

Guide to the Secure Configuration of Fedora

with profile `PCI-DSS v3.2.1 Control Baseline for Fedora`

— Ensures PCI-DSS v3.2.1 related security configuration settings are applied.

The SCAP Security Guide Project

<https://www.open-scap.org/security-policies/scap-security-guide>

This guide presents a catalog of security-relevant configuration settings for Fedora. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is available in the `scap-security-guide` package which is developed at <https://www.open-scap.org/security-policies/scap-security-guide>.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog*, *not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

| | |
|--------------------------|--|
| Evaluation target | Inanna. |
| Benchmark URL | <code>#scap_org.open-scap_comp_ssg-fedora-xccdf.xml</code> |
| Benchmark ID | <code>xccdf_org.ssgproject.content_benchmark_FEDORA</code> |
| Benchmark version | 0.1.75 |
| Profile ID | <code>xccdf_org.ssgproject.content_profile_pci-dss</code> |
| Started at | 2025-05-27T09:01:28-06:00 |
| Finished at | 2025-05-27T09:02:20-06:00 |
| Performed by | jeffrey |
| Test system | <code>cpe:/a:redhat:openscap:1.4.2</code> |

CPE Platforms

- `cpe:/o:fedoraproject:fedora:39`

- cpe:/o:fedoraproject:fedora:40
- cpe:/o:fedoraproject:fedora:41
- cpe:/o:fedoraproject:fedora:42
- cpe:/o:fedoraproject:fedora:43
- cpe:/o:fedoraproject:fedora:44
- cpe:/o:fedoraproject:fedora:45

Addresses

- IPv4 127.0.0.1
- IPv4 10.255.255.254
- IPv4 172.19.81.111
- IPv6 0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:215:5dff:fe85:4556
- MAC 00:00:00:00:00:00
- MAC 00:15:5D:85:45:56

Compliance and Scoring

The target system did not satisfy the conditions of 15 rules! Please review rule results and consider applying remediation.

Rule results

18 passed
15 failed
1 other

Severity of failed rules

0 other
1 low
12 medium
2 high

Score

| Scoring system | Score | Maximum | Percent |
|---------------------------|-----------|------------|---------|
| urn:xccdf:scoring:default | 46.875000 | 100.000000 | 46.88% |

Rule Overview

| Title | Severity | Result |
|--|----------|--------|
| Guide to the Secure Configuration of Fedora 15x fail 1x notchecked | | |
| System Settings 15x fail 1x notchecked | | |
| Installing and Maintaining Software 2x fail 1x notchecked | | |
| System and Software Integrity 1x fail | | |

| Title | Severity | Result |
|--|----------|---------------|
| Software Integrity Checking 1x fail | | |
| Verify Integrity with RPM 1x fail | | |
| Verify File Hashes with RPM | high | pass |
| Verify and Correct File Permissions with RPM | high | fail |
| Verify Integrity with AIDE | | |
| System Cryptographic Policies | | |
| Endpoint Protection Software | | |
| GNOME Desktop Environment | | |
| Updating Software 1x fail 1x notchecked | | |
| Ensure Fedora GPG Key Installed | high | fail |
| Ensure gpgcheck Enabled In Main dnf Configuration | high | notapplicable |
| Ensure gpgcheck Enabled for All dnf Package Repositories | high | pass |
| Ensure Software Patches Installed | medium | notchecked |
| Account and Access Control 12x fail | | |
| Protect Accounts by Configuring PAM 10x fail | | |
| Set Lockouts for Failed Password Attempts 3x fail | | |
| Limit Password Reuse | medium | fail |
| Lock Accounts After Failed Password Attempts | medium | fail |
| Set Lockout Time for Failed Password Attempts | medium | fail |
| Set Password Quality Requirements 4x fail | | |
| Set Password Quality Requirements with pam_pwquality 4x fail | | |
| Ensure PAM Enforces Password Requirements - Minimum Digit Characters | medium | fail |
| Ensure PAM Enforces Password Requirements - Minimum Lowercase Characters | medium | fail |
| Ensure PAM Enforces Password Requirements - Minimum Length | medium | fail |
| Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters | medium | fail |
| Set Password Hashing Algorithm 2x fail | | |
| Set Password Hashing Algorithm in /etc/libuser.conf | medium | notapplicable |

| Title | Severity | Result |
|---|----------|--------|
| Set Password Hashing Algorithm in /etc/login.defs | medium | fail |
| Set PAM's Password Hashing Algorithm | medium | fail |
| Ensure PAM Displays Last Logon/Access Notification | low | fail |
| Protect Physical Console Access | | |
| Protect Accounts by Restricting Password-Based Login 2x fail | | |
| Set Account Expiration Parameters 1x fail | | |
| Set Account Expiration Following Inactivity | medium | fail |
| Ensure All Accounts on the System Have Unique Names | medium | pass |
| Set Password Expiration Parameters 1x fail | | |
| Set Password Maximum Age | medium | fail |
| Verify Proper Storage and Existence of Password Hashes | | |
| GRUB2 bootloader configuration | | |
| Configure Syslog | | |
| Network Configuration and Firewalls 1x fail | | |
| IPSec Support 1x fail | | |
| Install libreswan Package | medium | fail |
| File Permissions and Masks | | |
| Services | | |
| System Accounting with auditd | | |

Red Hat and Red Hat Enterprise Linux are either registered trademarks or trademarks of Red Hat, Inc. in the United States and other countries. All other names are registered trademarks or trademarks of their respective companies.