



Overview of Operating Systems Security Features - LINUX

Introduction A key advantage of LINUX desktop operating system (OS) is its low cost and ease of customization to environment and/or solutions specific requirements, but this can also present security risks. A LINUX desktop that is part of the GC network environment may be compromised by malicious software (malware) or other threats that could spread through GC networks. Unsecure installation of the LINUX desktop OS could either expose stored GC information to unauthorized personnel or make critical information unavailable. For these reasons, departments should ensure that all LINUX desktop OS systems are configured and used securely.

Life Cycle Security should be addressed in each phase of an OS's life cycle: evaluation, configuration, deployment, management and decommissioning.

Working Environments LINUX OS security controls can vary based on the intended use. Typical end-uses include: Dedicated Production GC office desktops (most secure), development GC Office desktops (moderately secure), and mobile desktops (least secure) such as reception desks, conference rooms, and printing areas.

Basic Security Recommendations

Identification and Authentication – Current implementations of Linux are vulnerable through user passwords. Passwords are stored in clear text, meaning they are easily understood by any user that knows the password file location, and the default encryption tool for information does not meet the Government of Canada recommended encryption requirements. Departments are recommended to identify and use an alternative encryption tool that meets or exceeds Government of Canada requirements.

Authorization – Restrict access to administration tools and where possible remove extra default permissions for services and tools.

Access Control – Restrict access to the internal firewall system configuration, disallow remote "root" login, lockdown system accounts, review enabled service and scheduler security, and for systems that are running web services, harden web security.

Confidentiality – Ensure all accounts are protected by a password that meets departmental security requirements.

Integrity – Use up-to-date patch management, ensure systems have anti virus and malware protection, and disable automatic downloads.

Availability – Using partitioning software to create sections of the hard drive allows administrators to lock down access and enforce strict lock down on the startup services.

Accountability and Non-Repudiation –Purge unnecessary accounts, enable logging to start automatically on boot. Implement secure log files storage and enable time synchronization with a secure authorized time source.

Security Profile	Working Environment
Least Dangerous (Most Secure)	GC Production Desktops
Moderately Dangerous (Moderately Secure)	GC Development Desktops
More Dangerous (Less Secure)	Shared Desktops
Most Dangerous (Least Secure)	Mobile Desktops