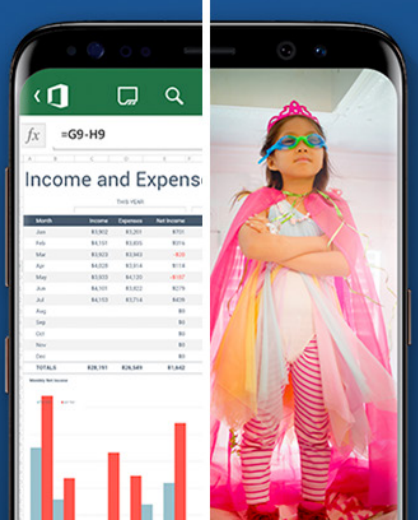
SAMSUNG Knox

Workspace



Work more productively

Modern mobile devices help us work more productively. A key feature that enables us to be productive is sharing information.

However, when we share private information, we introduce the possibility of malicious or accidental disclosure. So how do we isolate our private data while still maintaining productivity?

Secure Information

Knox Workspace encrypts your work data and isolates it from your personal data using a custom version of Security Enhancements for Android.

SE for Android is in charge of enforcing standard rules provided by Android and Knox security rules. Every time an application asks for resources, these security enhancements prohibit the exchange of data with applications that are outside of the workspace.

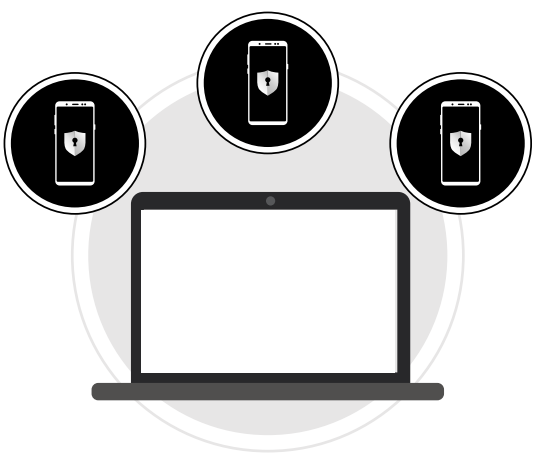
Encrypted Data

All data within Workspace is encrypted when Workspace is locked. The data can be decrypted when a user unlocks Knox Workspace using their iris, fingerprint, password, pattern, or pin.

If Knox detects that device integrity has been compromised, Knox Workspace data cannot be decrypted.

Mobile Device Management

In addition to data isolation and encryption, IT Admins can apply policies using Mobile Device Management software. IT Admins can configure policies to control device behaviors including password rules, geofencing, and sharing restrictions. Knox Workspace can be managed remotely without intruding on personal data.



Maximize Productivity

Knox Workspace protects your information while still maximizing productivity. Your sensitive data is kept isolated and encrypted while still being convenient to access and manage.

Check out our videos to learn more about Knox features

Multi-layered security

Real-time protection

Hardware-based encryption

Worldwide certification