



The AbsoluteSafe app is available with Absolute Manage MDM, allowing you to manage and secure the mobile devices in your deployment:

Intelligent

Track and locate unauthorized apps. Block non-compliant devices from accessing the network. Control how and when users connect with sensitive corporate data.

Automated

Efficiently manage all of your in-house custom apps. Automate time-consuming configuration and profile work.

Cross-Platform

Provide IT administrators with a choice of a Mac or PC interface to manage mobile devices.

Absolute[®]

MANAGE

AbsoluteSafe is an app available with Absolute Manage Mobile Device Management (MDM). It enables IT administrators to securely distribute sensitive or confidential files to iOS devices (iPad, iPhone, iPod touch) without using email.

Along with a secure media transfer, IT administrators can restrict the files from being emailed, printed, or moved outside of AbsoluteSafe and files can be password protected so that users must enter a password before they can access the files. There is no other technology available today that can provide such granular control and security over corporate data.

Data Encryption vs Data Removal

Many products rely on iOS hardware encryption to secure corporate data. If the device is at risk, lost, or stolen – or if it is employee-owned and the employee is leaving the organization – the IT administrator will remove the provisioning profile or configuration profile to block access to the associated data. However, this does not automatically delete the data. Instead it is locked behind the iOS hardware encryption, and is still vulnerable if the device is jailbroken.

AbsoluteSafe provides a more comprehensive data security option. When an IT administrator transfers documents or media to a managed device, it is controlled with a new Media policy, providing the following options:

- **If a file is removed from the Media Policy:** AbsoluteSafe will delete the file from all devices assigned to the policy
- **If the device is removed from the Media Policy:** AbsoluteSafe will delete all files from the device that are assigned to that policy

Data Control

With AbsoluteSafe IT administrators are able to designate levels of access to files and media. If the data is not confidential, they can permit it to be shared outside of AbsoluteSafe.

To completely lock down corporate files and documents in AbsoluteSafe, IT administrators can create a secure policy. This allows them to define a specific window of time when the documents will be available to the user, such as for the duration of a confidential meeting. Once the time expires, the documents are automatically removed from AbsoluteSafe and are no longer available to the end user.

Files may be opened and viewed within AbsoluteSafe using iOS native readers, which can handle multiple file formats, including common MS Office formats, PDFs and the following:

- Images (.jpeg, .png, .gif, .tiff)
- PDF (.pdf)
- Powerpoint (.ppt)
- Word (.doc)
- Rich Text Format (.rtf)
- Rich Text Format Directory (.rtfd)
- Excel (.xls)
- Keynote (.key)
- Numbers (.numbers)
- Pages (.pages)
- Keynote '09 (.key)
- Numbers '09 (.numbers)
- Pages '09 (.pages)
- 3GPP media (.3gp, .3gpp)
- 3GPP2 media (.3g2, .3gp2)
- AIFF audio (.aiff, .aif, .aifc, .cdda)
- AMR audio (.amr)
- MP3 audio (.mp3, .swa)
- MPEG-4 media (.mp4)
- MPEG audio (.mpeg, .mpg, .mp3, .swa)
- WAVE audio (.wav, .bwf)
- AAC audio (.m4a)
- AAC audio book (.m4b, .m4p)
- QuickTime Movie (.mov, .qt, .mqv)
- Video (.m4v)