



Transparent data protection for smartphones and tablets.

Dell Data Protection | Mobile Edition

Today employees, partners and vendors alike work any time, anywhere, using any device to download and share files. Personally owned smartphones and tablets, like desktops and laptops, have become a standard work tool. Accordingly, most organizations are embracing the bring your own device movement, recognizing it helps to both reduce equipment costs and increase productivity.

But without proper encryption and password enforcement, data accessed on mobile devices, whether from a corporate server or a public cloud, is unprotected. If the device is lost or stolen, or if data is accessed through an open wireless hotspot, it could be hijacked, putting companies in jeopardy of a security breach and compliance violations. IT teams are struggling to strike a balance between protecting data and impeding worker productivity by restricting data access.

Dell Data Protection | Mobile Edition helps to put IT back in control of data security by enabling you to protect data accessed on smartphones and tablets running iOS or Android operating systems. Agentless and easy to deploy, the solution is fully integrated with the Dell Data Protection | Enterprise Edition platform. Through Dell Data Protection | Mobile Edition, IT can easily inspect, install, or remove profiles, remove passcodes and conduct remote wipes, all from a single platform.

Comprehensive protection for enhanced end user productivity

By using the native security features available on iOS and Android platforms, Dell Data Protection | Mobile Edition reduces the need for additional security software on the device, simplifying support and enabling easy on-boarding with less impact to the end user experience. Automatic association of devices with users further minimizes disruption to workflow.

Secure iOS Devices

Dell Data Protection | Mobile Edition enables administrators to enforce policies at the user level and commands at the device level. Device management commands are sent to managed iPhone and iPad devices via the Apple Push Notification Service (APNS). Policies, restrictions and commands are implemented in iOS as a configuration profile, which are deployed over-the-air.

Secure Android Devices

Managed through the Microsoft Exchange ActiveSync (EAS) protocol, Android mobile device protection lets you set and enforce policies at the user level and commands at the device level. Device management commands are sent and enforced on Android devices via Exchange ActiveSync. Allow, block and remote wipe commands are deployed over-the-air.

iOS-Only Policies	
Grace period before device locks	Force iTunes password
Reset passcode	Allow untrusted https certs
Remote lock	Allow iCloud backup
Allow removal passcode	Allow iCloud document sync
Configuration profile removal by user	Allow iCloud key value sync
Allow YouTube	Allow iCloud photo stream
Allow iTunes	Web Payload - web clip URL
Allow installing apps	Web Payload - web clip label
Allow explicit content	Web Payload - web clip icon
Allow screen capture	Web Payload - allow web clip removal
Allow assistant (Siri)	
Shared iOS and EAS Policies	
Require passcode	Disable camera
Allow simple passcode	Allow browser
Number of complex characters	Minimum passcode length
Maximum passcode age	Require alphanumeric passcode
Number of unique passcodes before reuse	Inactivity period before device locks
Number of failed attempts before device wipes	
EAS-Only Policies	
Encrypt storage card	
Require device encryption	



Simplified management and compliance

Because Dell Data Protection | Mobile Edition is centrally managed using a single console, it helps to increase IT visibility and control, greatly reducing the compliance workload and the risk of a data breach. You can easily set policies and restrictions across the enterprise, and immediately execute commands like Remote Wipe, so you can quickly respond to and limit the scope of a data leak. Furthermore, automatic discovery of unenrolled devices and centralized management and reporting helps keep corporate data secure while enabling users to work uninterrupted.

Dell Data Protection | Mobile Edition enables you to:

- Set Policies and Restrictions - Set policies across the enterprise, such as requiring a PIN or disabling backups
- Execute Commands - Quickly issue commands, such as Remote Wipe and Reset Passcode
- Discover Devices - Automatically detect unenrolled devices
- Block Devices - Remove a device's access to Exchange server if it is lost or stolen, or must be deprovisioned
- Compile Compliance Reports - Compile compliance reports and meet auditor requirements

Protect cloud storage data

The pervasiveness of file sharing on public clouds makes it imperative to protect mobile devices as well, since end users commonly access cloud files via smartphones and tablets. Dell Data Protection | Mobile Edition was designed to work in tandem with Dell Data Protection | Cloud Edition, which transparently encrypts data as it moves into and out of public cloud storage. When used together, the solutions work seamlessly to allow end users to use public clouds as they always have, without interruption, while enabling companies to ensure their sensitive data stays secure and compliant.

Dell Data Protection | Enterprise Edition

Dell Data Protection | Mobile Edition is part of an integrated platform, Dell Data Protection | Enterprise Edition, which secures data across all physical and virtual endpoints, including:

- Desktops and laptops
- Smartphones and tablets
- Removable media
- Public and private clouds
- Self-encrypting drives
- BitLocker

Simple to install and easy to maintain, Dell Data Protection | Enterprise Edition is helping to protect data wherever it goes.

Technical Specifications

Supported operating systems:

- iOS 4.x, iOS 5.x, iOS 6 and later
- Android 2.2, 2.3 and later, 3.x and 4.0 and later

Supported devices:

- iPhones and iPads
- Android smartphones and Android tablets

Supported Exchange ActiveSync Servers:

- Exchange ActiveSync 12.0 – component of Exchange Server 2007
- Exchange ActiveSync 12.1 – component of Exchange Server 2007 SP1
- Exchange ActiveSync 14.0 – component of Exchange Server 2010
- Exchange ActiveSync 14.1 – component of Exchange Server 2010 SP1

Learn more at www.Dell.com/DataProtection