Guide to the Secure Configuration of Fedora

with profile Standard System Security Profile for Fedora
— This profile contains rules to ensure standard security baseline of a Fedora system.
Regardless of your system's workload all of these checks should pass.

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 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	#scap_org.open-scap_comp_ssg-fedora-xccdf.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_FEDORA
Benchmark version	0.1.75
Profile ID	xccdf_org.ssgproject.content_profile_standard
Started at	2025-05-27T19:00:58-06:00
Finished at	2025-05-27T19:07:39-06:00
Performed by	root
Test system	cpe:/a:redhat:openscap:1.4.2

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** 0:0:0:0:0:0:0:1
- **IPv6** fe80:0:0:0:215:5dff:fe85:45d4
- **MAC** 00:00:00:00:00:00
- **MAC** 00:15:5D:85:45:D4

Compliance and Scoring

The target system did not satisfy the conditions of 4 rules! Please review rule results and consider applying remediation.

Rule results

19 passed
4 failed
0 other

Severity of failed rules

0 other
1 low
2 medium
1 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	82.870369	100.000000	82.87%

Rule Overview

Title	Severity	Result
Guide to the Secure Configuration of Fedora **4x fail**		
System Settings **4x fail**		
Installing and Maintaining Software **1x fail**		

Title	Severity	Result
System and Software Integrity **1x fail**		
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		
Updating Software		
Account and Access Control **3x fail**		
Protect Accounts by Configuring PAM **1x fail**		
Ensure PAM Displays Last Logon/Access Notification	low	**fail**
Protect Accounts by Restricting Password-Based Login **2x fail**		
Set Account Expiration Parameters		
Set Password Expiration Parameters **2x fail**		
Set Password Maximum Age	medium	**fail**
Set Password Minimum Age	medium	**fail**
Set Password Warning Age	medium	**pass**
Verify Proper Storage and Existence of Password Hashes		
Restrict Root Logins		
Secure Session Configuration Files for Login Accounts		
Network Configuration and Firewalls		
File Permissions and Masks		
Services		
System Accounting with auditd		