual authenticator prior to using a group authenticator, and administrator users must never log in directly as root.

Satisfies: SRG-OS-000104-GPOS-00051,SRG-OS-000109-GPOS-00056,SRG-OS-000364-GPOS-00151

### Audit:

Verify the macOS system is configured to disable root login with the following command:

```
/usr/bin/dscl . -read /Users/root UserShell 2>&1 | /usr/bin/grep -c "/usr/bin/false"
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable root login with the following command:

```
/usr/bin/dscl . -create /Users/root UserShell /usr/bin/false
```

### Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5::IA-2 (5)

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

- NIST SP 800-53::IA-2 (5) (b)
- NIST SP 800-53A::IA-2 (5).2 (ii)
- NIST SP 800-53 Revision 4::IA-2 (5)

## 1.25 APPL-14-000110 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure SSH ServerAliveInterval option set to 900.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259445<br>RULE ID: SV-259445r970703 |
|-------------------------------------------------|

### Rationale:

SSH must be configured with an Active Server Alive Maximum Count set to 900.

Setting the Active Server Alive Maximum Count to 900 will log users out after a 900-second interval of inactivity.

Note: /etc/ssh/ssh\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

### Audit:

Verify the macOS system is configured to set the SSH ServerAliveInterval option set to 900 with the following command:

```
ret="pass"
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
sshCheck=$(/usr/bin/sudo -u $u /usr/bin/ssh -G . | /usr/bin/grep -c "^serveraliveinterval
900")
if [[ "$sshCheck" == "0" ]]; then
ret="fail"
break
fi
done
/bin/echo $ret
```

If the result is not "pass", this is a finding.

**Remediation:**

Configure the macOS system to set the SSH `ServerAliveInterval` option set to 900 with the following command:

```
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
config=$(/usr/bin/sudo -u $u /usr/bin/ssh -Gv . 2>&1 | /usr/bin/awk '/Reading
configuration data/ {print $NF}' | /usr/bin/tr -d '\r')
configarray=( ${f}config )
for c in $configarray; do
/usr/bin/sudo -u $u /usr/bin/grep -q '^ServerAliveInterval' "$c" && /usr/bin/sed -i "
's/.ServerAliveInterval./ServerAliveInterval 900/' "$c" || /bin/echo 'ServerAliveInterval
900' >> "$c"
done
done
```

**Additional Information:**

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

## 1.26 APPL-14-000120 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure SSHD Channel Timeout to 900.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259446<br>RULE ID: SV-259446r970703 |
|-------------------------------------------------|

### Rationale:

If SSHD is enabled it must be configured with session Channel Timeout set to 900.

This will set the time out when the session is inactive.

Note: /etc/ssh/sshd\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000163-GPOS-00072,SRG-OS-000279-GPOS-00109

### Audit:

Verify the macOS system is configured to set the SSHD Channel Timeout to 900 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk -F "=" '/channevertimeout session:*/{print $2}'
```

If the result is not "900", this is a finding.

## Remediation:

Configure the macOS system to set the SSHD Channel Timeout to 900 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '\n')
if [[ -z $include_dir ]]; then
/usr/bin/sed -i.bk "1s/.*/Include /etc/ssh/sshd_config.d/*/ /etc/ssh/sshd_config
fi
/usr/bin/grep -qxF 'channeltimeout session:=900' "${include_dir}01-mscp-sshd.conf"
2>/dev/null || echo "channeltimeout session:=900" >> "${include_dir}01-mscp-
sshd.conf"
for file in $(ls $include_dir); do
if [[ "$file" == "100-macos.conf" ]]; then
continue
fi
if [[ "$file" == "01-mscp-sshd.conf" ]]; then
break
fi
/bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

## Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

## 1.27 APPL-14-000130 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure SSHD unused connection timeout to 900.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259447<br>RULE ID: SV-259447r1009527 |
|--------------------------------------------------|

### Rationale:

If SSHD is enabled, it must be configured with unused connection timeout set to 900.

This will set the timeout when there are no open channels within a session.

Note: /etc/ssh/sshd\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000163-GPOS-00072,SRG-OS-000279-GPOS-00109

### Audit:

Verify the macOS system is configured to set the SSHD unused connection timeout to 900 with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/unusedconnectiontimeout/{print $2}'
```

If the result is not "900", this is a finding.

**Remediation:**

Configure the macOS system to set the SSHD unused connection timeout to 900 with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '\n')
if [[ -z $include_dir ]]; then
/usr/bin/sed -i.bk "1s/.*/Include /etc/ssh/sshd_config.d/*/ /etc/ssh/sshd_config
fi
/usr/bin/grep -qxF 'unusedconnectiontimeout 900' "${include_dir}01-miscp-sshd.conf"
2>/dev/null || echo "unusedconnectiontimeout 900" >> "${include_dir}01-miscp-
sshd.conf"
for file in $(ls ${include_dir}); do
if [[ "$file" == "100-macos.conf" ]]; then
continue
fi
if [[ "$file" == "01-miscp-sshd.conf" ]]; then
break
fi
/bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

**Additional Information:**

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

## 1.28 APPL-14-000140 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must set SSH Active Server Alive Maximum to 0.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259448<br>RULE ID: SV-259448r970703 |
|-------------------------------------------------|

### Rationale:

SSH must be configured with an Active Server Alive Maximum Count set to 0. Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session or an incomplete login attempt will also free up resources committed by the managed network element.

Note: /etc/ssh/ssh\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

### Audit:

Verify the macOS system is configured to set SSH Active Server Alive Maximum to 0 with the following command:

```
ret="pass"
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
sshCheck=$(/usr/bin/sudo -u $u /usr/bin/ssh -G . | /usr/bin/grep -c
"^serveralivecountmax 0")
if [[ "$sshCheck" == "0" ]]; then
ret="fail"
break
fi
done
/bin/echo $ret
If the result is not "pass", this is a finding.
```

**Remediation:**

Configure the macOS system to set SSH Active Server Alive Maximum to 0 with the following command:

```
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do
config=$(/usr/bin/sudo -u $u /usr/bin/ssh -Gv . 2>&1 | /usr/bin/awk '/Reading
configuration data/ {print $NF}' | /usr/bin/tr -d '\r')
configarray=( ${f}config )
for c in $configarray; do
/usr/bin/sudo -u $u /usr/bin/grep -q '^ServerAliveCountMax' "$c" && /usr/bin/sed -i "
's/.ServerAliveCountMax./ServerAliveCountMax 0/' "$c" || /bin/echo
'ServerAliveCountMax 0' >> "$c"
done
done
```

**Additional Information:**

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

## 1.29 APPL-14-000160 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce auto logout after 86400 seconds of inactivity.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259449<br>RULE ID: SV-259449r958636 |
|-------------------------------------------------|

### Rationale:

Auto logout must be configured to automatically terminate a user session and log out the after 86400 seconds of inactivity.

Note: The maximum that macOS can be configured for autologoff is 86400 seconds.

## [IMPORTANT]

**The automatic logout may cause disruptions to an organization's workflow and/or loss of data. Information system security officers (ISSOs) are advised to first fully weigh the potential risks posed to their organization before opting to disable the automatic logout setting.**

### Audit:

Verify the macOS system is configured to enforce auto logout after 86400 seconds of inactivity with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('.GlobalPreferences')
```

```
.objectForKey('com.apple.autologout.AutoLogOutDelay').js  
EOS
```

If the result is not "86400", this is a finding.

### Remediation:

Configure the macOS system to enforce auto logout after 86400 seconds of inactivity by installing the "com.apple.GlobalPreferences" configuration profile.

**Additional Information:**

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

## 1.30 APPL-14-000170 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must be configured to use an authorized time server.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259450<br>RULE ID: SV-259450r1038944 |
|--------------------------------------------------|

### Rationale:

Approved time servers must be the only servers configured for use.

This rule ensures the uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

An authoritative time server is synchronized with redundant United States Naval Observatory (USNO) time servers as designated for the appropriate DOD network.

Satisfies: SRG-OS-000355-GPOS-00143,SRG-OS-000356-GPOS-00144

### Audit:

Verify the macOS system is configured to use an authorized time server with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')
```

```
.objectForKey('timeServer').js  
EOS
```

If the result is not an authoritative time server which is synchronized with redundant USNO time servers as designated for the appropriate DOD network, this is a finding.

### Remediation:

Configure the macOS system to use an authorized time server by installing the "com.apple.MCX" configuration profile.

### Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (1) (a)

CCI-002046 The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

- NIST SP 800-53 Revision 4::AU-8 (1) (b)

## 1.31 APPL-14-000180 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enable time synchronization daemon.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259451<br>RULE ID: SV-259451r1038944 |
|--------------------------------------------------|

### Rationale:

The macOS time synchronization daemon (timed) must be enabled for proper time synchronization to an authorized time server.

Note: The time synchronization daemon is enabled by default on macOS.

Satisfies: SRG-OS-000355-GPOS-00143,SRG-OS-000356-GPOS-00144

### Audit:

Verify the macOS system is configured to enable time synchronization daemon with the following command:

```
/bin/launchctl list | /usr/bin/grep -c com.apple.timed
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to enable time synchronization daemon with the following command:

```
/bin/launchctl load -w /System/Library/LaunchDaemons/com.apple.timed.plist
```

### Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

CCI-004922 Synchronize system clocks within and between systems or system components.

- NIST SP 800-53 Revision 5::SC-45

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (1) (a)

CCI-002046 The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

- NIST SP 800-53 Revision 4::AU-8 (1) (b)

## 1.32 APPL-14-001001 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must be configured to audit all administrative action events.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259452<br>RULE ID: SV-259452r1009583 |
|--------------------------------------------------|

### Rationale:

Administrative action events include changes made to the system (e.g., modifying authentication policies). If audit records do not include "ad" events, it is difficult to identify incidents and to correlate incidents to subsequent events. Audit records can be generated from various components within the information system (e.g., via a module or policy filter).

Administrative and privileged access, including administrative use of the command line tools "kextload" and "kextunload" and changes to configuration settings, are logged by way of the "ad" flag.

Satisfies: SRG-OS-000004-GPOS-00004,SRG-OS-000239-GPOS-00089,SRG-OS-000240-GPOS-00090,SRG-OS-000241-GPOS-00091,SRG-OS-000327-GPOS-00127,SRG-OS-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000471-GPOS-00215,SRG-OS-000471-GPOS-00216,SRG-OS-000476-GPOS-00221

### Audit:

Verify the macOS system is configured to audit privileged access with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF } /etc/security/audit_control | /usr/bin/tr ',' '\n' | /usr/bin/grep -Ec 'ad'
```

If "ad" is not listed in the output, this is a finding.

### Remediation:

Configure the macOS system to audit privileged access with the following command:

```
/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
```

A text editor may also be used to implement the required updates to the "/etc/security/audit\_control" file.

### Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002234 Log the execution of privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (9)
- NIST SP 800-53 Revision 5::AC-6 (9)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-004188 Monitor the use of maintenance tools that execute with increased privilege.

- NIST SP 800-53 Revision 5::MA-3 (5)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

## 1.33 APPL-14-001002 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must be configured to audit all log on and log out events.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259453<br>RULE ID: SV-259453r958406 |
|-------------------------------------------------|

### Rationale:

The audit system must be configured to record all attempts to log in and out of the system (lo).

Frequently, an attacker that successfully gains access to a system has only gained access to an account with limited privileges, such as a guest account or a service account. The attacker must attempt to change to another user account with normal or elevated privileges in order to proceed. Auditing both successful and unsuccessful attempts to switch to another user account (by way of monitoring log on and log out events) mitigates this risk.

The information system monitors log on and log out events.

Satisfies: SRG-OS-000032-GPOS-00013,SRG-OS-000064-GPOS-00033,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000470-GPOS-00214,SRG-OS-000471-GPOS-00215,SRG-OS-000471-GPOS-00216,SRG-OS-000472-GPOS-00217,SRG-OS-000473-GPOS-00218

### Audit:

Verify the macOS system is configured to audit all log on and log out events with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ' ' '\n' |  
/usr/bin/grep -Ec '^lo'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to audit all log on and log out events with the following command:

```
/usr/bin/grep -qE "^flags.*[^\-]lo" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/  
s/$/,lo/' /etc/security/audit_control; /usr/sbin/audit -s
```

A text editor may also be used to implement the required updates to the "/etc/security/audit\_control" file.

**Additional Information:**

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53::AC-17 (1)
- NIST SP 800-53A::AC-17 (1).1
- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

## 1.34 APPL-14-001003 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enable security auditing.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259454<br>RULE ID: SV-259454r1009584 |
|--------------------------------------------------|

### Rationale:

Audit records establish what types of events have occurred, when they occurred, and which users were involved. These records aid an organization in their efforts to establish, correlate, and investigate the events leading up to an outage or attack.

The content required to be captured in an audit record varies based on the impact level of an organization's system. Content that may be necessary to satisfy this requirement includes, for example, time stamps, source addresses, destination addresses, user identifiers, event descriptions, success/fail indications, filenames involved, and access or flow control rules invoked.

The information system initiates session audits at system startup.

Note: Security auditing is enabled by default on macOS.

Satisfies: SRG-OS-000037-GPOS-00015,SRG-OS-000038-GPOS-00016,SRG-OS-000039-GPOS-00017,SRG-OS-000040-GPOS-00018,SRG-OS-000041-GPOS-00019,SRG-OS-000042-GPOS-00020,SRG-OS-000042-GPOS-00021,SRG-OS-000055-GPOS-00026,SRG-OS-000254-GPOS-00095,SRG-OS-000255-GPOS-00096,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099,SRG-OS-000303-GPOS-00120,SRG-OS-000337-GPOS-00129,SRG-OS-000358-GPOS-00145,SRG-OS-000359-GPOS-00146,SRG-OS-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000461-GPOS-00205,SRG-OS-000462-GPOS-00206,SRG-OS-000463-GPOS-00207,SRG-OS-000465-GPOS-00209,SRG-OS-000466-GPOS-00210,SRG-OS-000467-GPOS-00211,SRG-OS-000468-GPOS-00212,SRG-OS-000470-GPOS-00214,SRG-OS-000471-GPOS-00215,SRG-OS-000471-GPOS-00216,SRG-OS-000472-GPOS-00217,SRG-OS-000473-GPOS-00218,SRG-OS-000474-GPOS-00219,SRG-OS-000475-GPOS-00220,SRG-OS-000476-GPOS-00221,SRG-OS-000477-GPOS-00222

**Audit:**

Verify the macOS system is configured to enable the auditd service with the following command:

```
LAUNCHD_RUNNING=$(/bin/launchctl list | /usr/bin/grep -c com.apple.auditd)
if [[ $LAUNCHD_RUNNING == 1 ]] && [[ -e /etc/security/audit_control ]]; then
echo "pass"
else
echo "fail"
fi
```

If the result is not "pass", this is a finding.

**Remediation:**

Configure the macOS system to enable the auditd service with the following command:

```
LAUNCHD_RUNNING=$(/bin/launchctl list | /usr/bin/grep -c com.apple.auditd)
if [[ ! $LAUNCHD_RUNNING == 1 ]]; then
/bin/launchctl load -w /System/Library/LaunchDaemons/com.apple.auditd.plist
fi
if [[ ! -e /etc/security/audit_control ]] && [[ -e /etc/security/audit_control.example ]];then
/bin/cp /etc/security/audit_control.example /etc/security/audit_control
else
/usr/bin/touch /etc/security/audit_control
fi
```

**Additional Information:**

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 b

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53::AU-3

- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 c

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 e

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53::AU-3 (1)
- NIST SP 800-53A::AU-3 (1).1 (ii)
- NIST SP 800-53 Revision 4::AU-3 (1)
- NIST SP 800-53 Revision 5::AU-3 (1)

CCI-000159 Use internal system clocks to generate time stamps for audit records.

- NIST SP 800-53::AU-8
- NIST SP 800-53A::AU-8.1
- NIST SP 800-53 Revision 4::AU-8 a
- NIST SP 800-53 Revision 5::AU-8 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53::AU-14 (1)
- NIST SP 800-53A::AU-14 (1).1
- NIST SP 800-53 Revision 4::AU-14 (1)
- NIST SP 800-53 Revision 5::AU-14 (1)

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 f

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4::AU-12 (3)
- NIST SP 800-53 Revision 5::AU-12 (3)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-004188 Monitor the use of maintenance tools that execute with increased privilege.

- NIST SP 800-53 Revision 5::MA-3 (5)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

## 1.35 APPL-14-001010 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure system to shut down upon audit failure.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259455<br>RULE ID: SV-259455r1038966 |
|--------------------------------------------------|

### Rationale:

The audit service must be configured to shut down the computer if it is unable to audit system events.

Once audit failure occurs, user and system activity are no longer recorded, and malicious activity could go undetected. Audit processing failures can occur due to software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

- (i) If the failure was caused by the lack of audit record storage capacity, the operating system must continue generating audit records if possible (automatically restarting the audit service if necessary), overwriting the oldest audit records in a first-in-first-out manner.
- (ii) If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

### Audit:

Verify the macOS system is configured to shut down upon audit failure with the following command:

```
/usr/bin/awk -F':' '/^policy/ {print $NF}' /etc/security/audit_control | /usr/bin/tr ',' '\n' |  
/usr/bin/grep -Ec 'ahlt'
```

If the result is not "1", this is a finding.

**Remediation:**

Configure the macOS system to shut down upon audit failure with the following command:

```
/usr/bin/sed -i.bak 's/^policy.*/policy: ahlT,argv/' /etc/security/audit_control; /usr/sbin/audit -S
```

**Additional Information:**

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53::AU-5 b
- NIST SP 800-53A::AU-5.1 (iv)
- NIST SP 800-53 Revision 4::AU-5 b
- NIST SP 800-53 Revision 5::AU-5 b

## 1.36 APPL-14-001012 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit log files to be owned by root.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259456<br>RULE ID: SV-259456r958434 |
|-------------------------------------------------|

### Rationale:

Audit log files must be owned by root.

The audit service must be configured to create log files with the correct ownership to prevent normal users from reading audit logs.

Audit logs contain sensitive data about the system and users. If log files are set to only be readable and writable by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured with audit log files owned by root with the following command:

```
/bin/ls -n $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') |  
/usr/bin/awk '{s+=$3} END {print s}'
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with audit log files owned by root with the following command:

```
/usr/sbin/chown -R root /var/audit/*
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.37 APPL-14-001013 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit log folders to be owned by root.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259457<br>RULE ID: SV-259457r958434 |
|-------------------------------------------------|

### Rationale:

Audit log folders must be owned by root.

The audit service must be configured to create log folders with the correct ownership to prevent normal users from reading audit logs.

Audit logs contain sensitive data about the system and users. If log folders are set to only be readable and writable by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured with audit log folders owned by root with the following command:

```
/bin/ls -dn $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') |  
/usr/bin/awk '{print $3}'
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with audit log folders owned by root with the following command:

```
/usr/sbin/chown root /var/audit
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.38 APPL-14-001014 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit log files group to wheel.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259458<br>RULE ID: SV-259458r958434 |
|-------------------------------------------------|

### Rationale:

Audit log files must have the group set to wheel.

The audit service must be configured to create log files with the correct group ownership to prevent normal users from reading audit logs.

Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured with audit log files group-owned by wheel with the following command:

```
/bin/ls -n $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') |  
/usr/bin/awk '{s+=$4} END {print s}'
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with audit log files group-owned by wheel with the following command:

```
/usr/bin/chgrp -R wheel /var/audit/*
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.39 APPL-14-001015 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit log folders group to wheel.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259459<br>RULE ID: SV-259459r958434 |
|-------------------------------------------------|

### Rationale:

Audit log folders must have the group set to wheel.

The audit service must be configured to create log files with the correct group ownership to prevent normal users from reading audit logs.

Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured with audit log folders group-owned by wheel with the following command:

```
/bin/ls -dn $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') |  
/usr/bin/awk '{print $4}'
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with audit log folders group-owned by wheel with the following command:

```
/usr/bin/chgrp wheel /var/audit
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.40 APPL-14-001016 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit log files to mode 440 or less permissive.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259460<br>RULE ID: SV-259460r958434 |
|-------------------------------------------------|

### Rationale:

The audit service must be configured to create log files that are readable only by the root user and group wheel. To achieve this, audit log files must be configured to mode 440 or less permissive; thereby preventing normal users from reading, modifying, or deleting audit logs.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured with audit log files set to mode 440 or less with the following command:

```
/bin/ls -l $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}') |  
/usr/bin/awk '!/-r--r-----|current|total/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with audit log files set to mode 440 with the following command:

```
/bin/chmod 440 /var/audit/*
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.41 APPL-14-001017 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit log folders to mode 700 or less permissive.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259461<br>RULE ID: SV-259461r958434 |
|-------------------------------------------------|

### Rationale:

The audit log folder must be configured to mode 700 or less permissive so that only the root user is able to read, write, and execute changes to folders.

Because audit logs contain sensitive data about the system and users, the audit service must be configured to mode 700 or less permissive; thereby preventing normal users from reading, modifying, or deleting audit logs.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured with audit log folders set to mode 700 or less permissive with the following command:

```
/usr/bin/stat -f %A $(/usr/bin/grep '^dir' /etc/security/audit_control | /usr/bin/awk -F: '{print $2}')
```

If the result is not a mode of 700 or less permissive, this is a finding.

### Remediation:

Configure the macOS system with audit log folders set to mode 700 with the following command:

```
/bin/chmod 700 /var/audit
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.42 APPL-14-001020 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must be configured to audit all deletions of object attributes.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259462<br>RULE ID: SV-259462r1009585 |
|--------------------------------------------------|

### Rationale:

The audit system must be configured to record enforcement actions of attempts to delete file attributes (fd).

\*\*\*Enforcement actions are the methods or mechanisms used to prevent unauthorized changes to configuration settings. One common and effective enforcement action method is using access restrictions (i.e., denying modifications to a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions prevent attempts to delete a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000064-GPOS-00033,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099,SRG-OS-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000463-GPOS-00207,SRG-OS-000465-GPOS-00209,SRG-OS-000466-GPOS-00210,SRG-OS-000467-GPOS-00211,SRG-OS-000468-GPOS-00212

### Audit:

Verify the macOS system is configured to audit all deletions of object attributes with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF } /etc/security/audit_control | /usr/bin/tr ' ' '\n' | /usr/bin/grep -Ec '-fd'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to audit all deletions of object attributes with the following command:

```
/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
```

**Additional Information:**

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

## 1.43 APPL-14-001021 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must be configured to audit all changes of object attributes.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259463<br>RULE ID: SV-259463r1009586 |
|--------------------------------------------------|

### Rationale:

The audit system must be configured to record enforcement actions of attempts to modify file attributes (fm).

Enforcement actions are the methods or mechanisms used to prevent unauthorized changes to configuration settings. One common and effective enforcement action method is using access restrictions (i.e., modifications to a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions attempts to modify a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000064-GPOS-00033,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099,SRG-OS-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000462-GPOS-00206,SRG-OS-000463-GPOS-00207,SRG-OS-000465-GPOS-00209,SRG-OS-000466-GPOS-00210,SRG-OS-000467-GPOS-00211,SRG-OS-000468-GPOS-00212

### Audit:

Verify the macOS system is configured to audit all changes of object attributes with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF } /etc/security/audit_control | /usr/bin/tr ' ' '\n' | /usr/bin/grep -Ec '^fm'
```

If the result is not "1", this is a finding.

**Remediation:**

Configure the macOS system to audit all changes of object attributes with the following command:

```
/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
```

**Additional Information:**

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

## 1.44 APPL-14-001022 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must be configured to audit all failed read actions on the system.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259464<br>RULE ID: SV-259464r991573 |
|-------------------------------------------------|

### Rationale:

The audit system must be configured to record enforcement actions of access restrictions, including failed file read (-fr) attempts.

Enforcement actions are the methods or mechanisms used to prevent unauthorized access and/or changes to configuration settings. One common and effective enforcement action method is using access restrictions (e.g., denying access to a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions prevent attempts to read a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000463-GPOS-00207,SRG-OS-000057-GPOS-00027,SRG-OS-000465-GPOS-00209,SRG-OS-000474-GPOS-00219

### Audit:

Verify the macOS system is configured to audit all failed read actions on the system with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ' ' '\n' |  
/usr/bin/grep -Ec '-fr'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to audit all failed read actions on the system with the following command:

```
/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
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

## 1.45 APPL-14-001023 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must be configured to audit all failed write actions on the system.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259465<br>RULE ID: SV-259465r991573 |
|-------------------------------------------------|

### Rationale:

The audit system must be configured to record enforcement actions of access restrictions, including failed file write (-fw) attempts.

Enforcement actions are the methods or mechanisms used to prevent unauthorized access and/or changes to configuration settings. One common and effective enforcement action method is using access restrictions (e.g., denying users access to edit a file by applying file permissions).

This configuration ensures that audit lists include events in which enforcement actions prevent attempts to change a file.

Without auditing the enforcement of access restrictions, it is difficult to identify attempted attacks, as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000463-GPOS-00207,SRG-OS-000057-GPOS-00027,SRG-OS-000465-GPOS-00209,SRG-OS-000466-GPOS-00210,SRG-OS-000467-GPOS-00211,SRG-OS-000468-GPOS-00212

### Audit:

Verify the macOS system is configured to audit all failed write actions on the system with the following command:

```
/usr/bin/awk -F':' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ',' '\n' | /usr/bin/grep -Ec '-fw'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to audit all failed write actions on the system with the following command:

```
/usr/bin/grep -qE "^\s*-fw" /etc/security/audit_control || /usr/bin/sed -i.bak '/^flags/s/$/, -fw/' /etc/security/audit_control;/usr/sbin/audit -s
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

## 1.46 APPL-14-001024 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must be configured to audit all failed program execution on the system.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259466<br>RULE ID: SV-259466r1009587 |
|--------------------------------------------------|

### Rationale:

The audit system must be configured to record enforcement actions of access restrictions, including failed program execute (-ex) attempts.

Enforcement actions are the methods or mechanisms used to prevent unauthorized access and/or changes to configuration settings. One common and effective enforcement action method is using program execution restrictions (e.g., denying users access to execute certain processes).

This configuration ensures that audit lists include events in which program execution has failed.

Without auditing the enforcement of program execution, it is difficult to identify attempted attacks as there is no audit trail available for forensic investigation.

Satisfies: SRG-OS-000463-GPOS-00207,SRG-OS-000365-GPOS-00152,SRG-OS-000458-GPOS-00203,SRG-OS-000465-GPOS-00209

### Audit:

Verify the macOS system is configured to audit all failed program execution on the system with the following command:

```
/usr/bin/awk -F':' '/^flags/ { print $NF }' /etc/security/audit_control | /usr/bin/tr ',' '\n' | /usr/bin/grep -Ec '-ex'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to audit all failed program execution on the system with the following command:

```
/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
```

**Additional Information:**

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

## 1.47 APPL-14-001029 (Manual)

### Profile Applicability:

- SEVERITY: CAT III

### Description:

The macOS system must configure audit retention to seven days.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259467<br>RULE ID: SV-259467r958752 |
|-------------------------------------------------|

### Rationale:

The audit service must be configured to require records be kept for an organizational defined value before deletion, unless the system uses a central audit record storage facility.

When "expire-after" is set to "7d", the audit service will not delete audit logs until the log data criteria is met.

### Audit:

Verify the macOS system is configured audit retention to seven days with the following command:

```
/usr/bin/awk -F: 'expire-after/{print $2}' /etc/security/audit_control
```

If the result is not "7d", this is a finding.

### Remediation:

Configure the macOS system to set audit retention to seven days with the following command:

```
/usr/bin/sed -i.bak 's/^expire-after.*/expire-after:7d/' /etc/security/audit_control;  
/usr/sbin/audit -s
```

### Additional Information:

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4::AU-4
- NIST SP 800-53 Revision 5::AU-4

## 1.48 APPL-14-001030 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit capacity warning.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259468<br>RULE ID: SV-259468r958424 |
|-------------------------------------------------|

### Rationale:

The audit service must be configured to notify the system administrator when the amount of free disk space remaining reaches an organization defined value.

This rule ensures that the system administrator is notified in advance that action is required to free up more disk space for audit logs.

Satisfies: SRG-OS-000046-GPOS-00022,SRG-OS-000343-GPOS-00134

### Audit:

Verify the macOS system is configured to require a minimum of 25 percent free disk space for audit record storage with the following command:

```
/usr/bin/awk -F: '/^minfree/{print $2}' /etc/security/audit_control
```

If the result is not "25", this is a finding.

### Remediation:

Configure the macOS system to require a minimum of 25 percent free disk space for audit record storage with the following command:

```
/usr/bin/sed -i.bak 's/.minfree./minfree:25/' /etc/security/audit_control; /usr/sbin/audit -s
```

### Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4::AU-5 (1)
- NIST SP 800-53 Revision 5::AU-5 (1)

## 1.49 APPL-14-001031 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit failure notification.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259469<br>RULE ID: SV-259469r1038966 |
|--------------------------------------------------|

### Rationale:

The audit service must be configured to immediately print messages to the console or email administrator users when an auditing failure occurs.

It is critical for the appropriate personnel to be made aware immediately if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of a potentially harmful failure in the auditing system's capability, and system operation may be adversely affected.

Satisfies: SRG-OS-000047-GPOS-00023,SRG-OS-000344-GPOS-00135

### Audit:

Verify the macOS system is configured to produce audit failure notification with the following command:

```
/usr/bin/grep -c "logger -s -p" /etc/security/audit_warn
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to produce audit failure notification with the following command:

```
/usr/bin/sed -i.bak 's/logger -p/logger -s -p/' /etc/security/audit_warn; /usr/sbin/audit -s
```

### Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53::AU-5 b
- NIST SP 800-53A::AU-5.1 (iv)
- NIST SP 800-53 Revision 4::AU-5 b
- NIST SP 800-53 Revision 5::AU-5 b

CCI-001858 Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

- NIST SP 800-53 Revision 4::AU-5 (2)
- NIST SP 800-53 Revision 5::AU-5 (2)

## 1.50 APPL-14-001044 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure the system to audit all authorization and authentication events.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259470<br>RULE ID: SV-259470r1009588 |
|--------------------------------------------------|

### Rationale:

The auditing system must be configured to flag authorization and authentication (aa) events.

Authentication events contain information about the identity of a user, server, or client. Authorization events contain information about permissions, rights, and rules. If audit records do not include aa events, it is difficult to identify incidents and to correlate incidents to subsequent events.

Audit records can be generated from various components within the information system (e.g., via a module or policy filter).

Satisfies: SRG-OS-000365-GPOS-00152,SRG-OS-000392-GPOS-00172,SRG-OS-000458-GPOS-00203,SRG-OS-000463-GPOS-00207,SRG-OS-000465-GPOS-00209,SRG-OS-000466-GPOS-00210,SRG-OS-000467-GPOS-00211,SRG-OS-000468-GPOS-00212,SRG-OS-000471-GPOS-00215,SRG-OS-000471-GPOS-00216,SRG-OS-000475-GPOS-00220,SRG-OS-000477-GPOS-00222

### Audit:

Verify the macOS system is configured to audit logon events with the following command:

```
/usr/bin/awk -F:' ' /^flags/ { print $NF } /etc/security/audit_control | /usr/bin/tr ' ' '\n' |  
/usr/bin/grep -Ec 'aa'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to audit logon events with the following command:

```
/usr/bin/grep -qE "^flags.*[^-]aa" /etc/security/audit_control || /usr/bin/sed -i.bak /^flags/  
s/$/,aa/ /etc/security/audit_control; /usr/sbin/audit -s
```

**Additional Information:**

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4::MA-4 (1) (a)
- NIST SP 800-53 Revision 5::MA-4 (1) (a)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4::CM-5 (1)

## 1.51 APPL-14-001060 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must set smart card certificate trust to moderate.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259471<br>RULE ID: SV-259471r1009589 |
|--------------------------------------------------|

### Rationale:

The macOS system must be configured to block access to users who are no longer authorized (i.e., users with revoked certificates).

To prevent the use of untrusted certificates, the certificates on a smart card must meet the following criteria: its issuer has a system-trusted certificate, the certificate is not expired, its "valid-after" date is in the past, and it passes Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) checking.

By setting the smart card certificate trust level to moderate, the system will execute a soft revocation, i.e., if the OCSP/CRL server is unreachable, authentication will still succeed.

Note: Before applying this setting, refer to the smart card supplemental guidance.

Satisfies: SRG-OS-000066-GPOS-00034,SRG-OS-000377-GPOS-00162,SRG-OS-000384-GPOS-00167,SRG-OS-000403-GPOS-00182

### Audit:

Verify the macOS system is configured to check the revocation status of user certificates with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')
```

```
.objectForKey('checkCertificateTrust').js  
EOS
```

If the result is not "2", this is a finding.

### Remediation:

Configure the macOS system to check the revocation status of user certificates by installing the "com.apple.security.smartcard" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

**Additional Information:**

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

CCI-001954 Electronically verify Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

- NIST SP 800-53 Revision 5::IA-5 (2) (b) (2)

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

CCI-001991 The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

- NIST SP 800-53 Revision 4::IA-5 (2) (d)

## 1.52 APPL-14-001100 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable root logon for SSH.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259472<br>RULE ID: SV-259472r1009590 |
|--------------------------------------------------|

### Rationale:

If SSH is enabled to ensure individual accountability and prevent unauthorized access, logging in as root via SSH must be disabled.

The macOS system must require individuals to be authenticated with an individual authenticator prior to using a group authenticator, and administrator users must never log in directly as root.

Note: /etc/ssh/sshd\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000109-GPOS-00056,SRG-OS-000364-GPOS-00151

### Audit:

Verify the macOS system is configured to disable root login for SSH with the following command:

```
/usr/sbin/sshd -G | /usr/bin/awk '/permitrootlogin/{print $2}'
```

If the result is not "no", this is a finding.

## Remediation:

Configure the macOS system to disable root login for SSH with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d '\n')
if [[ -z $include_dir ]]; then
/usr/bin/sed -i.bk "1s/.*/Include /etc/ssh/sshd_config.d/*/ /etc/ssh/sshd_config
fi
/usr/bin/grep -qxF 'permitrootlogin no' "${include_dir}01-mscp-sshd.conf" 2>/dev/null ||
echo "permitrootlogin no" >> "${include_dir}01-mscp-sshd.conf"
for file in $(ls ${include_dir}); do
if [[ "$file" == "100-macos.conf" ]]; then
continue
fi
if [[ "$file" == "01-mscp-sshd.conf" ]]; then
break
fi
/bin/mv ${include_dir}${file} ${include_dir}20-${file}
done
```

## Additional Information:

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5::IA-2 (5)

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

- NIST SP 800-53::IA-2 (5) (b)
- NIST SP 800-53A::IA-2 (5).2 (ii)
- NIST SP 800-53 Revision 4::IA-2 (5)

## 1.53 APPL-14-001110 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit\_control group to wheel.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259473<br>RULE ID: SV-259473r958434 |
|-------------------------------------------------|

### Rationale:

/etc/security/audit\_control must have the group set to wheel.

The audit service must be configured with the correct group ownership to prevent normal users from manipulation audit log configurations.

Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000063-GPOS-00032,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured with the audit\_control group to wheel with the following command:

```
/bin/ls -dn /etc/security/audit_control | /usr/bin/awk '{print $4}'
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with the audit\_control group to wheel with the following command:

```
/usr/bin/chgrp wheel /etc/security/audit_control
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.54 APPL-14-001120 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit\_control owner to root.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259474<br>RULE ID: SV-259474r958434 |
|-------------------------------------------------|

### Rationale:

/etc/security/audit\_control must have the owner set to root.

The audit service must be configured with the correct ownership to prevent normal users from manipulation audit log configurations.

Audit logs contain sensitive data about the system and users. If log files are set to be readable and writable only by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000063-GPOS-00032,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured with the audit\_control owner to root with the following command:

```
/bin/ls -dn /etc/security/audit_control | /usr/bin/awk '{print $3}'
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with the audit\_control owner to root with the following command:

```
/usr/sbin/chown root /etc/security/audit_control
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.55 APPL-14-001130 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit\_control to mode 440 or less permissive.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259475<br>RULE ID: SV-259475r958434 |
|-------------------------------------------------|

### Rationale:

/etc/security/audit\_control must be configured so that it is readable only by the root user and group wheel.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000063-GPOS-00032,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured audit\_control to mode 440 or less with the following command:

```
/bin/ls -l /etc/security/audit_control | /usr/bin/awk '!/-r--[r-]-----|current|total/{print $1}' |  
/usr/bin/wc -l | /usr/bin/xargs
```

If the results are not "0", this is a finding.

### Remediation:

Configure the macOS system with the audit\_control to mode 440 with the following command:

```
/bin/chmod 440 /etc/security/audit_control
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1

- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.56 APPL-14-001140 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure audit\_control to not contain access control lists.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259476<br>RULE ID: SV-259476r958434 |
|-------------------------------------------------|

### Rationale:

/etc/security/audit\_control must not contain Access Control Lists (ACLs).

/etc/security/audit\_control contains sensitive configuration data about the audit service. This rule ensures that the audit service is configured to be readable and writable only by system administrators in order to prevent normal users from manipulating audit logs.

Satisfies: SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000063-GPOS-00032,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099

### Audit:

Verify the macOS system is configured without ACLs applied to audit\_control with the following command:

```
/bin/ls -le /etc/security/audit_control | /usr/bin/awk '{print $1}' | /usr/bin/grep -c ":",
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system without ACLs applied to audit\_control with the following command:

```
/bin/chmod -N /etc/security/audit_control
```

### Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9

- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53::AU-12 b
- NIST SP 800-53A::AU-12.1 (iii)
- NIST SP 800-53 Revision 4::AU-12 b
- NIST SP 800-53 Revision 5::AU-12 b

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## 1.57 APPL-14-002001 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Server Message Block sharing.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259478<br>RULE ID: SV-259478r958472 |
|-------------------------------------------------|

### Rationale:

Support for Server Message Block (SMB) file sharing is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities.

### Audit:

Verify the macOS system is configured to disable Server Message Block sharing with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.smbd" => disabled'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable Server Message Block sharing with the following command:

```
/bin/launchctl disable system/com.apple.smbd
```

The system may need to be restarted for the update to take effect.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

## 1.58 APPL-14-002003 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Network File System service.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259479<br>RULE ID: SV-259479r958472 |
|-------------------------------------------------|

### Rationale:

Support for Network File Systems (NFS) services is nonessential and, therefore, must be disabled.

### Audit:

Verify the macOS system is configured to disable network file system service with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.nfsd" => disabled'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable network file system service with the following command:

```
/bin/launchctl disable system/com.apple.nfsd
```

The system may need to be restarted for the update to take effect.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

## 1.59 APPL-14-001150 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must disable password authentication for SSH.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259477<br>RULE ID: SV-259477r1009591 |
|--------------------------------------------------|

### Rationale:

If remote logon through SSH is enabled, password-based authentication must be disabled for user logon.

All users must go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.

Note: /etc/ssh/sshd\_config will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000067-GPOS-00035,SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057,SRG-OS-000125-GPOS-00065,SRG-OS-000375-GPOS-00160

### Audit:

Verify the macOS system is configured to disable password authentication for SSH with the following command:

```
/usr/sbin/sshd -G | /usr/bin/grep -Ec
```

```
'^(passwordauthentication\s+no|kbdinteractiveauthentication\s+no)'
```

If the result is not "2", this is a finding.

## Remediation:

Configure the macOS system to disable password authentication for SSH with the following command:

```
include_dir=$(/usr/bin/awk '/^Include/ {print $2}' /etc/ssh/sshd_config | /usr/bin/tr -d ' ')\nif [[ -z $include_dir ]]; then\n  /usr/bin/sed -i.bk "1s/.Include /etc/ssh/sshd_config.d/*/ /etc/ssh/sshd_config\nfi\n  echo "passwordauthentication no" >> "${include_dir}01-mscp-sshd.conf"\n  echo "kbdinteractiveauthentication no" >> "${include_dir}01-mscp-sshd.conf"\n  for file in $(ls ${include_dir}); do\n    if [[ "$file" == "100-macos.conf" ]]; then\n      continue\n    fi\n    if [[ "$file" == "01-mscp-sshd.conf" ]]; then\n      break\n    fi\n  /bin/mv ${include_dir}${file} ${include_dir}20-${file}\ndone
```

## Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53::MA-4 c
- NIST SP 800-53A::MA-4.1 (iv)
- NIST SP 800-53 Revision 4::MA-4 c
- NIST SP 800-53 Revision 5::MA-4 c

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5::IA-2 (6) (a)

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1
- NIST SP 800-53 Revision 4::IA-2 (3)

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53::IA-2 (4)
- NIST SP 800-53A::IA-2 (4).1
- NIST SP 800-53 Revision 4::IA-2 (4)

CCI-001948 The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 4::IA-2 (11)

## 1.60 APPL-14-002004 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Location Services.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259480<br>RULE ID: SV-259480r958478 |
|-------------------------------------------------|

### Rationale:

The information system must be configured to provide only essential capabilities. Disabling Location Services helps prevent the unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling.

### Audit:

Verify the macOS system is configured to disable Location Services with the following command:

```
/usr/bin/sudo -u _locationd /usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.locationd')
```

```
.objectForKey('LocationServicesEnabled').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable Location Services with the following command:

```
/usr/bin/defaults write /var/db/locationd/Library/Preferences/ByHost/com.apple.locationd  
LocationServicesEnabled -bool false; /bin/launchctl kickstart -k  
system/com.apple.locationd
```

The system may need to be restarted for the update to take effect.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.61 APPL-14-002005 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Bonjour multicast.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259481<br>RULE ID: SV-259481r958478 |
|-------------------------------------------------|

### Rationale:

Bonjour multicast advertising must be disabled to prevent the system from broadcasting its presence and available services over network interfaces.

### Audit:

Verify the macOS system is configured to disable Bonjour multicast with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.mDNSResponder')
```

```
.objectForKey('NoMulticastAdvertisements').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable Bonjour multicast by installing the "com.apple.mDNSResponder" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.62 APPL-14-002006 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Unix-to-Unix Copy Protocol service.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259482<br>RULE ID: SV-259482r958472 |
|-------------------------------------------------|

### Rationale:

The system must not have the Unix-to-Unix Copy Protocol (UUCP) service active.

UUCP, a set of programs that enable the sending of files between different Unix systems as well as sending commands to be executed on another system, is not essential and must be disabled in order to prevent the unauthorized connection of devices, transfer of information, and tunneling.

Note: UUCP service is disabled at startup by default macOS.

### Audit:

Verify the macOS system is configured to disable Unix-to-Unix copy protocol service with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.uucp" => disabled'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable Unix-to-Unix copy protocol service with the following command:

```
/bin/launchctl disable system/com.apple.uucp
```

The system may need to be restarted for the update to take effect.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

## 1.63 APPL-14-002007 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Internet Sharing.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259483<br>RULE ID: SV-259483r958478 |
|-------------------------------------------------|

### Rationale:

If the system does not require Internet Sharing, support for it is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Disabling Internet sharing helps prevent the unauthorized connection of devices, unauthorized transfer of information, and unauthorized tunneling.

### Audit:

Verify the macOS system is configured to disable Internet Sharing with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')
```

```
.objectForKey('forceInternetSharingOff').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable Internet Sharing by installing the "com.apple.MCX" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.64 APPL-14-002008 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable the built-in web server.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259484<br>RULE ID: SV-259484r958472 |
|-------------------------------------------------|

### Rationale:

The built-in web server is a nonessential service built into macOS and must be disabled.

Note: The built in web server service is disabled at startup by default macOS.

### Audit:

Verify the macOS system is configured to disable the built-in web server with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "org.apache.httpd" => disabled'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable the built-in web server with the following command:

```
/bin/launchctl disable system/org.apache.httpd
```

The system may need to be restarted for the update to take effect.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

## 1.65 APPL-14-002009 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable AirDrop.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259485<br>RULE ID: SV-259485r958472 |
|-------------------------------------------------|

### Rationale:

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.

Satisfies: SRG-OS-000080-GPOS-00048,SRG-OS-000095-GPOS-00049,SRG-OS-000300-GPOS-00118

### Audit:

Verify the macOS system is configured to disable AirDrop with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowAirDrop').js
```

```
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable AirDrop by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

## 1.66 APPL-14-002010 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable FaceTime.app.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259486<br>RULE ID: SV-259486r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in FaceTime.app must be disabled.

The FaceTime.app establishes a connection to Apple's iCloud service, even when security controls have been put in place to disable iCloud access.

## [IMPORTANT]

Apple has deprecated the use of application restriction controls (<https://github.com/apple/device-management/blob/eb51fb0cb9626cac4717858556912c257a734ce0/mdm/profiles/com.apple.applicationaccess.new.yaml#L67-L70>). Using these controls may not work as expected. Third-party software may be required to fulfill the compliance requirements.

### Audit:

Verify the macOS system is configured to disable FaceTime.app with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new'))
```

```
.objectForKey('familyControlsEnabled'))
let pathlist =
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new')
```

```
.objectForKey('pathBlackList').js
for ( let app in pathlist ) {
if ( ObjC.unwrap(pathlist[app]) == "/Applications/FaceTime.app" && pref1 == true ){
return("true")
}
}
return("false")
}
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable FaceTime.app by installing the "com.apple.applicationaccess.new" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.67 APPL-14-002012 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable the iCloud Calendar services.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259487<br>RULE ID: SV-259487r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in Calendar.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated calendar synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud Calendar services with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudCalendar').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Calendar services by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.68 APPL-14-002013 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Reminders.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259488<br>RULE ID: SV-259488r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in Reminders.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated reminders synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud Reminders with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudReminders').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Reminders by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.69 APPL-14-002014 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Address Book.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259489<br>RULE ID: SV-259489r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in Contacts.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data, and, therefore, automated contact synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud Address Book with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudAddressBook').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Address Book by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.70 APPL-14-002015 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Mail.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259490<br>RULE ID: SV-259490r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in Mail.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated mail synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud Mail with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudMail').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Mail by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.71 APPL-14-002016 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Notes.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259491<br>RULE ID: SV-259491r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in Notes.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated Notes synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud Notes with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudNotes').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Notes by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.72 APPL-14-002017 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable the camera.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259492<br>RULE ID: SV-259492r1009529 |
|--------------------------------------------------|

### Rationale:

macOS must be configured to disable the camera.

### Audit:

If the device or operating system does not have a camera installed, this requirement is not applicable.

This requirement is not applicable to mobile devices (smartphones and tablets), where the use of the camera is a local authorizing official (AO) decision.

This requirement is not applicable to dedicated VTC suites located in approved VTC locations that are centrally managed.

For an external camera, if there is not a method for the operator to manually disconnect camera at the end of collaborative computing sessions, this is a finding.

For a built-in camera, the camera must be protected by a camera cover (e.g., laptop camera cover slide) when not in use. If the built-in camera is not protected with a camera cover, or is not physically disabled, this is a finding.

If the camera is not disconnected, covered, or physically disabled, verify the macOS system is configured to disable the camera with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCamera').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable the camera by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.73 APPL-14-002020 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Siri.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259493<br>RULE ID: SV-259493r958478 |
|-------------------------------------------------|

### Rationale:

Support for Siri is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities.

### Audit:

Verify the macOS system is configured to disable Siri with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowAssistant').js
```

```
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable Siri by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.74 APPL-14-002021 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable sending diagnostic and usage data to Apple.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259494<br>RULE ID: SV-259494r958564 |
|-------------------------------------------------|

### Rationale:

The ability to submit diagnostic data to Apple must be disabled.

The information system must be configured to provide only essential capabilities. Disabling the submission of diagnostic and usage information will mitigate the risk of unwanted data being sent to Apple.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

### Audit:

Verify the macOS system is configured to disable sending diagnostic and usage data to Apple with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
function run() {  
let pref1 = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.SubmitDiagInfo')  
  
.objectForKey('AutoSubmit').js  
let pref2 = $.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowDiagnosticSubmission').js  
if ( pref1 == false && pref2 == false ){  
return("true")  
} else {  
return("false")  
}  
}  
}
```

```
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable sending diagnostic and usage data to Apple by installing the "com.apple.applicationaccess" configuration profile.

**Additional Information:**

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

## 1.75 APPL-14-002022 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Remote Apple Events.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259495<br>RULE ID: SV-259495r958472 |
|-------------------------------------------------|

### Rationale:

If the system does not require Remote Apple Events, support for Apple Remote Events is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Disabling Remote Apple Events helps prevent the unauthorized connection of devices, the unauthorized transfer of information, and unauthorized tunneling.

Satisfies: SRG-OS-000080-GPOS-00048,SRG-OS-000096-GPOS-00050

### Audit:

Verify the macOS system is configured to disable Remote Apple Events with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c '"com.apple.AEServer" => disabled'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable Remote Apple Events with the following commands:

```
/usr/sbin/systemsetup -setremoteappleevents off  
/bin/launchctl disable system/com.apple.AEServer
```

Note: Systemsetup with -setremoteappleevents flag will fail unless Full Disk Access to systemsetup or its parent process is granted. This requires supervision.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

## 1.76 APPL-14-002035 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Apple ID setup during Setup Assistant.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259496<br>RULE ID: SV-259496r958478 |
|-------------------------------------------------|

### Rationale:

The prompt for Apple ID setup during Setup Assistant must be disabled.

macOS will automatically prompt new users to set up an Apple ID while they are going through Setup Assistant if this is not disabled, misleading new users to think they need to create Apple ID accounts upon their first log on.

### Audit:

Verify the macOS system is configured to disable Apple ID setup during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')
```

```
.objectForKey('SkipCloudSetup').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable Apple ID setup during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.77 APPL-14-002036 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Privacy Setup services during Setup Assistant.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259497<br>RULE ID: SV-259497r958478 |
|-------------------------------------------------|

### Rationale:

The prompt for Privacy Setup services during Setup Assistant must be disabled.

Organizations must apply organizationwide configuration settings. The macOS Privacy Setup services prompt guides new users through enabling their own specific privacy settings; this is not essential and, therefore, must be disabled to prevent against the risk of individuals electing privacy settings with the potential to override organizationwide settings.

### Audit:

Verify the macOS system is configured to disable Privacy Setup services during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')
```

```
.objectForKey('SkipPrivacySetup').js
```

```
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable Privacy Setup services during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.78 APPL-14-002037 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Storage Setup during Setup Assistant.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259498<br>RULE ID: SV-259498r958478 |
|-------------------------------------------------|

### Rationale:

The prompt to set up iCloud storage services during Setup Assistant must be disabled.

The default behavior of macOS is to prompt new users to set up storage in iCloud. Disabling the iCloud storage setup prompt provides organizations more control over the storage of their data.

### Audit:

Verify the macOS system is configured to disable iCloud Storage Setup during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')
```

```
.objectForKey('SkipiCloudStorageSetup').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Storage Setup during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.79 APPL-14-002038 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must disable Trivial File Transfer Protocol service.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259499<br>RULE ID: SV-259499r987796 |
|-------------------------------------------------|

### Rationale:

If the system does not require Trivial File Transfer Protocol (TFTP), support it is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Disabling TFTP helps prevent the unauthorized connection of devices and the unauthorized transfer of information.

Note: TFTP service is disabled at startup by default macOS.

Satisfies: SRG-OS-000074-GPOS-00042,SRG-OS-000080-GPOS-00048

### Audit:

Verify the macOS system is configured to disable trivial file transfer protocol service with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.tftpd" => disabled'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable trivial file transfer protocol service with the following command:

```
/bin/launchctl disable system/com.apple.tftpd
```

The system may need to be restarted for the update to take effect.

### Additional Information:

CCI-000197 For password-based authentication, transmit passwords only over cryptographically-protected channels.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)
- NIST SP 800-53 Revision 5::IA-5 (1) (c)

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

## 1.80 APPL-14-002039 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Siri Setup during Setup Assistant.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259500<br>RULE ID: SV-259500r958478 |
|-------------------------------------------------|

### Rationale:

The prompt for Siri during Setup Assistant must be disabled.

Organizations must apply organizationwide configuration settings. The macOS Siri Assistant Setup prompt guides new users through enabling their own specific Siri settings; this is not essential and, therefore, must be disabled to prevent against the risk of individuals electing Siri settings with the potential to override organizationwide settings.

### Audit:

Verify the macOS system is configured to disable Siri Setup during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')
```

```
.objectForKey('SkipSiriSetup').js
```

```
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable Siri Setup during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.81 APPL-14-002040 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Keychain synchronization.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259501<br>RULE ID: SV-259501r958478 |
|-------------------------------------------------|

### Rationale:

The macOS system's ability to automatically synchronize a user's passwords to their iCloud account must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, password management and synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud Keychain synchronization with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudKeychainSync').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Keychain synchronization by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.82 APPL-14-002041 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Document synchronization.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259502<br>RULE ID: SV-259502r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in iCloud document synchronization service must be disabled to prevent organizational data from being synchronized to personal or nonapproved storage.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated document synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud Document synchronization with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudDocumentSync').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Document synchronization by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.83 APPL-14-002042 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Bookmarks.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259503<br>RULE ID: SV-259503r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in Safari.app bookmark synchronization via the iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated bookmark synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud Bookmarks with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudBookmarks').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Bookmarks by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.84 APPL-14-002043 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Photo Library.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259504<br>RULE ID: SV-259504r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in Photos.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated photo synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable the iCloud Photo Library with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudPhotoLibrary').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable the iCloud Photo Library by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.85 APPL-14-002050 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Screen Sharing and Apple Remote Desktop.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259505<br>RULE ID: SV-259505r958472 |
|-------------------------------------------------|

### Rationale:

Support for both Screen Sharing and Apple Remote Desktop (ARD) is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities. Disabling screen sharing and ARD helps prevent the unauthorized connection of devices, the unauthorized transfer of information, and unauthorized tunneling.

### Audit:

Verify the macOS system is configured to disable Screen Sharing and Apple Remote Desktop with the following command:

```
/bin/launchctl print-disabled system | /usr/bin/grep -c "com.apple.screensharing" => disabled'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable Screen Sharing and Apple Remote Desktop with the following command:

```
/bin/launchctl disable system/com.apple.screensharing
```

The system may need to be restarted for the update to take effect.

Note: This will apply to the whole system.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

## 1.86 APPL-14-002051 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable the TouchID System Settings pane.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259506<br>RULE ID: SV-259506r958478 |
|-------------------------------------------------|

### Rationale:

The System Settings pane for TouchID must be disabled.

Disabling the System Settings pane prevents the users from configuring TouchID.

### Audit:

Verify the macOS system is configured to disable the TouchID System Settings pane with the following command:

```
/usr/bin/profiles show -output stdout-xml | /usr/bin/xmllint --xpath  
'//key[text()="DisabledSystemSettings"]/following-sibling::*[1]' - | /usr/bin/grep -c  
"com.apple.Touch-ID-Settings.extension"  
If the result is not "1", this is a finding.
```

### Remediation:

Configure the macOS system to disable the TouchID System Settings pane by installing the "com.apple.systempreferences" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.87 APPL-14-002052 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable the System Settings pane for Wallet and Apple Pay.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259507<br>RULE ID: SV-259507r958478 |
|-------------------------------------------------|

### Rationale:

The System Settings pane for Wallet and Apple Pay must be disabled.

Disabling the System Settings pane prevents the users from configuring Wallet and Apple Pay.

### Audit:

Verify the macOS system is configured to disable the System Settings pane for Wallet and Apple Pay with the following command:

```
/usr/bin/profiles show -output stdout-xml | /usr/bin/xmllint --xpath  
'//key[text()="DisabledSystemSettings"]/following-sibling::*[1]' - | /usr/bin/grep -c  
"com.apple.WalletSettingsExtension"
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable the System Settings pane for Wallet and Apple Pay by installing the "com.apple.systempreferences" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.88 APPL-14-002053 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable the system settings pane for Siri.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259508<br>RULE ID: SV-259508r958478 |
|-------------------------------------------------|

### Rationale:

The System Settings pane for Siri must be hidden.

Hiding the System Settings pane prevents the users from configuring Siri.

### Audit:

Verify the macOS system is configured to disable the system settings pane for Siri with the following command:

```
/usr/bin/profiles show -output stdout-xml | /usr/bin/xmllint --xpath  
'//key[text()="DisabledSystemSettings"]/following-sibling::*[1]' - | /usr/bin/grep -c  
com.apple.Siri-Settings.extension  
If the result is not "1", this is a finding.
```

### Remediation:

Configure the macOS system to disable the system settings pane for Siri by installing the "com.apple.systempreferences" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.89 APPL-14-002060 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must apply gatekeeper settings to block applications from unidentified developers.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259509<br>RULE ID: SV-259509r1009592 |
|--------------------------------------------------|

### Rationale:

The information system implements cryptographic mechanisms to authenticate software prior to installation.

Gatekeeper settings must be configured correctly to only allow the system to run applications downloaded from the Mac App Store or applications signed with a valid Apple Developer ID code. Administrator users will still have the option to override these settings on a per-app basis. Gatekeeper is a security feature that ensures that applications must be digitally signed by an Apple-issued certificate in order to run. Digital signatures allow the macOS to verify that the application has not been modified by a malicious third party.

### Audit:

Verify the macOS system is configured to apply gatekeeper settings to block applications from unidentified developers with the following command:

```
/usr/sbin/spctl --status --verbose | /usr/bin/grep -c "developer id enabled"
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to apply gatekeeper settings to block applications from unidentified developers with the following command:

```
/usr/sbin/spctl --global-enable; /usr/sbin/spctl --enable
```

### Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

## 1.90 APPL-14-002062 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must disable Bluetooth when no approved device is connected.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259510<br>RULE ID: SV-259510r958908 |
|-------------------------------------------------|

### Rationale:

The macOS system must be configured to disable Bluetooth unless an approved device is connected.

## [IMPORTANT]

**Information system security officers (ISSOs) may make the risk-based decision not to disable Bluetooth to maintain necessary functionality, but they are advised to first fully weigh the potential risks posed to their organization.**

Satisfies: SRG-OS-000423-GPOS-00187,SRG-OS-000481-GPOS-00481

### Audit:

Verify the macOS system is configured to disable Bluetooth with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCXBluetooth')
```

```
.objectForKey('DisableBluetooth').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable Bluetooth by installing the "com.apple.MCXBluetooth" configuration profiles.

### Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

## 1.91 APPL-14-002063 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable the guest account.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259511<br>RULE ID: SV-259511r958796 |
|-------------------------------------------------|

### Rationale:

Guest access must be disabled.

Turning off guest access prevents anonymous users from accessing files.

### Audit:

Verify the macOS system is configured to disable the guest account with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
let pref1 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')
    .objectForKey('DisableGuestAccount'))
let pref2 = ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')
    .objectForKey('EnableGuestAccount'))
if ( pref1 == true && pref2 == false ) {
return("true")
} else {
return("false")
}
}
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable the guest account by installing the "com.apple.MCX" configuration profile.

### Additional Information:

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

## 1.92 APPL-14-002064 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must enable Gatekeeper.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259512<br>RULE ID: SV-259512r1009593 |
|--------------------------------------------------|

### Rationale:

Gatekeeper must be enabled.

Gatekeeper is a security feature that ensures applications are digitally signed by an Apple-issued certificate before they are permitted to run. Digital signatures allow the macOS host to verify that the application has not been modified by a malicious third party.

Administrator users will still have the option to override these settings on a case-by-case basis.

### Audit:

Verify the macOS system is configured to enable gatekeeper with the following command:

```
/usr/sbin/spctl --status | /usr/bin/grep -c "assessments enabled"
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to enable gatekeeper with the following command:

```
/usr/sbin/spctl --global-enable
```

### Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 4::CM-5 (3)

## 1.93 APPL-14-002066 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable unattended or automatic log on to the system.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259513<br>RULE ID: SV-259513r991591 |
|-------------------------------------------------|

### Rationale:

Automatic logon must be disabled.

When automatic logons are enabled, the default user account is automatically logged on at boot time without prompting the user for a password. Even if the screen is later locked, a malicious user would be able to reboot the computer and find it already logged in. Disabling automatic logons mitigates this risk.

### Audit:

Verify the macOS system is configured to disable unattended or automatic logon to the system with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')
```

```
.objectForKey('com.apple.login.mcx.DisableAutoLoginClient').js
```

```
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable unattended or automatic logon to the system by installing the "com.apple.loginwindow" configuration profile.

### Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## 1.94 APPL-14-002068 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must secure user's home folders.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259514<br>RULE ID: SV-259514r991592 |
|-------------------------------------------------|

### Rationale:

The system must be configured to prevent access to other user's home folders.

The default behavior of macOS is to allow all valid users access to the top level of every other user's home folder while restricting access only to the Apple default folders within.

### Audit:

Verify the macOS system is configured so that permissions are set correctly on user home directories with the following command:

```
/usr/bin/find /System/Volumes/Data/Users -mindepth 1 -maxdepth 1 -type d ! ( -perm 700 -o -perm 711 ) | /usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest" | /usr/bin/wc -l | /usr/bin/xargs
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system to set the appropriate permissions for each user on the system with the following command:

```
IFS=$'\n'
for userDirs in $( /usr/bin/find /System/Volumes/Data/Users -mindepth 1 -maxdepth 1 -type d ! ( -perm 700 -o -perm 711 ) | /usr/bin/grep -v "Shared" | /usr/bin/grep -v "Guest" ); do
/bin/chmod og-rwx "$userDirs"
done
unset IFS
```

### Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## 1.95 APPL-14-002069 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must require administrator privileges to modify systemwide settings.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259515<br>RULE ID: SV-259515r958726 |
|-------------------------------------------------|

### Rationale:

The system must be configured to require an administrator password in order to modify the systemwide preferences in System Settings.

Some Preference Panes in System Settings contain settings that affect the entire system. Requiring a password to unlock these systemwide settings reduces the risk of a nonauthorized user modifying system configurations.

### Audit:

Verify the macOS system is configured to require administrator privileges to modify systemwide settings with the following command:

```
authDBs=("system.preferences" "system.preferences.energysaver"
"system.preferences.network" "system.preferences.printing"
"system.preferences.sharing" "system.preferences.softwareupdate"
"system.preferences.startupdisk" "system.preferences.timemachine")
result="1"
for section in ${authDBs[@]}; do
if [[ $(/usr/bin/security -q authorizationdb read "$section" | /usr/bin/xmllint -xpath
'name(//*[contains(text(), "shared")]/following-sibling::[1])' -) != "false" ]]; then
result="0"
fi
done
echo $result
If the result is not "1", this is a finding.
```

**Remediation:**

Configure the macOS system to require administrator privileges to modify systemwide settings with the following command:

```
authDBs=("system.preferences" "system.preferences.energysaver"
"system.preferences.network" "system.preferences.printing"
"system.preferences.sharing" "system.preferences.softwareupdate"
"system.preferences.startupdisk" "system.preferences.timemachine")
for section in ${authDBs[@]}; do
/usr/bin/security -q authorizationdb read "$section" > "/tmp/$section.plist"
key_value=$(/usr/libexec/PlistBuddy -c "Print :shared" "/tmp/$section.plist" 2>&1)
if [[ "$key_value" == "Does Not Exist" ]]; then
/usr/libexec/PlistBuddy -c "Add :shared bool false" "/tmp/$section.plist"
else
/usr/libexec/PlistBuddy -c "Set :shared false" "/tmp/$section.plist"
fi
/usr/bin/security -q authorizationdb write "$section" < "/tmp/$section.plist"
done
```

**Additional Information:**

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

## 1.96 APPL-14-002080 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Airplay Receiver.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259516<br>RULE ID: SV-259516r958478 |
|-------------------------------------------------|

### Rationale:

Airplay Receiver allows users to send content from another Apple device to be displayed on the screen as it is being played from another device.

Support for Airplay Receiver is nonessential and must be disabled.

The information system must be configured to provide only essential capabilities.

Satisfies: SRG-OS-000095-GPOS-00049,SRG-OS-000300-GPOS-00118

### Audit:

Verify the macOS system is configured to disable Airplay Receiver with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowAirPlayIncomingRequests').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable Airplay Receiver by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

## 1.97 APPL-14-002090 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable TouchID for unlocking the device.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259517<br>RULE ID: SV-259517r958400 |
|-------------------------------------------------|

### Rationale:

TouchID enables the ability to unlock a macOS system with a user's fingerprint.

TouchID must be disabled for "Unlocking your Mac" on all macOS devices that are capable of using TouchID.

The system must remain locked until the user establishes access using an authorized identification and authentication method.

### Audit:

Verify the macOS system is configured to disable TouchID for unlocking the device with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowFingerprintForUnlock').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable TouchID for unlocking the device by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53::AC-11 b
- NIST SP 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

## 1.98 APPL-14-002100 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Media Sharing.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259518<br>RULE ID: SV-259518r958472 |
|-------------------------------------------------|

### Rationale:

Media sharing must be disabled.

When Media Sharing is enabled, the computer starts a network listening service that shares the contents of the user's music collection with other users in the same subnet.

The information system must be configured to provide only essential capabilities. Disabling Media Sharing helps prevent the unauthorized connection of devices and the unauthorized transfer of information. Disabling Media Sharing mitigates this risk.

Note: The Media Sharing preference panel will still allow "Home Sharing" and "Share media with guests" to be checked but the service will not be enabled.

**Audit:**

Verify the macOS system is configured to disable media sharing with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.preferences.sharing.SharingPrefsExtension'))

.objectForKey('homeSharingUIStatus'))
let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.preferences.sharing.SharingPrefsExtension'))

.objectForKey('legacySharingUIStatus'))
let pref3 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.preferences.sharing.SharingPrefsExtension'))

.objectForKey('mediaSharingUIStatus'))
if ( pref1 == 0 && pref2 == 0 && pref3 == 0 ) {
return("true")
} else {
return("false")
}
}
EOS
```

If the result is not "true", this is a finding.

**Remediation:**

Configure the macOS system to disable media sharing by installing the "com.apple.preferences.sharing.SharingPrefsExtension" configuration profile.

**Additional Information:**

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

## 1.99 APPL-14-002110 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Bluetooth sharing.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259519<br>RULE ID: SV-259519r958472 |
|-------------------------------------------------|

### Rationale:

Bluetooth Sharing must be disabled.

Bluetooth Sharing allows users to wirelessly transmit files between the macOS and Bluetooth-enabled devices, including personally owned cellphones and tablets. A malicious user might introduce viruses or malware onto the system or extract sensitive files via Bluetooth Sharing. When Bluetooth Sharing is disabled, this risk is mitigated.

### [NOTE]

*The check and fix are for the currently logged on user. To get the currently logged on user, run the following. [source,bash]*

```
CURRENT_USER=$( /usr/sbin/scutil <<< "show  
State:/Users/ConsoleUser" | /usr/bin/awk '/Name :/ && !  
/loginwindow/ { print $3 }' )
```

====

Satisfies: SRG-OS-000080-GPOS-00048,SRG-OS-000095-GPOS-00049

### Audit:

Verify the macOS system is configured to disable Bluetooth sharing with the following command:

```
/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults -currentHost read  
com.apple.Bluetooth PrefKeyServicesEnabled
```

If the result is not "0", this is a finding.

**Remediation:**

Configure the macOS system to disable Bluetooth sharing with the following command:  
`/usr/bin/sudo -u "$CURRENT_USER" /usr/bin/defaults -currentHost write com.apple.Bluetooth PrefKeyServicesEnabled -bool false`

**Additional Information:**

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.100 APPL-14-002120 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable AppleID and Internet Account modifications.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259520<br>RULE ID: SV-259520r958478 |
|-------------------------------------------------|

### Rationale:

The system must disable account modification.

Account modification includes adding additional or modifying internet accounts in Apple Mail, Calendar, Contacts, in the Internet Account System Setting Pane, or the AppleID System Setting Pane.

This prevents the addition of unauthorized accounts.

## [IMPORTANT]

**Some organizations may allow the use and configuration of the built-in Mail.app, Calendar.app, and Contacts.app for organizational communication. Information system security officers (ISSOs) may make the risk-based decision not to disable the Internet Accounts System Preference pane to avoid losing this functionality, but they are advised to first fully weigh the potential risks posed to their organization.**

### Audit:

Verify the macOS system is configured to disable account modification with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowAccountModification').js
```

```
EOS
```

If the result is not "false", this is a finding.

**Remediation:**

Configure the macOS system to disable account modification by installing the "com.apple.applicationaccess" configuration profile.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.101 APPL-14-002130 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable CD/DVD Sharing.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259521<br>RULE ID: SV-259521r958478 |
|-------------------------------------------------|

### Rationale:

CD/DVD Sharing must be disabled.

### Audit:

Verify the macOS system is configured to disable CD/DVD Sharing with the following command:

```
/usr/bin/pgrep -q ODSAgent; /bin/echo $?
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable CD/DVD Sharing with the following command:

```
/bin/launchctl unload /System/Library/LaunchDaemons/com.apple.ODSAgent.plist
```

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.102 APPL-14-002140 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable content caching service.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259522<br>RULE ID: SV-259522r958478 |
|-------------------------------------------------|

### Rationale:

Content caching must be disabled.

Content caching is a macOS service that helps reduce internet data usage and speed up software installation on Mac computers. It is not recommended for devices furnished to employees to act as a caching server.

### Audit:

Verify the macOS system is configured to disable content caching service with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowContentCaching').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable content caching service by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.103 APPL-14-002150 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud desktop and document folder synchronization.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259523<br>RULE ID: SV-259523r958478 |
|-------------------------------------------------|

### Rationale:

The macOS system's ability to automatically synchronize a user's desktop and documents folder to their iCloud Drive must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated file synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud desktop and document folder synchronization with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudDesktopAndDocuments').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud desktop and document folder synchronization by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.104 APPL-14-002160 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Game Center.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259524<br>RULE ID: SV-259524r958478 |
|-------------------------------------------------|

### Rationale:

This works only with supervised devices (MDM) and allows Apple Game Center to be disabled. The rationale is Game Center is using Apple ID and will share data on AppleID-based services; therefore, Game Center must be disabled. This setting also prohibits the functionality of adding friends to Game Center.

### Audit:

Verify the macOS system is configured to disable iCloud Game Center with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowGameCenter').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Game Center by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.105 APPL-14-002170 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable iCloud Private Relay.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259525<br>RULE ID: SV-259525r958478 |
|-------------------------------------------------|

### Rationale:

Enterprise networks may be required to audit all network traffic by policy; therefore, iCloud Private Relay must be disabled.

Network administrators can also prevent the use of this feature by blocking DNS resolution of mask.icloud.com and mask-h2.icloud.com.

### Audit:

Verify the macOS system is configured to disable the iCloud Private Relay with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudPrivateRelay').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable the iCloud Private Relay by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.106 APPL-14-002180 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Find My service.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259526<br>RULE ID: SV-259526r958478 |
|-------------------------------------------------|

### Rationale:

The Find My service must be disabled.

A Mobile Device Management (MDM) solution must be used to carry out remote locking and wiping instead of Apple's Find My service.

Apple's Find My service uses a personal AppleID for authentication. Organizations should rely on MDM solutions, which have much more secure authentication requirements, to perform remote lock and remote wipe.

**Audit:**

Verify the macOS system is configured to disable Find My service with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
function run() {
let pref1 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')

.objectForKey('allowFindMyDevice'))
let pref2 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')

.objectForKey('allowFindMyFriends'))
let pref3 =
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.icloud.managed')

.objectForKey('DisableFMMiCloudSetting'))
if ( pref1 == false && pref2 == false && pref3 == true ) {
return("true")
} else {
return("false")
}
}
EOS
```

If the result is not "true", this is a finding.

**Remediation:**

Configure the macOS system to disable Find My service by installing the "com.apple.applicationaccess" configuration profile.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.107 APPL-14-002190 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable password autofill.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259527<br>RULE ID: SV-259527r958478 |
|-------------------------------------------------|

### Rationale:

Password Autofill must be disabled.

macOS allows users to save passwords and use the Password Autofill feature in Safari and compatible apps. To protect against malicious users gaining access to the system, this feature must be disabled to prevent users from being prompted to save passwords in applications.

### Audit:

Verify the macOS system is configured to disable password autofill with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowPasswordAutoFill').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable password autofill by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.108 APPL-14-002200 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable personalized advertising.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259528<br>RULE ID: SV-259528r958478 |
|-------------------------------------------------|

### Rationale:

Ad tracking and targeted ads must be disabled.

The information system must be configured to provide only essential capabilities. Disabling ad tracking ensures that applications and advertisers are unable to track users' interests and deliver targeted advertisements.

### Audit:

Verify the macOS system is configured to disable personalized advertising with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowApplePersonalizedAdvertising').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable personalized advertising by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.109 APPL-14-002210 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable sending Siri and Dictation information to Apple.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259529<br>RULE ID: SV-259529r958478 |
|-------------------------------------------------|

### Rationale:

The ability for Apple to store and review audio of Siri and Dictation interactions must be disabled.

The information system must be configured to provide only essential capabilities. Disabling the submission of Siri and Dictation information will mitigate the risk of unwanted data being sent to Apple.

### Audit:

Verify the macOS system is configured to disable sending Siri and Dictation information to Apple with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.assistant.support')
```

```
.objectForKey('Siri Data Sharing Opt-In Status').js  
EOS
```

If the result is not "2", this is a finding.

### Remediation:

Configure the macOS system to disable sending Siri and Dictation information to Apple by installing the "com.apple.assistant.support" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.110 APPL-14-002220 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce on device dictation.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259530<br>RULE ID: SV-259530r958478 |
|-------------------------------------------------|

### Rationale:

Dictation must be restricted to on device only to prevent potential data exfiltration.

The information system must be configured to provide only essential capabilities.

### Audit:

For Intel-based systems, this is not applicable.

Verify the macOS system is configured to enforce on device dictation with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('forceOnDeviceOnlyDictation').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to enforce on device dictation by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.111 APPL-14-002230 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable dictation.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259531<br>RULE ID: SV-259531r958478 |
|-------------------------------------------------|

### Rationale:

Dictation must be disabled on Intel-based Macs as the feature On Device Dictation is only available on Apple Silicon devices.

### Audit:

For Apple Silicon-based systems, this is not applicable.  
Verify the macOS system is configured to disable dictation with the following command:  
`/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')`

`.objectForKey('allowDictation').js  
EOS  
If the result is not "false", this is a finding.`

### Remediation:

Configure the macOS system to disable dictation by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.112 APPL-14-002240 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Printer Sharing.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259532<br>RULE ID: SV-259532r958478 |
|-------------------------------------------------|

### Rationale:

Printer Sharing must be disabled.

### Audit:

Verify the macOS system is configured to disable Printer Sharing with the following command:

```
/usr/sbin/cupsctl | /usr/bin/grep -c "_share_printers=0"
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable Printer Sharing with the following commands:

```
/usr/sbin/cupsctl --no-share-printers
```

```
/usr/bin/lpstat -p | awk '{print $2}' | /usr/bin/xargs -l{} lpadmin -p {} -o printer-is-shared=false
```

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.113 APPL-14-002250 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Remote Management.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259533<br>RULE ID: SV-259533r958478 |
|-------------------------------------------------|

### Rationale:

Remote Management must be disabled.

### Audit:

Verify the macOS system is configured to disable Remote Management with the following command:

```
/usr/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c "RemoteDesktopEnabled = 0"
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable Remote Management with the following commands:

```
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -deactivate -stop
```

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.114 APPL-14-002260 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable the Bluetooth system settings pane.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259534<br>RULE ID: SV-259534r958478 |
|-------------------------------------------------|

### Rationale:

The Bluetooth System Setting pane must be disabled to prevent access to the Bluetooth configuration.

### Audit:

Verify the macOS system is configured to disable the Bluetooth system settings pane with the following command:

```
/usr/bin/profiles show -output stdout-xml | /usr/bin/xmllint --xpath  
'//key[text()="DisabledSystemSettings"]/following-sibling::*[1]' - | /usr/bin/grep -c  
com.apple.BluetoothSettings
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to disable the Bluetooth system settings pane by installing the "com.apple.systempreferences" configuration profiles.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.115 APPL-14-002270 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable the iCloud Freeform services.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259535<br>RULE ID: SV-259535r958478 |
|-------------------------------------------------|

### Rationale:

The macOS built-in Freeform.app connection to Apple's iCloud service must be disabled.

Apple's iCloud service does not provide an organization with enough control over the storage and access of data and, therefore, automated calendar synchronization must be controlled by an organization approved service.

### Audit:

Verify the macOS system is configured to disable iCloud Freeform services with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowCloudFreeform').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable iCloud Freeform services by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.116 APPL-14-003001 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must issue or obtain public key certificates from an approved service provider.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259536<br>RULE ID: SV-259536r958868 |
|-------------------------------------------------|

### Rationale:

The organization must issue or obtain public key certificates from an organization-approved service provider and ensure only approved trust anchors are in the System Keychain.

### Audit:

Verify the macOS system is configured to issue or obtain public key certificates from an approved service provider with the following command:

```
/usr/bin/security dump-keychain /Library/Keychains/System.keychain | /usr/bin/awk -F'"'
```

```
'/lab/' {print $4}'
```

If the result does not contain a list of approved certificate authorities, this is a finding.

### Remediation:

Configure the macOS system to issue or obtain public key certificates from an approved service provider by obtaining the approved certificates from the appropriate authority and install them to the System Keychain.

### Additional Information:

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

## 1.117 APPL-14-003007 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must require passwords contain a minimum of one numeric character.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259537<br>RULE ID: SV-259537r1009594 |
|--------------------------------------------------|

### Rationale:

The macOS must be configured to require at least one numeric character be used when a password is created.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

### Audit:

Verify the macOS system is configured to require passwords contain a minimum of one numeric character with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --  
xpath '//dict/key[text()="policyIdentifier"]/following-sibling::*[1]/text()' - | /usr/bin/grep  
"requireAlphanumeric" -c
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to require passwords contain a minimum of one numeric character by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

### Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

- NIST SP 800-53 Revision 5::IA-5 (1) (f)

CCI-000194 The information system enforces password complexity by the minimum number of numeric characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

## 1.118 APPL-14-003008 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must restrict maximum password lifetime to 60 days.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259538<br>RULE ID: SV-259538r1038967 |
|--------------------------------------------------|

### Rationale:

The macOS must be configured to enforce a maximum password lifetime limit of at least 60 days.

This rule ensures that users are forced to change their passwords frequently enough to prevent malicious users from gaining and maintaining access to the system.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

### Audit:

Verify the macOS system is configured to restrict maximum password lifetime to 60 days with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --  
xpath '//dict/key[text()="policyAttributeExpiresEveryNDays"]/following-sibling::*[1]/text()' -  
If the result is not "60" or less, this is a finding.
```

### Remediation:

Configure the macOS system to restrict maximum password lifetime to 60 days by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

### Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000199 The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53::IA-5 (1) (d)
- NIST SP 800-53A::IA-5 (1).1 (v)

- NIST SP 800-53 Revision 4::IA-5 (1) (d)

## 1.119 APPL-14-003010 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must require a minimum password length of 14 characters.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259540<br>RULE ID: SV-259540r1009596 |
|--------------------------------------------------|

### Rationale:

The macOS must be configured to require a minimum of 14 characters be used when a password is created.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

### Audit:

Verify the macOS system is configured to enforce a minimum 14-character password length with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --  
xpath 'boolean(//*[contains(text(),"policyAttributePassword matches \"{14}\")])' -  
If the result is not "true", this is a finding.
```

### Remediation:

Configure the macOS system to enforce a 14-character password length by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

### Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

- NIST SP 800-53 Revision 5::IA-5 (1) (f)

CCI-000205 The information system enforces minimum password length.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (i)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

## 1.120 APPL-14-003011 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must require passwords contain a minimum of one special character.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259541<br>RULE ID: SV-259541r1009597 |
|--------------------------------------------------|

### Rationale:

The macOS must be configured to require at least one special character be used when a password is created.

Special characters are those characters that are not alphanumeric. Examples include: ~ ! @ # \$ % ^ \* .

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

### Audit:

Verify the macOS system is configured to require passwords contain a minimum of one special character with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --  
xpath 'boolean(//*[contains(text(),"policyAttributePassword matches ""(.^[a-zA-Z0-  
9].*){1,}"")])' -
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to require passwords contain a minimum of one special character by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

### Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

- NIST SP 800-53 Revision 5::IA-5 (1) (f)

CCI-001619 The information system enforces password complexity by the minimum number of special characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

## 1.121 APPL-14-003012 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable password hints.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259542<br>RULE ID: SV-259542r958470 |
|-------------------------------------------------|

### Rationale:

Password hints must be disabled.

Password hints leak information about passwords that are currently in use and can lead to loss of confidentiality.

### Audit:

Verify the macOS system is configured to disable password hints with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')
```

```
.objectForKey('RetriesUntilHint').js
```

```
EOS
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system to disable password hints by installing the "com.apple.loginwindow" configuration profile.

### Additional Information:

CCI-000206 Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

- NIST SP 800-53::IA-6
- NIST SP 800-53A::IA-6.1
- NIST SP 800-53 Revision 4::IA-6
- NIST SP 800-53 Revision 5::IA-6

## 1.122 APPL-14-003013 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enable firmware password.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259543<br>RULE ID: SV-259543r991589 |
|-------------------------------------------------|

### Rationale:

A firmware password must be enabled and set.

Single user mode, recovery mode, the Startup Manager, and several other tools are available on macOS by holding the "Option" key down during startup. Setting a firmware password restricts access to these tools.

To set a firmware passcode use the following command:

*[source,bash]*

*/usr/sbin/firmwarepasswd -setpasswd*

Note: If firmware password or passcode is forgotten, the only way to reset the forgotten password is through the use of a machine specific binary generated and provided by Apple. Schedule a support call and provide proof of purchase before the firmware binary will be generated.

Note: Firmware passwords are not supported on Apple Silicon devices. This rule is only applicable to Intel devices.

### Audit:

For Apple Silicon systems, this is not applicable.

Verify the macOS system is configured with a firmware password with the following command:

*/usr/sbin/firmwarepasswd -check | /usr/bin/grep -c "Password Enabled: Yes"*

If the result is not "1", this is a finding.

**Remediation:**

Configure the macOS system with a firmware password with the following command:  
`/usr/sbin/firmwarepasswd -setpasswd`

Note: If firmware password or passcode is forgotten, the only way to reset the forgotten password is through a machine-specific binary generated and provided by Apple. Users must schedule a support call and provide proof of purchase before the firmware binary will be generated.

**Additional Information:**

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## 1.123 APPL-14-003014 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must remove password hints from user accounts.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259544<br>RULE ID: SV-259544r958470 |
|-------------------------------------------------|

### Rationale:

User accounts must not contain password hints. Password hints leak information about passwords that are currently in use and can lead to loss of confidentiality.

### Audit:

Verify the macOS system is configured to remove password hints from user accounts with the following command:

```
/usr/bin/dscl . -list /Users hint | /usr/bin/awk '{print $2}' | /usr/bin/wc -l | /usr/bin/xargs
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system to remove password hints from user accounts with the following command:

```
for u in $(/usr/bin/dscl . -list /Users UniqueID | /usr/bin/awk '$2 > 500 {print $1}'); do  
/usr/bin/dscl . -delete /Users/$u hint  
done
```

### Additional Information:

CCI-000206 Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

- NIST SP 800-53::IA-6
- NIST SP 800-53A::IA-6.1
- NIST SP 800-53 Revision 4::IA-6
- NIST SP 800-53 Revision 5::IA-6

## 1.124 APPL-14-003020 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce smart card authentication.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259545<br>RULE ID: SV-259545r1009598 |
|--------------------------------------------------|

### Rationale:

Smart card authentication must be enforced.

The use of smart card credentials facilitates standardization and reduces the risk of unauthorized access.

When enforceSmartCard is set to "true", the smart card must be used for logon, authorization, and unlocking the screen saver.

CAUTION: enforceSmartCard will apply to the whole system. No users will be able to log on with their password unless the profile is removed or a user is exempt from smart card enforcement.

Note: enforceSmartcard requires allowSmartcard to be set to true in order to work.

Satisfies: SRG-OS-000067-GPOS-00035,SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057,SRG-OS-000375-GPOS-00160,SRG-OS-000376-GPOS-00161

### Audit:

Verify the macOS system is configured to enforce multifactor authentication with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')
```

```
.objectForKey('enforceSmartCard').js  
EOS
```

If the result is not "true", this is a finding.

**Remediation:**

Configure the macOS system to enforce multifactor authentication by installing the "com.apple.security.smartcard" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

**Additional Information:**

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (b)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (1)

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5::IA-2 (6) (a)

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)

- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1
- NIST SP 800-53 Revision 4::IA-2 (3)

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53::IA-2 (4)
- NIST SP 800-53A::IA-2 (4).1
- NIST SP 800-53 Revision 4::IA-2 (4)

CCI-001948 The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 4::IA-2 (11)

## 1.125 APPL-14-003030 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must allow smart card authentication.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259546<br>RULE ID: SV-259546r1009599 |
|--------------------------------------------------|

### Rationale:

Smart card authentication must be allowed.

The use of smart card credentials facilitates standardization and reduces the risk of unauthorized access.

When enabled, the smart card can be used for logon, authorization, and screen saver unlocking.

Satisfies: SRG-OS-000068-GPOS-00036,SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057,SRG-OS-000376-GPOS-00161

### Audit:

Verify the macOS system is configured to allow smart card authentication with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.smartcard')
```

```
.objectForKey('allowSmartCard').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to enforce multifactor authentication by installing the "com.apple.security.smartcard" configuration profile.

Note: To ensure continued access to the operating system, consult the supplemental guidance provided with the STIG before applying the configuration profile.

### Additional Information:

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (c)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (2)

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1
- NIST SP 800-53 Revision 4::IA-2 (3)

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53::IA-2 (4)
- NIST SP 800-53A::IA-2 (4).1
- NIST SP 800-53 Revision 4::IA-2 (4)

## 1.126 APPL-14-003050 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce multifactor authentication for logon.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259547<br>RULE ID: SV-259547r1009600 |
|--------------------------------------------------|

### Rationale:

The system must be configured to enforce multifactor authentication.

All users must go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.

IMPORTANT: Modification of Pluggable Authentication Modules (PAM) now requires user authorization or use of a Privacy Preferences Policy Control (PPPC) profile from MDM that authorizes modifying system administrator files or full disk access.

Note: /etc/pam.d/login will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057

### Audit:

Verify the macOS system is configured to enforce multifactor authentication for login with the following command:

```
/usr/bin/grep -Ec
```

```
'^(auth\s+sufficient\s+pam_smartcard.so|auth\s+required\s+pam_deny.so)'
```

```
/etc/pam.d/login
```

If the result is not "2", this is a finding.

### Remediation:

Configure the macOS system to enforce multifactor authentication for login with the following commands:

```
/bin/cat > /etc/pam.d/login << LOGIN_END
```

## login: auth account password session

```
auth sufficient pam_smartcard.so
auth optional pam_krb5.so use_kcminit
auth optional pam_ntlm.so try_first_pass
auth optional pam_mount.so try_first_pass
auth required pam_opendirectory.so try_first_pass
auth required pam_deny.so
account required pam_nologin.so
account required pam_opendirectory.so
password required pam_opendirectory.so
session required pam_launchd.so
session required pam_uwtmp.so
session optional pam_mount.so
LOGIN_END
/bin/chmod 644 /etc/pam.d/login
/usr/sbin/chown root:wheel /etc/pam.d/login
```

### Additional Information:

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1
- NIST SP 800-53 Revision 4::IA-2 (3)

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53::IA-2 (4)
- NIST SP 800-53A::IA-2 (4).1
- NIST SP 800-53 Revision 4::IA-2 (4)

## 1.127 APPL-14-003051 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce multifactor authentication for the su command.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259548<br>RULE ID: SV-259548r1009601 |
|--------------------------------------------------|

### Rationale:

The system must be configured such that, when the su command is used, multifactor authentication is enforced.

All users must go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.

IMPORTANT: Modification of Pluggable Authentication Modules (PAM) now requires user authorization or use of a Privacy Preferences Policy Control (PPPC) profile from MDM that authorizes modifying system administrator files or full disk access.

Note: /etc/pam.d/su will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057

### Audit:

Verify the macOS system is configured to enforce multifactor authentication for the su command with the following command:

```
/usr/bin/grep -Ec
```

```
'^(auth\s+sufficient\s+pam_smartcard.so|auth\s+required\s+pam_rootok.so)'
```

```
/etc/pam.d/su
```

If the result is not "2", this is a finding.

### Remediation:

Configure the macOS system to enforce multifactor authentication for the su command with the following commands:

```
/bin/cat > /etc/pam.d/su << SU_END
```

## su: auth account password session

```
auth sufficient pam_smartcard.so
auth required pam_rootok.so
auth required pam_group.so no_warn group=admin,wheel ruser root_only fail_safe
account required pam_permit.so
account required pam_opendirectory.so no_check_shell
password required pam_opendirectory.so
session required pam_launchd.so
SU_END
```

## Fix new file ownership and permissions

```
/bin/chmod 644 /etc/pam.d/su
/usr/sbin/chown root:wheel /etc/pam.d/su
```

### Additional Information:

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1
- NIST SP 800-53 Revision 4::IA-2 (3)

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53::IA-2 (4)
- NIST SP 800-53A::IA-2 (4).1
- NIST SP 800-53 Revision 4::IA-2 (4)

## 1.128 APPL-14-003052 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce multifactor authentication for privilege escalation through the sudo command.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259549<br>RULE ID: SV-259549r1009602 |
|--------------------------------------------------|

### Rationale:

The system must be configured to enforce multifactor authentication when the sudo command is used to elevate privilege.

All users must go through multifactor authentication to prevent unauthenticated access and potential compromise to the system.

IMPORTANT: Modification of Pluggable Authentication Modules (PAM) now requires user authorization, or use of a Privacy Preferences Policy Control (PPPC) profile from MDM that authorizes modifying system administrator files or full disk access.

Note: /etc/pam.d/sudo will be automatically modified to its original state following any update or major upgrade to the operating system.

Satisfies: SRG-OS-000105-GPOS-00052,SRG-OS-000106-GPOS-00053,SRG-OS-000107-GPOS-00054,SRG-OS-000108-GPOS-00055,SRG-OS-000112-GPOS-00057

### Audit:

Verify the macOS system is configured to enforce multifactor authentication for privilege escalation through the sudo command with the following command:

```
/usr/bin/grep -Ec
```

```
^(auth\s+sufficient\s+pam_smartcard.so|auth\s+required\s+pam_deny.so)'
```

```
/etc/pam.d/sudo
```

If the result is not "2", this is a finding.

### Remediation:

Configure the macOS system to enforce multifactor authentication for privilege escalation through the sudo command with the following commands:

```
/bin/cat > /etc/pam.d/sudo << SUDO_END
```

## **sudo: auth account password session**

```
auth sufficient pam_smartcard.so
auth required pam_opendirectory.so
auth required pam_deny.so
account required pam_permit.so
password required pam_deny.so
session required pam_permit.so
SUDO_END
/bin/chmod 444 /etc/pam.d/sudo
/usr/sbin/chown root:wheel /etc/pam.d/sudo
```

### **Additional Information:**

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5::IA-2 (6) (b)

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1

- NIST SP 800-53 Revision 4::IA-2 (3)

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53::IA-2 (4)
- NIST SP 800-53A::IA-2 (4).1
- NIST SP 800-53 Revision 4::IA-2 (4)

## 1.129 APPL-14-003060 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must require passwords contain a minimum of one lowercase character and one uppercase character.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259550<br>RULE ID: SV-259550r1038909 |
|--------------------------------------------------|

### Rationale:

The macOS be configured to require at least one lowercase character and one uppercase character be used when a password is created.

This rule enforces password complexity by requiring users to set passwords that are less vulnerable to malicious users.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

Note: The configuration profile generated must be installed from an MDM server.

Satisfies: SRG-OS-000069-GPOS-00037,SRG-OS-000070-GPOS-00038

### Audit:

Verify the macOS system is configured to require passwords contain a minimum of one lowercase character and one uppercase character with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --  
xpath 'boolean(//*[contains(text(),"policyAttributePassword matches ""^(?=[A-Z])(?=[a-  
z])(?=[0-9]).*$"")])' -
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to require at least one lowercase character and one uppercase character in password complexity by installing the "com.apple.mobiledevice.passwordpolicy" configuration profile.

### Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

- NIST SP 800-53 Revision 5::IA-5 (1) (f)

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

## 1.130 APPL-14-003070 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must set minimum password lifetime to 24 hours.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259551<br>RULE ID: SV-259551r1038913 |
|--------------------------------------------------|

### Rationale:

The macOS must be configured to enforce a minimum password lifetime limit of 24 hours.

This rule discourages users from cycling through their previous passwords to get back to a preferred one.

Note: The guidance for password-based authentication in NIST 800-53 (Rev 5) and NIST 800-63B state that complexity rules should be organizationally defined. The values defined are based on common complexity values, but an organization may define its own password complexity rules.

### Audit:

Verify the macOS system is configured to set minimum password lifetime to 24 hours with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --  
xpath '//dict/key[text()="policyAttributeMinimumLifetimeHours"]/following-  
sibling::integer[1]/text()' - | /usr/bin/awk '{ if ($1 >= 24 ) {print "yes"} else {print "no"}}'
```

If the result is not "yes", this is a finding.

### Remediation:

Configure the macOS system to set minimum password lifetime to 24 hours.

This setting may be enforced using local policy or by a directory service.

To set local policy to require a minimum password lifetime, edit the current password policy to contain the following within the "policyCategoryPasswordContent":

*[source,xml]*

*[source,bash]*

*/usr/bin/pwpolicy setaccountpolicies \$pwpolicy\_file*

**Additional Information:**

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000198 The information system enforces minimum password lifetime restrictions.

- NIST SP 800-53::IA-5 (1) (d)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (d)

## 1.131 APPL-14-003080 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable accounts after 35 days of inactivity.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259552<br>RULE ID: SV-259552r1038915 |
|--------------------------------------------------|

### Rationale:

The macOS must be configured to disable accounts after 35 days of inactivity.

This rule prevents malicious users from making use of unused accounts to gain access to the system while avoiding detection.

### Audit:

Verify the macOS system is configured to disable accounts after 35 days of inactivity with the following command:

```
/usr/bin/pwpolicy -getaccountpolicies 2> /dev/null | /usr/bin/tail +2 | /usr/bin/xmllint --  
xpath '//dict/key[text()="policyAttributeInactiveDays"]/following-sibling::integer[1]/text()' -  
If the result is not "35", this is a finding.
```

### Remediation:

Configure the macOS system to disable accounts after 35 days of inactivity with the following command.

This setting may be enforced using local policy or by a directory service.

To set local policy to disable an inactive user after 35 days, edit the current password policy to contain the following within the "policyCategoryAuthentication":

*[source,xml]*

*[source,bash]*

```
/usr/bin/pwpolicy setaccountpolicies $pwpolicy_file
```

### Additional Information:

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5::AC-2 (3) (a)

CCI-003628 Disable accounts when the accounts are no longer associated to a user.

- NIST SP 800-53 Revision 5::AC-2 (3) (b)

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53::IA-4 e
- NIST SP 800-53A::IA-4.1 (iii)
- NIST SP 800-53 Revision 4::IA-4 e

## 1.132 APPL-14-004001 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure Apple System Log files to be owned by root and group to wheel.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259553<br>RULE ID: SV-259553r958564 |
|-------------------------------------------------|

### Rationale:

The Apple System Logs (ASL) must be owned by root.

ASL logs contain sensitive data about the system and users. If ASL log files are set to only be readable and writable by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

### Audit:

Verify the macOS system is configured with Apple System Log files owned by root and group to wheel with the following command:

```
/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk '!/^root:wheel:/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with Apple System Log files owned by root and group to wheel with the following command:

```
/usr/sbin/chown root:wheel $(/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk '!/^root:wheel:/{print $1}' | /usr/bin/awk -F":" '!/^root:wheel:/{print $3}')
```

### Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

## 1.133 APPL-14-004002 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure Apple System Log files to mode 640 or less permissive.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259554<br>RULE ID: SV-259554r958564 |
|-------------------------------------------------|

### Rationale:

The Apple System Logs (ASL) must be configured to be writable by root and readable only by the root user and group wheel. To achieve this, ASL log files must be configured to mode 640 permissive or less; thereby preventing normal users from reading, modifying, or deleting audit logs. System logs frequently contain sensitive information that could be used by an attacker. Setting the correct permissions mitigates this risk.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

### Audit:

Verify the macOS system is configured with Apple System Log files to mode 640 or less permissive with the following command:

```
/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk '!/640/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with Apple System Log files to mode 640 with the following command:

```
/bin/chmod 640 $(/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -e '^>' /etc/asl.conf /etc/asl/* | /usr/bin/awk '{ print $2 }') 2> /dev/null | /usr/bin/awk -F":" '!/640/{print $2}')
```

### Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

## 1.134 APPL-14-004022 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must require users to reauthenticate for privilege escalation when using the "sudo" command.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259555<br>RULE ID: SV-259555r1050789 |
|--------------------------------------------------|

### Rationale:

The file /etc/sudoers must include a timestamp\_timeout of 0.

Without reauthentication, users may access resources or perform tasks for which they do not have authorization. When operating systems provide the capability to escalate a functional capability or change user authenticators, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156,SRG-OS-000373-GPOS-00157,SRG-OS-000373-GPOS-00158

### Audit:

Verify the macOS system requires reauthentication when using the "sudo" command to elevate privileges with the following command:

```
/usr/bin/sudo /usr/bin/sudo -V | /usr/bin/grep -c "Authentication timestamp timeout: 0.0 minutes"
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to require reauthentication when using "sudo" with the following command:

```
/usr/bin/find /etc/sudoers* -type f -exec sed -i " 'timestamp_timeout/d' '{}' ;  
/bin/echo "Defaults timestamp_timeout=0" >> /etc/sudoers.d/mscp
```

### Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

## 1.135 APPL-14-004030 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure system log files to be owned by root and group to wheel.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259556<br>RULE ID: SV-259556r958564 |
|-------------------------------------------------|

### Rationale:

The system log files must be owned by root.

System logs contain sensitive data about the system and users. If log files are set to only be readable and writable by system administrators, the risk is mitigated.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

### Audit:

Verify the macOS system is configured with system log files owned by root and group to wheel with the following command:

```
/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk '!/^root:wheel:/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with system log files owned by root and group to wheel with the following command:

```
/usr/sbin/chown root:wheel $(/usr/bin/stat -f '%Su:%Sg:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk -F":" '!/^root:wheel:/{print $3}')
```

### Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

## 1.136 APPL-14-004040 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure system log files to mode 640 or less permissive.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259557<br>RULE ID: SV-259557r958564 |
|-------------------------------------------------|

### Rationale:

The system logs must be configured to be writable by root and readable only by the root user and group wheel. To achieve this, system log files must be configured to mode 640 permissive or less; thereby preventing normal users from reading, modifying, or deleting audit logs. System logs frequently contain sensitive information that could be used by an attacker. Setting the correct permissions mitigates this risk.

Satisfies: SRG-OS-000205-GPOS-00083,SRG-OS-000206-GPOS-00084

### Audit:

Verify the macOS system is configured with system log files set to mode 640 or less permissive with the following command:

```
/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk '!/640/{print $1}' | /usr/bin/wc -l | /usr/bin/tr -d ' '
```

If the result is not "0", this is a finding.

### Remediation:

Configure the macOS system with system log files set to mode 640 or less permissive with the following command:

```
/bin/chmod 640 $(/usr/bin/stat -f '%A:%N' $(/usr/bin/grep -v '^#' /etc/newsyslog.conf | /usr/bin/awk '{ print $1 }') 2> /dev/null | /usr/bin/awk '!/640/{print $1}' | awk -F":" '!/640/{print $2}')
```

### Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

## 1.137 APPL-14-004050 (Manual)

### Profile Applicability:

- SEVERITY: CAT III

### Description:

The macOS system must configure install.log retention to 365.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259558<br>RULE ID: SV-259558r958752 |
|-------------------------------------------------|

### Rationale:

The install.log must be configured to require records be kept for an organizational-defined value before deletion, unless the system uses a central audit record storage facility.

### Audit:

Verify the macOS system is configured with install.log retention to 365 with the following command:

```
/usr/sbin/aslmanager -dd 2>&1 | /usr/bin/awk '/var/log/install.log/ {count++} /Processing module com.apple.install/,/Finished/ { for (i=1;i<=NR;i++) { if ($i == "TTL" && $(i+2) >= 365) { ttl="True" }; if ($i == "MAX") {max="True"}}} END{if (count > 1) { print "Multiple config files for /var/log/install, manually remove"} else if (ttl != "True") { print "TTL not configured" } else if (max == "True") { print "Max Size is configured, must be removed" } else { print "Yes" } }'
```

If the result is not "yes", this is a finding.

### Remediation:

Configure the macOS system with install.log retention to 365 with the following command:

```
/usr/bin/sed -i "s/* file /var/log/install.log.*/ file /var/log/install.log format='$(Time)(JZ)$Host $(Sender)[$(PID)]: $Message' rotate=utc compress file_max=50M size_only ttl=365/g" /etc/asl/com.apple.install
```

Note: If there are multiple configuration files in /etc/asl that are set to process the file /var/log/install.log, these files will have to be manually removed.

### Additional Information:

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4::AU-4
- NIST SP 800-53 Revision 5::AU-4

## 1.138 APPL-14-004060 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure sudoers timestamp type.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259559<br>RULE ID: SV-259559r1050789 |
|--------------------------------------------------|

### Rationale:

The file /etc/sudoers must be configured to not include a timestamp\_type of global or ppid and be configured for timestamp record types of tty.

This rule ensures that the "sudo" command will prompt for the administrator's password at least once in each newly opened terminal window. This prevents a malicious user from taking advantage of an unlocked computer or an abandoned logon session by bypassing the normal password prompt requirement.

Satisfies: SRG-OS-000373-GPOS-00156,SRG-OS-000373-GPOS-00157

### Audit:

Verify the macOS system is configured with sudoers timestamp type with the following command:

```
/usr/bin/sudo /usr/bin/sudo -V | /usr/bin/awk -F": " '/Type of authentication timestamp record/{print $2}'
```

If the result is not "tty", this is a finding.

### Remediation:

Configure the macOS system with sudoers timestamp type with the following command:

```
/usr/bin/find /etc/sudoers* -type f -exec sed -i " /timestamp_type/d; /!tty_tickets/d" {} ;
```

### Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11

- NIST SP 800-53 Revision 5::IA-11

## 1.139 APPL-14-005001 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must ensure System Integrity Protection is enabled.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259560<br>RULE ID: SV-259560r1038911 |
|--------------------------------------------------|

### Rationale:

System Integrity Protection (SIP) must be enabled.

SIP is vital to protecting the integrity of the system as it prevents malicious users and software from making unauthorized and/or unintended modifications to protected files and folders; ensures the presence of an audit record generation capability for defined auditable events for all operating system components; protects audit tools from unauthorized access, modification, and deletion; restricts the root user account and limits the actions that the root user can perform on protected parts of the macOS; and prevents nonprivileged users from granting other users direct access to the contents of their home directories and folders.

Note: SIP is enabled by default in macOS.

Satisfies: SRG-OS-000051-GPOS-00024,SRG-OS-000054-GPOS-00025,SRG-OS-000057-GPOS-00027,SRG-OS-000058-GPOS-00028,SRG-OS-000059-GPOS-00029,SRG-OS-000062-GPOS-00031,SRG-OS-000080-GPOS-00048,SRG-OS-000122-GPOS-00063,SRG-OS-000256-GPOS-00097,SRG-OS-000257-GPOS-00098,SRG-OS-000258-GPOS-00099,SRG-OS-000259-GPOS-00100,SRG-OS-000278-GPOS-00108,SRG-OS-000350-GPOS-00138

### Audit:

Verify the macOS system is configured to enable System Integrity Protection with the following command:

```
/usr/bin/csrutil status | /usr/bin/grep -c 'System Integrity Protection status: enabled.'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to enable "System Integrity Protection" by booting into "Recovery" mode, launch "Terminal" from the "Utilities" menu, and run the following command:

```
/usr/bin/csrutil enable
```

### **Additional Information:**

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53::AU-6 (4)
- NIST SP 800-53A::AU-6 (4).1
- NIST SP 800-53 Revision 4::AU-6 (4)
- NIST SP 800-53 Revision 5::AU-6 (4)

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53::AU-7 (1)
- NIST SP 800-53A::AU-7 (1).1
- NIST SP 800-53 Revision 4::AU-7 (1)
- NIST SP 800-53 Revision 5::AU-7 (1)

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a

- NIST SP 800-53 Revision 5::AU-12 a

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001496 Implement cryptographic mechanisms to protect the integrity of audit tools.

- NIST SP 800-53::AU-9 (3)
- NIST SP 800-53A::AU-9 (3).1
- NIST SP 800-53 Revision 4::AU-9 (3)
- NIST SP 800-53 Revision 5::AU-9 (3)

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

CCI-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

## 1.140 APPL-14-005020 (Manual)

### Profile Applicability:

- SEVERITY: CAT I

### Description:

The macOS system must enforce FileVault.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259561<br>RULE ID: SV-259561r958552 |
|-------------------------------------------------|

### Rationale:

FileVault must be enforced.

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Satisfies: SRG-OS-000185-GPOS-00079,SRG-OS-000404-GPOS-00183,SRG-OS-000405-GPOS-00184

### Audit:

Verify the macOS system is configured to enforce FileVault with the following command:  
dontAllowDisable=\$(/usr/bin/osascript -l JavaScript << EOS  
\$.NSUserDefaults.alloc.initWithSuiteName('com.apple.MCX')

```
.objectForKey('dontAllowFDEDisable').js  
EOS  
)  
fileVault=$(/usr/bin/fdesetup status | /usr/bin/grep -c "FileVault is On.")  
if [[ "$dontAllowDisable" == "true" ]] && [[ "$fileVault" == 1 ]]; then  
echo "1"  
else  
echo "0"  
fi  
If the result is not "1", this is a finding.
```

### Remediation:

Note: Refer to the FileVault supplemental to implement this rule.

### Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

CCI-002475 Implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

CCI-002476 Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

## 1.141 APPL-14-005050 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enable the application firewall.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259562<br>RULE ID: SV-259562r991593 |
|-------------------------------------------------|

### Rationale:

The macOS Application Firewall is the built-in firewall that comes with macOS, and it must be enabled.

When the macOS Application Firewall is enabled, the flow of information within the information system and between interconnected systems will be controlled by approved authorizations.

### Audit:

Verify the macOS system is configured to enable the application firewall with the following command:

```
profile="$(/usr/bin/osascript -l JavaScript << EOS
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.security.firewall')

.objectForKey('EnableFirewall').js
EOS
)"
plist="$(/usr/bin/defaults read /Library/Preferences/com.apple.alf globalstate
2>/dev/null)"
if [[ "$profile" == "true" ]] && [[ "$plist" =~ [1,2] ]]; then
echo "true"
else
echo "false"
fi
If the result is not "true", this is a finding.
```

### Remediation:

Configure the macOS system to enable the application firewall with the following command:

```
/usr/bin/defaults write /Library/Preferences/com.apple.alf globalstate -int 1
```

**Additional Information:**

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## 1.142 APPL-14-005052 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must configure login window to prompt for username and password.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259563<br>RULE ID: SV-259563r958482 |
|-------------------------------------------------|

### Rationale:

The login window must be configured to prompt all users for both a username and a password.

By default, the system displays a list of known users on the login window, which can make it easier for a malicious user to gain access to someone else's account. Requiring users to type in both their username and password mitigates the risk of unauthorized users gaining access to the information system.

### Audit:

Verify the macOS system is configured to prompt for username and password at the login window with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.loginwindow')
```

```
.objectForKey('SHOWFULLNAME').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to prompt for username and password at the login window by installing the "com.apple.loginwindow" configuration profile.

### Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

## 1.143 APPL-14-005054 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable TouchID prompt during Setup Assistant.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259564<br>RULE ID: SV-259564r958478 |
|-------------------------------------------------|

### Rationale:

The prompt for TouchID during Setup Assistant must be disabled.

macOS prompts new users through enabling TouchID during Setup Assistant; this is not essential, and therefore must be disabled to prevent against the risk of individuals electing to enable TouchID to override organizationwide settings.

### Audit:

Verify the macOS system is configured to disable TouchID prompt during Setup Assistant with the following command:  
`/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')`

`.objectForKey('SkipTouchIDSetup').js  
EOS`

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable TouchID prompt during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.144 APPL-14-005055 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Screen Time prompt during Setup Assistant.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259565<br>RULE ID: SV-259565r958478 |
|-------------------------------------------------|

### Rationale:

The prompt for Screen Time setup during Setup Assistant must be disabled.

### Audit:

Verify the macOS system is configured to disable Screen Time prompt during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')
```

```
.objectForKey('SkipScreenTime').js
```

```
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable Screen Time prompt during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.145 APPL-14-005056 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Unlock with Apple Watch during Setup Assistant.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259566<br>RULE ID: SV-259566r958478 |
|-------------------------------------------------|

### Rationale:

The prompt for Apple Watch unlock setup during Setup Assistant must be disabled.

Disabling Apple watches is a necessary step to ensuring that the information system retains a session lock until the user reestablishes access using an authorized identification and authentication procedures.

### Audit:

Verify the macOS system is configured to disable Unlock with Apple Watch during Setup Assistant with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SetupAssistant.managed')
```

```
.objectForKey('SkipUnlockWithWatch').js  
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to disable Unlock with Apple Watch during Setup Assistant by installing the "com.apple.SetupAssistant.managed" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.146 APPL-14-005058 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Handoff.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259567<br>RULE ID: SV-259567r958472 |
|-------------------------------------------------|

### Rationale:

Handoff must be disabled.

Handoff allows users to continue working on a document or project when the user switches from one Apple device to another. Disabling Handoff prevents data transfers to unauthorized devices.

Satisfies: SRG-OS-000080-GPOS-00048,SRG-OS-000095-GPOS-00049,SRG-OS-000300-GPOS-00118

### Audit:

Verify the macOS system is configured to disable handoff with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowActivityContinuation').js
```

```
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable handoff by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

## 1.147 APPL-14-005060 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable proximity-based password sharing requests.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259568<br>RULE ID: SV-259568r958478 |
|-------------------------------------------------|

### Rationale:

Proximity-based password sharing requests must be disabled.

The default behavior of macOS is to allow users to request passwords from other known devices (macOS and iOS). This feature must be disabled to prevent passwords from being shared.

### Audit:

Verify the macOS system is configured to disable proximity-based password sharing requests with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowPasswordProximityRequests').js
```

```
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable proximity-based password sharing requests by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.148 APPL-14-005061 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must disable Erase Content and Settings.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259569<br>RULE ID: SV-259569r958478 |
|-------------------------------------------------|

### Rationale:

Erase Content and Settings must be disabled.

### Audit:

Verify the macOS system is configured to disable Erase Content and Settings with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess')
```

```
.objectForKey('allowEraseContentAndSettings').js  
EOS
```

If the result is not "false", this is a finding.

### Remediation:

Configure the macOS system to disable Erase Content and Settings by installing the "com.apple.applicationaccess" configuration profile.

### Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

## 1.149 APPL-14-005070 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enable Authenticated Root.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259570<br>RULE ID: SV-259570r958472 |
|-------------------------------------------------|

### Rationale:

Authenticated Root must be enabled.

When Authenticated Root is enabled the macOS is booted from a signed volume that is cryptographically protected to prevent tampering with the system volume.

Note: Authenticated Root is enabled by default on macOS systems.

WARNING: If more than one partition with macOS is detected, the csrutil command will hang awaiting input.

### Audit:

Verify the macOS system is configured to enable authenticated root with the following command:

```
/usr/bin/csrutil authenticated-root | /usr/bin/grep -c 'enabled'
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to enable authenticated root with the following command:

```
/usr/bin/csrutil authenticated-root enable
```

Note: To reenable "Authenticated Root", boot the affected system into "Recovery" mode, launch "Terminal" from the "Utilities" menu, and run the command.

### Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

## 1.150 APPL-14-005080 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must prohibit user installation of software into /users/.

|                                                  |
|--------------------------------------------------|
| GROUP ID: V-259571<br>RULE ID: SV-259571r1009608 |
|--------------------------------------------------|

### Rationale:

Users must not be allowed to install software into /users/.

Allowing users who do not possess explicit privileges to install software presents the risk of untested and potentially malicious software being installed on the system. Explicit privileges (escalated or administrative privileges) provide the regular user with explicit capabilities and control that exceeds the rights of a regular user.

## [IMPORTANT]

Apple has deprecated the use of application restriction controls (<https://github.com/apple/device-management/blob/eb51fb0cb9626cac4717858556912c257a734ce0/mdm/profiles/com.apple.applicationaccess.new.yaml#L67-L70>). Using these controls may not work as expected. Third-party software may be required to fulfill the compliance requirements.

### Audit:

Verify the macOS system is configured to prohibit user installation of software into /users/ with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
function run() {
```

```
let pref1 =
```

```
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new'))
```

```
.objectForKey('familyControlsEnabled'))
```

```
let pathlist =
```

```
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess.new')
```

```
.objectForKey('pathBlackList').js
```

```
for ( let app in pathlist ) {
```

```
if ( ObjC.unwrap(pathlist[app]) == "/Users/" && pref1 == true ){
```

```
return("true")
```

```
}
```

```
}
```

```
return("false")
```

```
}
```

```
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to prohibit user installation of software into /users/ by installing the "com.apple.applicationaccess.new" configuration profile.

### Additional Information:

CCI-003980 Allow user installation of software only with explicit privileged status.

- NIST SP 800-53 Revision 5::CM-11 (2)

CCI-001812 The information system prohibits user installation of software without explicit privileged status.

- NIST SP 800-53 Revision 4::CM-11 (2)

## 1.151 APPL-14-005090 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must authorize USB devices before allowing connection.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259572<br>RULE ID: SV-259572r986236 |
|-------------------------------------------------|

### Rationale:

USB devices connected to a Mac must be authorized.

## [IMPORTANT]

**This feature is removed if a smart card is paired or smart card attribute mapping is configured.**

### Audit:

Verify the macOS system is configured to authorize USB devices before allowing connection with the following command:

```
/usr/bin/osascript -l JavaScript << EOS
```

```
function run() {
```

```
let pref1 =
```

```
ObjC.unwrap($.NSUserDefaults.alloc.initWithSuiteName('com.apple.applicationaccess'))
```

```
.objectForKey('allowUSBRestrictedMode'))
```

```
if ( pref1 == false ) {
```

```
return("false")
```

```
} else {
```

```
return("true")
```

```
}
```

```
}
```

```
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to authorize USB devices before allowing connection by installing the "com.apple.applicationaccess" configuration profile.

**Additional Information:**

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4::IA-3
- NIST SP 800-53 Revision 5::IA-3

CCI-003959 Prohibit the use or connection of unauthorized hardware components.

- NIST SP 800-53 Revision 5::CM-7 (9) (b)

## 1.152 APPL-14-005100 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must ensure secure boot level set to full.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259573<br>RULE ID: SV-259573r958944 |
|-------------------------------------------------|

### Rationale:

The Secure Boot security setting must be set to full.

Full security is the default Secure Boot setting in macOS. During startup, when Secure Boot is set to full security, the Mac will verify the integrity of the operating system before allowing the operating system to boot.

Note: This will only return a proper result on T2 or Apple Silicon Macs.

Satisfies: SRG-OS-000445-GPOS-00199,SRG-OS-000446-GPOS-00200,SRG-OS-000447-GPOS-00201

### Audit:

Verify the macOS system is configured to ensure secure boot level set to full using the following command:

```
/usr/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c "SecureBootLevel = full"
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system to ensure secure boot level set to full by booting into Recovery Mode and enable Full Secure Boot.

### Additional Information:

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4::SI-6 a
- NIST SP 800-53 Revision 5::SI-6 a

CCI-002699 Perform verification of the correct operation of organization-defined security functions: when the system is in an organization-defined transitional state; upon command by a user with appropriate privileges; and/or on an organization-defined frequency.

- NIST SP 800-53 Revision 4::SI-6 b
- NIST SP 800-53 Revision 5::SI-6 b

CCI-002702 Shut the system down, restart the system, and/or initiate organization-defined alternative action(s) when anomalies in the operation of the organization-defined security functions are discovered.

- NIST SP 800-53 Revision 4::SI-6 d
- NIST SP 800-53 Revision 5::SI-6 d

## 1.153 APPL-14-005110 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce enrollment in mobile device management.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259574<br>RULE ID: SV-259574r991589 |
|-------------------------------------------------|

### Rationale:

Users must enroll their Mac in a Mobile Device Management (MDM) software.

User Approved MDM (UAMDM) enrollment or enrollment via Apple Business Manager (ABM)/Apple School Manager (ASM) is required to manage certain security settings. Currently these include:

- Allowed Kernel Extensions
- Allowed Approved System Extensions
- Privacy Preferences Policy Control Payload
- ExtensibleSingleSignOn
- FDEFileVault

In macOS 11, UAMDM grants Supervised status on a Mac, unlocking the following MDM features, which were previously locked behind ABM:

- Activation Lock Bypass
- Access to Bootstrap Tokens
- Scheduling Software Updates
- Query list and delete local users

### Audit:

Verify the macOS system is configured to enforce enrollment in mobile device management with the following command:

```
/usr/bin/profiles status -type enrollment | /usr/bin/awk -F: '/MDM enrollment/ {print $2}' |  
/usr/bin/grep -c "Yes (User Approved)"
```

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system by ensuring that system is enrolled via UAMDM.

**Additional Information:**

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## 1.154 APPL-14-005120 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enable recovery lock.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259575<br>RULE ID: SV-259575r991589 |
|-------------------------------------------------|

### Rationale:

A recovery lock password must be enabled and set.

Single user mode, recovery mode, the Startup Manager, and several other tools are available on macOS by holding down specific key combinations during startup. Setting a recovery lock restricts access to these tools.

IMPORTANT: Recovery lock passwords are not supported on Intel devices. This rule is only applicable to Apple Silicon devices.

### Audit:

For non-Apple Silicon systems, this is not applicable.

Verify the macOS system is configured with recovery lock with the following command:  
`/usr/libexec/mdmclient QuerySecurityInfo | /usr/bin/grep -c "IsRecoveryLockEnabled = 1"`

If the result is not "1", this is a finding.

### Remediation:

Configure the macOS system with recovery lock with the SetRecoveryLock command. This can be used to set a Recovery Lock password and must be from the MDM.

### Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## 1.155 APPL-14-005130 (Manual)

### Profile Applicability:

- SEVERITY: CAT II

### Description:

The macOS system must enforce installation of XProtect Remediator and Gatekeeper updates automatically.

|                                                 |
|-------------------------------------------------|
| GROUP ID: V-259576<br>RULE ID: SV-259576r991589 |
|-------------------------------------------------|

### Rationale:

Software Update must be configured to update XProtect Remediator and Gatekeeper automatically.

This setting enforces definition updates for XProtect Remediator and Gatekeeper; with this setting in place, new malware and adware that Apple has added to the list of malware or untrusted software will not execute. These updates do not require the computer to be restarted.

<https://support.apple.com/en-us/HT207005>

Note: Software update will automatically update XProtect Remediator and Gatekeeper by default in the macOS.

### Audit:

Verify the macOS system is configured to enforce installation of XProtect Remediator and Gatekeeper updates automatically with the following command:

```
/usr/bin/osascript -l JavaScript << EOS  
$.NSUserDefaults.alloc.initWithSuiteName('com.apple.SoftwareUpdate')
```

```
.objectForKey('ConfigDataInstall').js
```

```
EOS
```

If the result is not "true", this is a finding.

### Remediation:

Configure the macOS system to enforce installation of XProtect Remediator and Gatekeeper updates automatically by installing the "com.apple.SoftwareUpdate" configuration profile.

### Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

# Appendix: Summary Table

| CIS Benchmark Recommendation |                         | Set Correctly            |                          |
|------------------------------|-------------------------|--------------------------|--------------------------|
|                              |                         | Yes                      | No                       |
| <b>1</b>                     | <b>STIG RULES</b>       |                          |                          |
| 1.1                          | APPL-14-000001 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2                          | APPL-14-000002 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3                          | APPL-14-000003 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4                          | APPL-14-000005 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5                          | APPL-14-000009 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6                          | APPL-14-000007 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7                          | APPL-14-000012 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8                          | APPL-14-000014 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9                          | APPL-14-000022 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.10                         | APPL-14-000023 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.11                         | APPL-14-000024 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.12                         | APPL-14-000025 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13                         | APPL-14-000030 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.14                         | APPL-14-000031 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.15                         | APPL-14-000033 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.16                         | APPL-14-000051 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.17                         | APPL-14-000052 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.18                         | APPL-14-000053 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                         | Set Correctly            |                          |
|------------------------------|-------------------------|--------------------------|--------------------------|
|                              |                         | Yes                      | No                       |
| 1.19                         | APPL-14-000054 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.20                         | APPL-14-000057 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.21                         | APPL-14-000060 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.22                         | APPL-14-000070 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.23                         | APPL-14-000090 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.24                         | APPL-14-000100 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.25                         | APPL-14-000110 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.26                         | APPL-14-000120 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.27                         | APPL-14-000130 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.28                         | APPL-14-000140 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.29                         | APPL-14-000160 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.30                         | APPL-14-000170 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.31                         | APPL-14-000180 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.32                         | APPL-14-001001 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.33                         | APPL-14-001002 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.34                         | APPL-14-001003 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.35                         | APPL-14-001010 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.36                         | APPL-14-001012 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.37                         | APPL-14-001013 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.38                         | APPL-14-001014 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.39                         | APPL-14-001015 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                         | Set Correctly            |                          |
|------------------------------|-------------------------|--------------------------|--------------------------|
|                              |                         | Yes                      | No                       |
| 1.40                         | APPL-14-001016 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.41                         | APPL-14-001017 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.42                         | APPL-14-001020 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.43                         | APPL-14-001021 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.44                         | APPL-14-001022 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.45                         | APPL-14-001023 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.46                         | APPL-14-001024 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.47                         | APPL-14-001029 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.48                         | APPL-14-001030 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.49                         | APPL-14-001031 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.50                         | APPL-14-001044 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.51                         | APPL-14-001060 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.52                         | APPL-14-001100 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.53                         | APPL-14-001110 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.54                         | APPL-14-001120 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.55                         | APPL-14-001130 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.56                         | APPL-14-001140 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.57                         | APPL-14-002001 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.58                         | APPL-14-002003 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.59                         | APPL-14-001150 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.60                         | APPL-14-002004 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                         | Set Correctly            |                          |
|------------------------------|-------------------------|--------------------------|--------------------------|
|                              |                         | Yes                      | No                       |
| 1.61                         | APPL-14-002005 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.62                         | APPL-14-002006 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.63                         | APPL-14-002007 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.64                         | APPL-14-002008 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.65                         | APPL-14-002009 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.66                         | APPL-14-002010 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.67                         | APPL-14-002012 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.68                         | APPL-14-002013 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.69                         | APPL-14-002014 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.70                         | APPL-14-002015 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.71                         | APPL-14-002016 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.72                         | APPL-14-002017 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.73                         | APPL-14-002020 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.74                         | APPL-14-002021 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.75                         | APPL-14-002022 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.76                         | APPL-14-002035 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.77                         | APPL-14-002036 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.78                         | APPL-14-002037 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.79                         | APPL-14-002038 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.80                         | APPL-14-002039 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.81                         | APPL-14-002040 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                         | Set Correctly            |                          |
|------------------------------|-------------------------|--------------------------|--------------------------|
|                              |                         | Yes                      | No                       |
| 1.82                         | APPL-14-002041 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.83                         | APPL-14-002042 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.84                         | APPL-14-002043 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.85                         | APPL-14-002050 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.86                         | APPL-14-002051 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.87                         | APPL-14-002052 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.88                         | APPL-14-002053 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.89                         | APPL-14-002060 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.90                         | APPL-14-002062 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.91                         | APPL-14-002063 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.92                         | APPL-14-002064 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.93                         | APPL-14-002066 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.94                         | APPL-14-002068 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.95                         | APPL-14-002069 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.96                         | APPL-14-002080 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.97                         | APPL-14-002090 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.98                         | APPL-14-002100 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.99                         | APPL-14-002110 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.100                        | APPL-14-002120 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.101                        | APPL-14-002130 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.102                        | APPL-14-002140 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                         | Set Correctly            |                          |
|------------------------------|-------------------------|--------------------------|--------------------------|
|                              |                         | Yes                      | No                       |
| 1.103                        | APPL-14-002150 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.104                        | APPL-14-002160 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.105                        | APPL-14-002170 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.106                        | APPL-14-002180 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.107                        | APPL-14-002190 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.108                        | APPL-14-002200 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.109                        | APPL-14-002210 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.110                        | APPL-14-002220 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.111                        | APPL-14-002230 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.112                        | APPL-14-002240 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.113                        | APPL-14-002250 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.114                        | APPL-14-002260 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.115                        | APPL-14-002270 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.116                        | APPL-14-003001 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.117                        | APPL-14-003007 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.118                        | APPL-14-003008 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.119                        | APPL-14-003010 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.120                        | APPL-14-003011 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.121                        | APPL-14-003012 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.122                        | APPL-14-003013 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.123                        | APPL-14-003014 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                         | Set Correctly            |                          |
|------------------------------|-------------------------|--------------------------|--------------------------|
|                              |                         | Yes                      | No                       |
| 1.124                        | APPL-14-003020 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.125                        | APPL-14-003030 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.126                        | APPL-14-003050 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.127                        | APPL-14-003051 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.128                        | APPL-14-003052 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.129                        | APPL-14-003060 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.130                        | APPL-14-003070 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.131                        | APPL-14-003080 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.132                        | APPL-14-004001 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.133                        | APPL-14-004002 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.134                        | APPL-14-004022 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.135                        | APPL-14-004030 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.136                        | APPL-14-004040 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.137                        | APPL-14-004050 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.138                        | APPL-14-004060 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.139                        | APPL-14-005001 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.140                        | APPL-14-005020 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.141                        | APPL-14-005050 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.142                        | APPL-14-005052 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.143                        | APPL-14-005054 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.144                        | APPL-14-005055 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                         | Set Correctly            |                          |
|------------------------------|-------------------------|--------------------------|--------------------------|
|                              |                         | Yes                      | No                       |
| 1.145                        | APPL-14-005056 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.146                        | APPL-14-005058 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.147                        | APPL-14-005060 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.148                        | APPL-14-005061 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.149                        | APPL-14-005070 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.150                        | APPL-14-005080 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.151                        | APPL-14-005090 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.152                        | APPL-14-005100 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.153                        | APPL-14-005110 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.154                        | APPL-14-005120 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.155                        | APPL-14-005130 (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: Change History

| Date         | Version | Changes for this version |
|--------------|---------|--------------------------|
| Sep 10, 2025 | 1.0.0   | Initial CIS Release      |