

Guide to the Secure Configuration of Ubuntu 22.04

with profile CIS Ubuntu Linux 22.04 LTS Benchmark for Level 2 - Server

— This profile defines a baseline that aligns to the "Level 2 - Server" configuration from the Center for Internet Security® Ubuntu Linux 22.04 LTS Benchmark™, v2.0.0, released 2024-03-28.

This profile includes Center for Internet Security® Ubuntu Linux 22.04 LTS Benchmark™ content.

The SCAP Security Guide Project
<https://www.open-scap.org/security-policies/scap-security-guide> (<https://www.open-scap.org/security-policies/scap-security-guide>)
This guide presents a catalog of security-relevant configuration settings for Ubuntu 22.04. 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> (<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	pkrmvmjzamy0addc
Benchmark URL	/usr/share/xml/scap/ssg/content/content/build/ssg-ubuntu2204-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU_22-04
Profile ID	xccdf_org.ssgproject.content_profile_cis_level2_server
Started at	2025-09-23T00:31:58
Finished at	2025-09-23T00:33:01
Performed by	packer

CPE Platforms

- cpe:/o:canonical:ubuntu_linux:22.04::~lts~~~~

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.0.4
- IPv6 0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:7e1e:52ff:fe1b:24ef
- MAC 00:00:00:00:00:00
- MAC 7C:1E:52:1B:24:EF

Compliance and Scoring

The target system did not satisfy the conditions of 112 rules! Furthermore, the results of 31 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

223 passed

112 failed

31 other

Severity of failed rules

3

18 low

87 medium

4

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	44.819675	100.000000	44.82%

Rule Overview

Title	Severity	Result
Guide to the Secure Configuration of Ubuntu 22.04 112x fail 30x error 1x unknown		
System Settings 88x fail 10x error 1x unknown		
Installing and Maintaining Software 10x fail 5x error		
System and Software Integrity 4x fail		
Software Integrity Checking 4x fail		
Verify Integrity with AIDE 4x fail		
Install AIDE	medium	fail
Build and Test AIDE Database	medium	fail
Configure AIDE to Verify the Audit Tools	medium	fail
Configure Periodic Execution of AIDE	medium	fail
Package "prelink" Must not be Installed	medium	pass
Disk Partitioning 6x fail		
Ensure /dev/shm is configured	low	pass
Ensure /home Located On Separate Partition	low	fail
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail
Ensure /var/log Located On Separate Partition	low	fail
Ensure /var/log/audit Located On Separate Partition	low	fail
Ensure /var/tmp Located On Separate Partition	medium	fail
GNOME Desktop Environment		
Sudo 5x error		
Install sudo Package	medium	pass
Ensure Only Users Logged In To Real tty Can Execute Sudo - sudo use_ptty	medium	error
Ensure Sudo Logfile Exists - sudo logfile	low	error
Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate	medium	error
Ensure Users Re-Authenticate for Privilege Escalation - sudo	medium	error
Require Re-Authentication When Using the sudo Command	medium	error

Account and Access Control 22x fail 5x error		
Warning Banners for System Accesses		
Protect Accounts by Configuring PAM 12x fail		
Set Lockouts for Failed Password Attempts 8x fail		
Verify pam_pwhistory module is activated	medium	fail
Limit Password Reuse	medium	fail
Limit Password Reuse	medium	fail
Enforce Password History with use_authtok	medium	fail
Require use_authtok for pam_unix.so	medium	pass
Lock Accounts After Failed Password Attempts	medium	fail
Ensure pam_faillock module is enabled	medium	fail
Set Root Lockout Time for Failed Password Attempts	medium	fail
Set Lockout Time for Failed Password Attempts	medium	fail
Set Password Quality Requirements 1x fail		
Set Password Quality Requirements with pam_pwquality 1x fail		
Ensure PAM Enforces Password Requirements - Minimum Digit Characters	medium	notapplicable
Ensure PAM Enforces Password Requirements - Prevent the Use of Dictionary Words	medium	notapplicable
Ensure PAM Enforces Password Requirements - Minimum Different Characters	medium	notapplicable
Ensure PAM Enforces Password Requirements - Enforce for root User	medium	notapplicable
Ensure PAM Enforces Password Requirements - Enforcing	medium	notapplicable
Ensure PAM Enforces Password Requirements - Minimum Lowercase Characters	medium	notapplicable
Set Password Maximum Consecutive Repeating Characters	medium	notapplicable
Limit the maximum number of sequential characters in passwords	medium	notapplicable
Ensure PAM Enforces Password Requirements - Minimum Different Categories	medium	notapplicable
Ensure PAM Enforces Password Requirements - Minimum Length	medium	notapplicable
Ensure PAM Enforces Password Requirements - Minimum Special Characters	medium	notapplicable
Verify pam_pwquality module is activated	medium	fail
Ensure PAM Enforces Password Requirements - Minimum Uppercase Characters	medium	notapplicable
Set Password Hashing Algorithm		
Install pam-modules Package	medium	fail
Install pam_pwquality Package	medium	fail
Install pam-runtime Package	medium	fail
Verify pam_unix module is activated	medium	pass
Protect Accounts by Restricting Password-Based Login 6x fail 5x error		
Set Account Expiration Parameters 1x fail		
Set Account Expiration Following Inactivity	medium	fail
Ensure All Accounts on the System Have Unique Names	medium	pass
Ensure shadow Group is Empty	medium	pass

Set Password Expiration Parameters 2x fail 3x error		
Set Password Maximum Age	medium	fail
Set Password Minimum Age	medium	fail
Set Existing Passwords Maximum Age	medium	error
Set Existing Passwords Minimum Age	medium	error
Set Password Warning Age	medium	pass
Set existing passwords a period of inactivity before they been locked	medium	error
Verify Proper Storage and Existence of Password Hashes 1x fail 1x error		
Verify All Account Password Hashes are Shadowed	medium	pass
Ensure all users last password change date is in the past	medium	pass
Avoid using remember in pam_unix module	medium	pass
All GIDs referenced in /etc/passwd must be defined in /etc/group	low	pass
Ensure There Are No Accounts With Blank or Null Passwords	high	error
Prevent Login to Accounts With Empty Password	high	fail
Verify No .forward Files Exist	medium	pass
Verify No netrc Files Exist	medium	pass
Restrict Root Logins 2x fail 1x error		
Verify Only Root Has UID 0	high	pass
Verify Root Has A Primary GID 0	high	pass
Ensure the Group Used by pam_wheel.so Module Exists on System and is Empty	medium	fail
Ensure root account access is controlled	medium	error
Verify Only Group Root Has GID 0	high	pass
Verify Non-Interactive Accounts Are Locked	medium	pass
Ensure that System Accounts Do Not Run a Shell Upon Login	medium	pass
Enforce Usage of pam_wheel with Group Parameter for su Authentication	medium	fail
Ensure All Accounts on the System Have Unique User IDs	medium	pass
Ensure All Groups on the System Have Unique Group ID	medium	pass
Ensure All Groups on the System Have Unique Group Names	medium	pass
Ensure nologin Shell is Not Listed in /etc/shells	medium	pass
Secure Session Configuration Files for Login Accounts 4x fail		
Ensure that No Dangerous Directories Exist in Root's Path		
Ensure that Users Have Sensible Umask Values 3x fail		
Ensure the Default Bash Umask is Set Correctly	medium	fail
Ensure the Default Umask is Set Correctly in login.defs	medium	fail
Ensure the Default Umask is Set Correctly in /etc/profile	medium	fail
Ensure the Root Bash Umask is Set Correctly	medium	pass
Set Interactive Session Timeout	medium	fail
User Initialization Files Must Be Group-Owned By The Primary Group	medium	pass

User Initialization Files Must Be Owned By the Primary User	medium	pass
All Interactive Users Home Directories Must Exist	medium	pass
All Interactive User Home Directories Must Be Group-Owned By The Primary Group	medium	pass
All Interactive User Home Directories Must Be Owned By The Primary User	medium	pass
Ensure User Bash History File Has Correct Permissions	medium	pass
Ensure All User Initialization Files Have Mode 0740 Or Less Permissive	medium	pass
All Interactive User Home Directories Must Have mode 0750 Or Less Permissive	medium	pass
AppArmor 3x fail 1x unknown		
Ensure AppArmor Utils is installed	medium	fail
Ensure AppArmor is installed	medium	pass
Enforce all AppArmor Profiles	medium	fail
All AppArmor Profiles are in enforce or complain mode	medium	unknown
Ensure AppArmor is enabled in the bootloader configuration	medium	fail
GRUB2 bootloader configuration 3x fail		
Non-UEFI GRUB2 bootloader configuration 2x fail		
Verify /boot/grub/grub.cfg User Ownership	medium	pass
Verify /boot/grub/grub.cfg Permissions	medium	fail
Set Boot Loader Password in grub2	high	fail
UEFI GRUB2 bootloader configuration 1x fail		
Set the UEFI Boot Loader Password	high	fail
ziPL bootloader configuration		
Configure Syslog 1x fail		
systemd-journald 1x fail		
Install systemd-journal-remote Package	medium	notapplicable
Enable systemd-journal-upload Service	medium	notapplicable
Enable systemd-journald Service	medium	pass
Ensure journald is configured to compress large log files	medium	notapplicable
Ensure journald ForwardToSyslog is disabled	medium	fail
Ensure journald is configured to write log files to persistent disk	medium	notapplicable
Disable systemd-journal-remote Socket	medium	pass
Configure systemd-journal-upload TLS parameters: ServerKeyFile, ServerCertificateFile and TrustedCertificateFile	medium	notapplicable
Configure systemd-journal-upload URL	medium	notapplicable
Network Configuration and Firewalls 34x fail		
iptables and ip6tables		
IPv6 7x fail		
Configure IPv6 Settings if Necessary 7x fail		
Configure Accepting Router Advertisements on All IPv6 Interfaces	medium	fail
Disable Accepting ICMP Redirects for All IPv6 Interfaces	medium	fail

Disable Kernel Parameter for Accepting Source-Routed Packets on all IPv6 Interfaces	medium	fail
Disable Kernel Parameter for IPv6 Forwarding	medium	fail
Disable Accepting Router Advertisements on all IPv6 Interfaces by Default	medium	fail
Disable Kernel Parameter for Accepting ICMP Redirects by Default on IPv6 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on IPv6 Interfaces by Default	medium	fail
Kernel Parameters Which Affect Networking 13x fail		
Network Related Kernel Runtime Parameters for Hosts and Routers 10x fail		
Disable Accepting ICMP Redirects for All IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on all IPv4 Interfaces	medium	fail
Enable Kernel Parameter to Log Martian Packets on all IPv4 Interfaces	unknown	fail
Enable Kernel Parameter to Use Reverse Path Filtering on all IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Secure ICMP Redirects on all IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting ICMP Redirects by Default on IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on IPv4 Interfaces by Default	medium	pass
Enable Kernel Parameter to Log Martian Packets on all IPv4 Interfaces by Default	unknown	fail
Enable Kernel Parameter to Use Reverse Path Filtering on all IPv4 Interfaces by Default	medium	fail
Configure Kernel Parameter for Accepting Secure Redirects By Default	medium	fail
Enable Kernel Parameter to Ignore ICMP Broadcast Echo Requests on IPv4 Interfaces	medium	pass
Enable Kernel Parameter to Ignore Bogus ICMP Error Responses on IPv4 Interfaces	unknown	pass
Enable Kernel Parameter to Use TCP Syncookies on Network Interfaces	medium	fail
Network Parameters for Hosts Only 3x fail		
Disable Kernel Parameter for Sending ICMP Redirects on all IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Sending ICMP Redirects on all IPv4 Interfaces by Default	medium	fail
Disable Kernel Parameter for IP Forwarding on IPv4 Interfaces	medium	fail
nftables 5x fail		
Install nftables Package	medium	notapplicable
Verify nftables Service is Enabled	medium	fail
Verify nftables Service is Disabled	medium	pass
Ensure nftables Default Deny Firewall Policy	medium	notapplicable
Ensure nftables Rules are Permanent	medium	fail
Ensure Base Chains Exist for Nftables	medium	fail
Set nftables Configuration for Loopback Traffic	medium	fail
Ensure a Table Exists for Nftables	medium	fail
Uncomplicated Firewall (ufw) 5x fail		
Install ufw Package	medium	pass
Remove ufw Package	medium	fail

Verify ufw Enabled	medium	pass <div>.....</div>
Verify ufw Active	medium	fail <div>.....</div>
Ensure ufw Default Deny Firewall Policy	medium	fail <div>.....</div>
Set UFW Loopback Traffic	medium	fail <div>.....</div>
Ensure ufw Firewall Rules Exist for All Open Ports	medium	fail <div>.....</div>
Uncommon Network Protocols 4x fail		
Disable DCCP Support	medium	fail <div>.....</div>
Disable RDS Support	low	fail <div>.....</div>
Disable SCTP Support	medium	fail <div>.....</div>
Disable TIPC Support	low	fail <div>.....</div>
Wireless Networking		
File Permissions and Masks 15x fail		
Verify Permissions on Important Files and Directories 1x fail		
Verify Permissions on Files with Local Account Information and Credentials		
Verify Permissions on Files within /var/log Directory		
Ensure No World-Writable Files Exist	medium	pass <div>.....</div>
Ensure All Files Are Owned by a Group	medium	pass <div>.....</div>
Ensure All Files Are Owned by a User	medium	pass <div>.....</div>
Verify permissions of log files	medium	fail <div>.....</div>
Restrict Dynamic Mounting and Unmounting of Filesystems 8x fail		
Remove autofs Package	low	pass <div>.....</div>
Disable the Automounter	medium	notapplicable <div>.....</div>
Disable Mounting of cramfs	low	fail <div>.....</div>
Disable Mounting of freevxfs	low	fail <div>.....</div>
Disable Mounting of hfs	low	fail <div>.....</div>
Disable Mounting of hfsplus	low	fail <div>.....</div>
Disable Mounting of jffs2	low	fail <div>.....</div>
Disable Mounting of squashfs	low	fail <div>.....</div>
Disable Mounting of udf	low	fail <div>.....</div>
Disable Modprobe Loading of USB Storage Driver	medium	fail <div>.....</div>
Restrict Partition Mount Options 3x fail		
Add nodev Option to /dev/shm	medium	fail <div>.....</div>
Add noexec Option to /dev/shm	medium	fail <div>.....</div>
Add nosuid Option to /dev/shm	medium	fail <div>.....</div>
Add nodev Option to /home	unknown	notapplicable <div>.....</div>
Add nosuid Option to /home	medium	notapplicable <div>.....</div>
Add nodev Option to /tmp	medium	notapplicable <div>.....</div>
Add noexec Option to /tmp	medium	notapplicable <div>.....</div>

Add nosuid Option to /tmp	medium	notapplicable
Add nodev Option to /var/log/audit	medium	notapplicable
Add noexec Option to /var/log/audit	medium	notapplicable
Add nosuid Option to /var/log/audit	medium	notapplicable
Add nodev Option to /var/log	medium	notapplicable
Add noexec Option to /var/log	medium	notapplicable
Add nosuid Option to /var/log	medium	notapplicable
Add nodev Option to /var	medium	notapplicable
Add nosuid Option to /var	medium	notapplicable
Add nodev Option to /var/tmp	medium	notapplicable
Add noexec Option to /var/tmp	medium	notapplicable
Add nosuid Option to /var/tmp	medium	notapplicable
Restrict Programs from Dangerous Execution Patterns 3x fail		
Disable Core Dumps 2x fail		
Disable Core Dumps for All Users	medium	fail
Disable Core Dumps for SUID programs	medium	fail
Enable ExecShield 1x fail		
Enable Randomized Layout of Virtual Address Space	medium	fail
Restrict usage of ptrace to descendant processes	medium	pass
Services 20x fail 20x error		
Apport Service 1x fail		
Disable Apport Service	unknown	fail
Avahi Server 2x fail		
Disable Avahi Server if Possible 2x fail		
Uninstall avahi Server Package	medium	fail
Disable Avahi Server Software	medium	fail
Cron and At Daemons 8x fail		
Restrict at and cron to Authorized Users if Necessary 2x fail		
Ensure that /etc/at.allow exists	medium	fail
Ensure that /etc/cron.allow exists	medium	fail
Ensure that /etc/cron.deny does not exist	medium	pass
Verify Group Who Owns /etc/at.allow file	medium	pass
Verify Group Who Owns /etc/at.deny file	medium	pass
Verify Group Who Owns /etc/cron.allow file	medium	pass
Verify User Who Owns /etc/at.allow file	medium	pass
Verify User Who Owns /etc/at.deny file	medium	pass
Verify User Who Owns /etc/cron.allow file	medium	pass
Verify Permissions on /etc/at.allow file	medium	pass
Verify Permissions on /etc/at.deny file	medium	pass

Verify Permissions on /etc/cron.allow file	medium	pass
Install the cron service	medium	pass
Enable cron Service	medium	pass
Verify Group Who Owns cron.d	medium	pass
Verify Group Who Owns cron.daily	medium	pass
Verify Group Who Owns cron.hourly	medium	pass
Verify Group Who Owns cron.monthly	medium	pass
Verify Group Who Owns cron.weekly	medium	pass
Verify Group Who Owns Crontab	medium	pass
Verify Owner on cron.d	medium	pass
Verify Owner on cron.daily	medium	pass
Verify Owner on cron.hourly	medium	pass
Verify Owner on cron.monthly	medium	pass
Verify Owner on cron.weekly	medium	pass
Verify Owner on crontab	medium	pass
Verify Permissions on cron.d	medium	fail
Verify Permissions on cron.daily	medium	fail
Verify Permissions on cron.hourly	medium	fail
Verify Permissions on cron.monthly	medium	fail
Verify Permissions on cron.weekly	medium	fail
Verify Permissions on crontab	medium	fail
Deprecated services		
DHCP		
DNS Server		
FTP Server 1x fail		
Disable vsftpd if Possible		
Remove ftp Package	low	fail
Web Server		
IMAP and POP3 Server		
LDAP		
Mail Server Software		
NFS and RPC		
Network Time Protocol 4x fail		
The Chrony package is installed	medium	pass
Install the systemd_timesyncd Service	high	fail
The Chronyd service is enabled	medium	pass
Enable systemd_timesyncd Service	high	notapplicable
The Chronyd service is disabled	medium	fail

Disable systemd_timesyncd Service	medium	notapplicable
Chrony Configure Pool and Server	medium	fail
Ensure that chronyd is running under chrony user account	medium	pass
Ensure a Single Time Synchronization Service is in Use	medium	pass
Configure Systemd Timesyncd Servers	medium	fail
Obsolete Services 2x fail		
Xinetd		
NIS		
Rlogin, Rsh, and Rexec		
Chat/Messaging Services		
Telnet 1x fail		
Remove telnet Clients	low	fail
TFTP Server		
Uninstall rsync Package	medium	fail
Ensure rsyncd service is disabled	medium	pass
Print Support		
Proxy Server		
Samba(SMB) Microsoft Windows File Sharing Server		
SNMP Server		
SSH Server 1x fail 20x error		
Configure OpenSSH Server if Necessary 20x error		
Set SSH Client Alive Count Max	medium	error
Set SSH Client Alive Interval	medium	error
Disable Host-Based Authentication	medium	error
Disable SSH Access via Empty Passwords	high	error
Disable SSH Forwarding	medium	error
Disable GSSAPI Authentication	medium	error
Disable SSH Support for .rhosts Files	medium	error
Disable SSH Root Login	medium	error
Do Not Allow SSH Environment Options	medium	error
Enable PAM	medium	error
Enable SSH Warning Banner	medium	error
Limit Users' SSH Access	unknown	error
Ensure SSH LoginGraceTime is configured	medium	error
Set LogLevel to INFO	low	error
Set SSH authentication attempt limit	medium	error
Set SSH MaxSessions limit	medium	error
Ensure SSH MaxStartups is configured	medium	error

Use Only Strong Ciphers	medium	error
Use Only Strong Key Exchange algorithms	medium	error
Use Only Strong MACs	medium	error
Verify Group Who Owns SSH Server config file	medium	pass
Verify Owner on SSH Server config file	medium	pass
Verify Permissions on SSH Server config file	medium	fail
Verify Permissions on SSH Server Private *_key Key Files	medium	pass
Verify Permissions on SSH Server Public *.pub Key Files	medium	pass
X Window System 1x fail		
Disable X Windows 1x fail		
Remove the X Windows Package Group	medium	fail
System Accounting with auditd 4x fail		
Configure auditd Rules for Comprehensive Auditing		
Configure auditd Data Retention		
System Accounting with auditd		
Ensure the default plugins for the audit dispatcher are Installed	medium	fail
Ensure the audit Subsystem is Installed	medium	fail
Enable auditd Service	medium	notapplicable
Enable Auditing for Processes Which Start Prior to the Audit Daemon	low	fail
Extend Audit Backlog Limit for the Audit Daemon	low	fail

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.