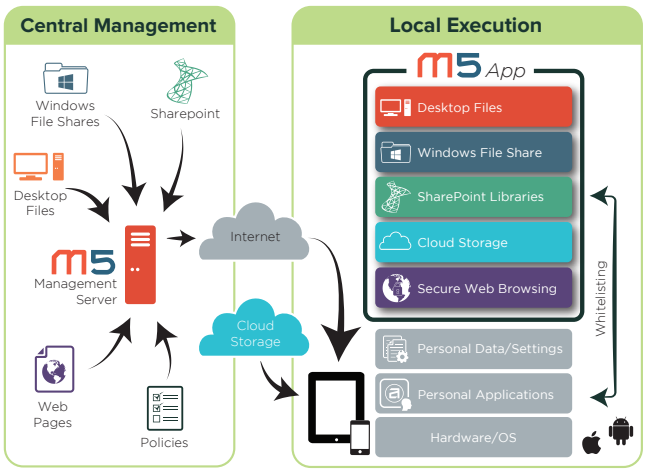
Secure Access and Document Delivery for iOS Devices

Today, business happens wherever your employees happen to be. To be effective and productive, your users must consume their critical corporate data on the go: using their mobile devices they expect access to the same data they have on their PCs including PDFs, Microsoft Office docs, or any number of other data formats. M5 LiveData allows them to be connected to their corporate information at all times – working offline or securely online without the need for a VPN client.

M5 is the only iOS solution that offers you enterprise-class security and management, offline use, and an intuitive native interface for accessing local, SharePoint and Intranet files without needing a VPN. Here's how it works:

M5 LiveData Architecture



Users download the M5 LiveData app from the Apple AppStore and connect to corporate resources with the credentials you provide them from inside the secure LiveData container. Administrators set policies and white list access to authorized resources from the management console.

LiveData In Action

Here are just a few examples of how Moka5 customers are using LiveData today:

- Providing physicians with secure access to patient records from their iOS devices
- Electronically distributing confidential corporate boarding meeting materials to authorized individuals
- Remotely provisioning and de-provisioning access for contractors, independent agents, and remote employees
- Helping teachers connect to student grading portals from home
- Giving mobile professionals access to corporate file shares, network resources, and data from M5 LivePCs that have been backed up to the cloud or corporate network location

LiveData Capabilities

M5 LiveData extends data continuity by giving your mobile workforce secure access to corporate network resources and file shares from their iOS devices. A policy-enforced container, LiveData operates on personal (or corporate-owned) iOS devices and allows IT to manage the container without sacrificing user's privacy and control of their mobile devices.

Local execution. With LiveData, users can securely view files, including desktop files, Windows File Shares, SharePoint, and internal web pages, from their iPad and iPhone, and even cache them locally for offline use.

Strong security. Key protection features include:

- Active Directory (AD) integration for user authentication
- Existing AD access permissions determine individual users' access to Windows file shares
- Moka5 ticketing authentication mechanism ensures that only authorized devices can connect to internal network resources
- Securely browse internal web apps without a VPN client on an iOS device
- Remotely revoke or wipe LiveData on a lost or stolen iOS device
- Encrypted network traffic (sent as http over SSL) prevents man-in-the-middle attacks
- Encrypted data on local storage – secure data using AES-128 encryption

Policy-enforcement. More than 130 management and security policies on a single, unified platform, including if or how data can be shared outside the LiveData container.

- Data restrictions: restrictions on copying, sending or receiving corporate files to and from external apps, or attaching files to email
- “Whitelisting” gives IT the ability to allow interaction between the secure container and permitted external apps on the iOS device
- Passcode Lock Settings: enforce passcode history, passcode complexity, and passcode change frequency
- Security Settings: set offline lease time (suspend) or offline auto-kill time (secure wipe) if the LiveData container fails to communicate with the Management Server
- Control *Favorites* and *Trusted Sites* for secure web browsing

Data segregation with layering. Separation of corporate data and internal web apps from personal data, settings, and apps.

Self-service provisioning. Users can easily download LiveData from the Apple App Store.