GroupLogic

Enterprise Security with mobilEcho

Enterprise Security from the Ground Up

When enterprise mobility strategies are discussed, security is usually one of the first topics on the table. So it should come as no surprise that mobilEcho, GroupLogic's Mobile File Management (MFM) product, was designed from the ground up to combine mobile file access with enterprise security. mobilEcho is the industry's first and only mobile MFM software for enterprise iPad users. mobilEcho enables enterprises to provide secure access to enterprise file servers for iPad users, eliminating the need for work-arounds and third-party mobile applications that compromise the security of corporate files and assets. Configurable and deployable across the enterprise within minutes, mobilEcho promotes efficient IT management while ensuring corporate security and compliance standards are met. Enterprise end-users of mobilEcho can access, browse, search and interact with corporate files as well as cache files for offline access, improving overall mobile worker productivity regardless of job function.

Specific to security, mobilEcho takes into consideration three critical components that need to be secured when remotely accessing files from corporate servers: the server itself, the network and the mobile client. In addition, the various stakeholders - the end-user, the IT administrator, and the security team - each have different requirements. mobilEcho addresses each of them independently and collectively. This document describes how mobilEcho enables simple, secure and managed mobile file access.

Security on the Server

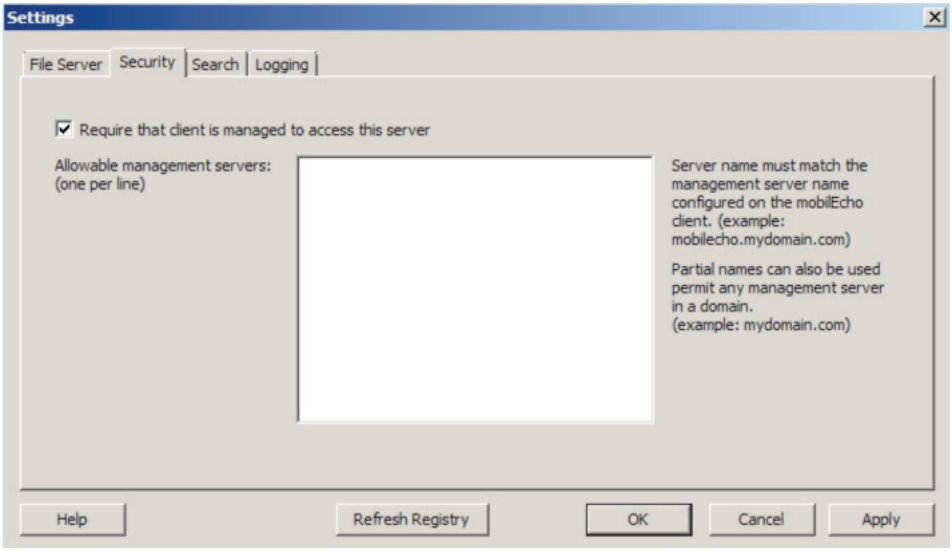
mobilEcho security starts on your corporate servers. Unlike consumer and cloud-based solutions for the iPad, mobilEcho allows the IT organization to stay in charge since your valuable business content and files remain on corporate-controlled servers. The mobilEcho server software runs on all editions of Windows 2003 and 2008 and integrates with capabilities of the existing environment. mobilEcho uses your established NTFS permissions to regulate file access and seamlessly integrates with Active Directory for user authentication and permissions. mobilEcho also includes the mobilEcho Client Management system, which allows the mobilEcho client application's capabilities and security settings to be remotely managed by IT, on a per-user or per-group basis.

When a user logs in from their mobilEcho iPad client, their encrypted credentials are sent across the network securely. File access is governed by your existing Active Directory permissions, and can optionally be restricted further with mobilEcho Client Management permissions and feature controls. For example, you could decide to allow read-only access to users in certain groups that may normally have full read/write access from their desktop. This restriction may be put in place to prevent iPad users from deleting files, for example.

You can also require users to have a mobilEcho Client Management profile to connect to the server. iPads with the mobilEcho client application installed, but that are not permitted by corporate IT with a Client Management profile, are denied access to your mobilEcho file servers. This ensures that all clients connecting to your servers are constrained by the policies that you have configured.

There are many additional options available to the administrator for controlling policies and access. See the Management Capabilities section for more information.

Figure 1: The server administrator can require that connected iPads be managed by a Mobile Device Management server



Security on the Network

mobilEcho ensures that all data transfer is secure between the server and the iPad. All mobilEcho traffic is sent end-to-end as encrypted HTTPS, so it's as secure as Internet banking. It doesn't matter whether your user is accessing a file server from the office, over 3G or from a public WIFI hotspot. The data is always encrypted and secure.

If you want to allow access from outside your firewall, there are several options:

1. Port 443 access: mobilEcho uses HTTPS for encrypted transport so it fits in naturally with common firewall rules allowing HTTPS traffic on port 443. If you allow port 443 access to your mobilEcho server, authorized iPad clients can connect while inside or outside of your firewall. mobilEcho can also be configured to use any other port you prefer.
2. VPN: iPads support VPN connections, so if you prefer to run all remote traffic through a VPN, mobilEcho supports that. Both the built in iOS VPN client and third-party VPN clients are supported. iOS management profiles can be applied directly or through Mobile Device Management (MDM) systems to configure the certificate-based iOS "VPN-on-demand" feature, for seamless access to mobilEcho servers and other corporate resources.
3. Reverse proxy server: If you have a reverse proxy server set up, iPad clients can connect without the need for an open firewall port or a VPN connection.

The mobilEcho Client Management system also has the ability to configure the client application to only allow connections to servers with valid X.509 SSL certificates.

Security on the iPad

mobilEcho security extends from server to network to iPad. On the iPad, multiple layers of security can protect your corporate files:

Login Password: To log into a mobilEcho server from the iPad application, a user must provide a valid username and password, which is authenticated through Active Directory or a local user account set up on the mobilEcho server. The login credentials are sent securely encrypted from the iPad application to the server and stored securely encrypted in the iOS keychain, if the saving of passwords is allowed by Client Management. Through mobilEcho Client Management, users can be required to log in once per server connection, once per application session, or credentials can be saved for all sessions.

App Password: The mobilEcho client application has a password lock option. It can be set to require a password every time mobilEcho is launched or after a certain number of minutes of inactivity. An App Password can be required through a mobilEcho Client Management profile.

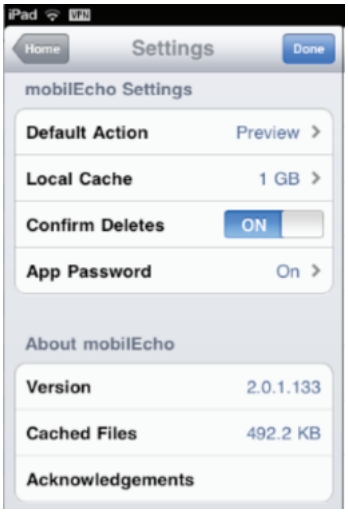
iPad Passcode: Setting a Passcode Lock on the iPad itself adds two more layers of security. First, it forces the user to enter a password to unlock the iPad, protecting the entire device. It also activates the iPad's Apple Data Protection file encryption capabilities.

Encryption on Device with Apple Data Protection: mobilEcho automatically uses Apple Data Protection (ADP) to encrypt all of mobilEcho's local files and settings. Apple Data Protection is available on iOS 4.0 and later and is enabled by setting an iOS device passcode. A device passcode can be required using an iOS configuration profile issued by the Apple iPhone Configuration Utility or by a Mobile Device Management (MDM) system. For more information about Apple Data Protection see http://support.apple.com/kb/HT4175. Note that devices upgraded from iOS 3 to iOS 4 require that a full restore be performed so that their file system can be upgraded to support Apple Data Protection.

Remote Management: Administrators can enforce the use of mobilEcho app passwords and iPad passcodes and other permissions through mobilEcho Client Management and iOS management profiles. See the Management Capabilities section for more information.

Remote Wipe: An administrator can selectively remote wipe the mobilEcho files and settings on an iPad the next time it tries to connect. This ensures all corporate data is destroyed and returns the app to an unmanaged state.

Figure 2: The iPad client can specify password and cache settings, or they can be enforced by the server.



Management Capabilities

mobilEcho Client Management provides comprehensive tools to allow administrators to set policies and permissions for mobile devices that access the server. These tools ensure IT has full control over mobile device access to corporate files.

Client Management options include:

- User profiles
- Group profiles
- Password policies
- Application-level file permission policies (view, edit, create, delete, rename)
- Application-level file distribution policies (allow emailing, printing, editing in other applications)
- Caching policy
- Assignment of servers displayed in the client application
- Remote application lock password reset
- Remote wipe capability

mobilEcho Client Management allows profiles to be assigned to Active Directory users or groups. Group profiles are assigned an order of precedence and a user is governed by the highest priority group profile they are a member of. In the case that a specific user needs a special set of capabilities, user profiles can be created and take precedence over group profiles, ensuring that the user gets the profile settings required.

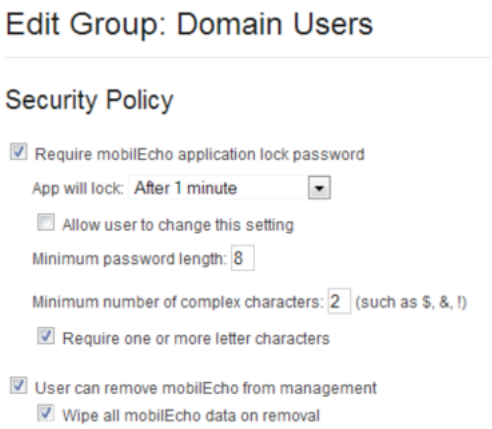
Once mobilEcho Client Management profiles have been established, users are configured for management by using their iPad to open a URL or attachment that is sent to them by IT. This action launches the mobilEcho application and directs it to the Client Management server. The user is prompted for their username and password, asked to set an application lock password if required, warned of any restrictions that will remove existing files from the device, and from that point on, the mobilEcho client application is managed by established management profile settings. Each time the mobilEcho client is started, it calls home to the Client Management server and is updated with any setting changes or assigned servers that have been added or removed from the profile.

As a complement to mobilEcho Client Management, administrators can also use a Mobile Device Management (MDM) system to enforce iOS level policies for corporate iPads. For example, you can require the use of an iOS Passcode Lock through an iPad Configuration Profile set up through an MDM server. The profile can also be configured to require that any iPad data backed up through iTunes will be encrypted on the computer. For more information about Mobile Device Management, see http://www.apple.com/ipad/business/integration/mdm.

Management Options

The screen shots below illustrate some of the management options available with mobilEcho.

Figure 3: The IT administrator can require the use of mobilEcho application lock passwords through a profile setting on the mobilEcho Client Management server. When that option is enabled, users will be required to enter a mobilEcho app password when they start the mobilEcho application. If an application lock password is required, the user will not be able to disable the password from within the mobilEcho client app.



Through mobilEcho Client Management application settings, it is possible to restrict the capabilities of clients to fit your security requirements. Corporate files can be sandboxed into mobilEcho's securely encrypted storage by disabling the ability to email files, print, or open files in other iPad applications. The ability to store or cache files locally on the device can also be disabled completely, ensuring that sensitive files are never on the device if it is lost or stolen.

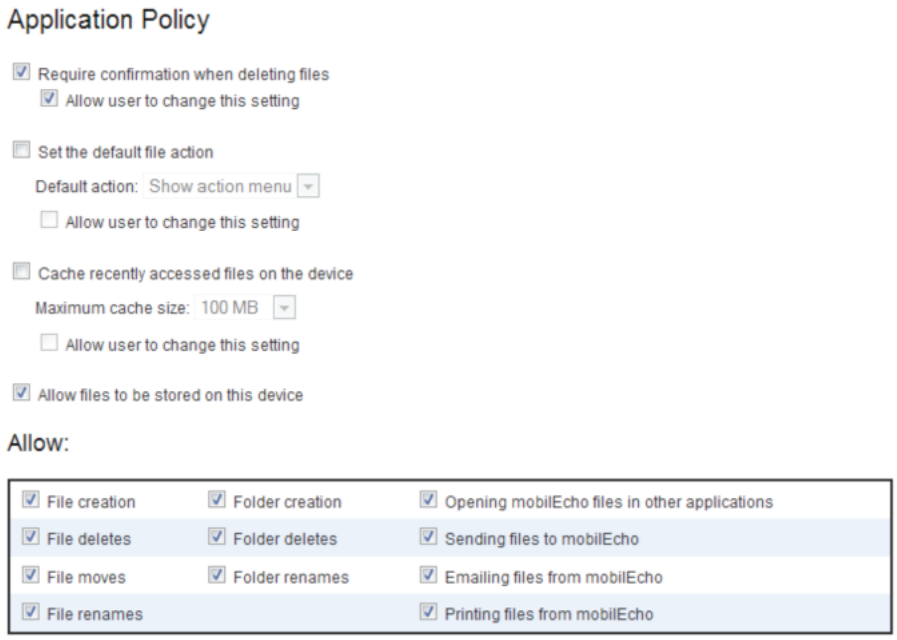
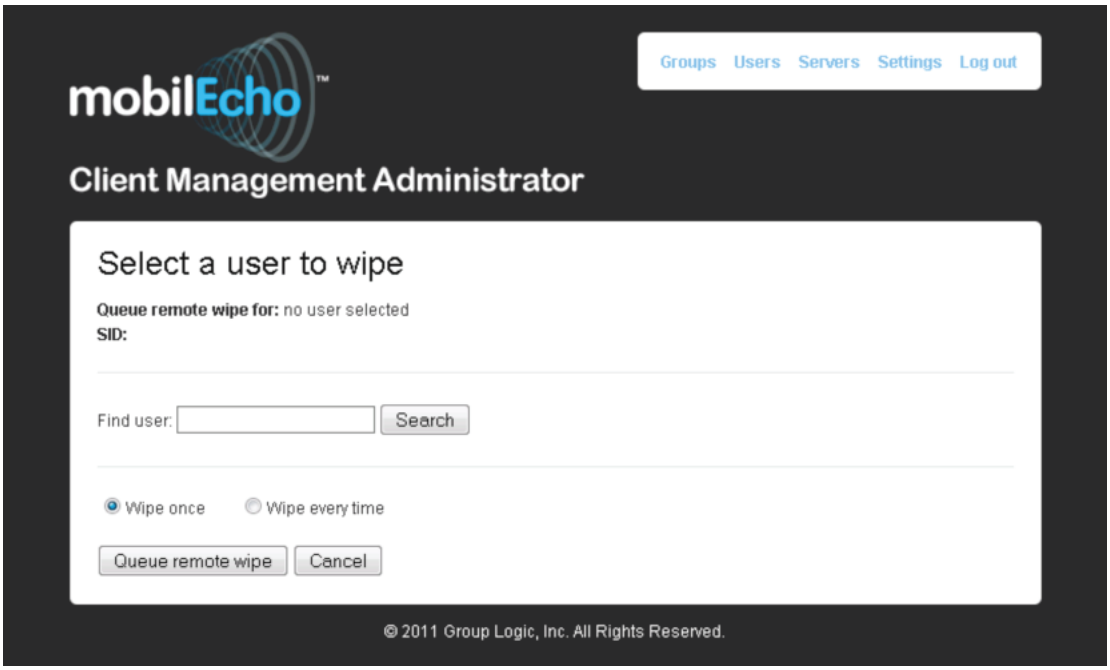
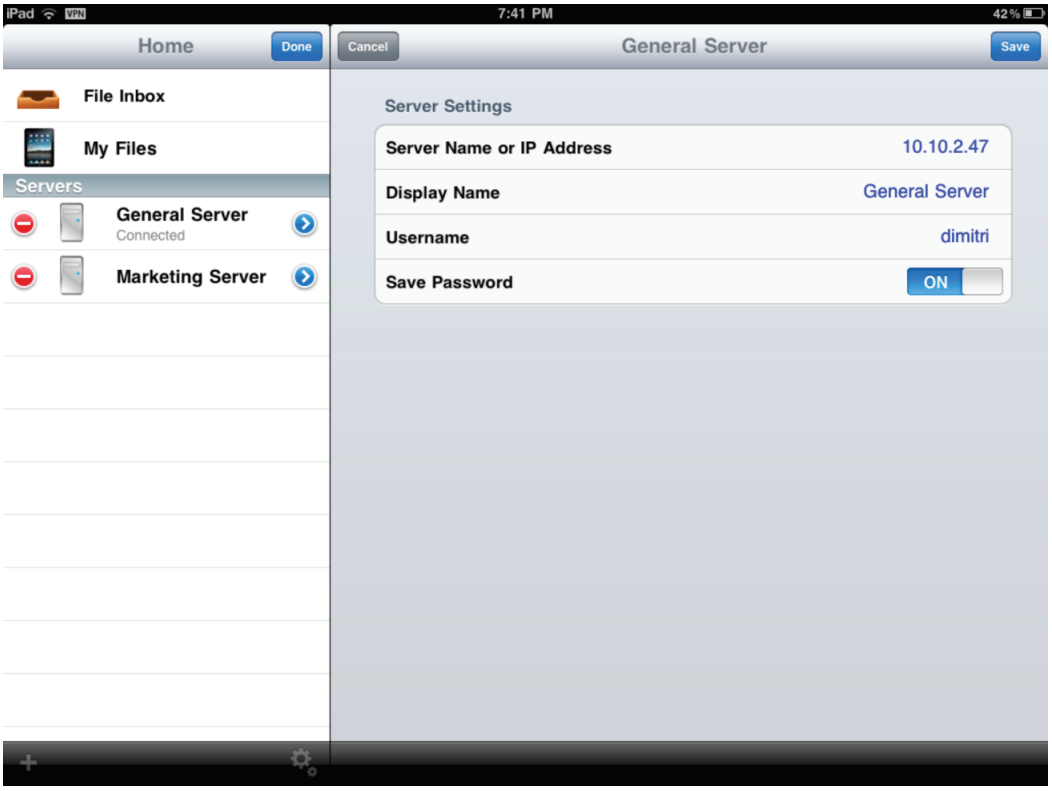
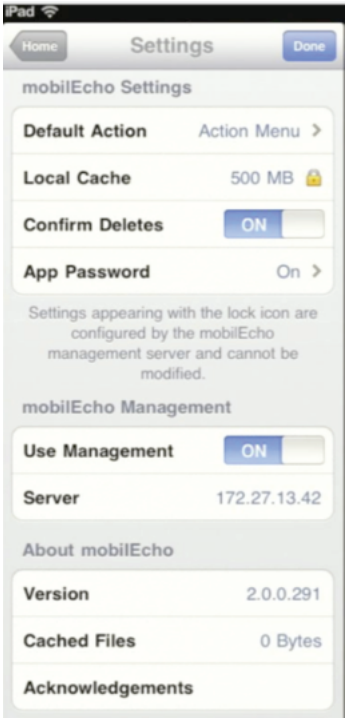


Figure 4: If an iPad is lost or stolen, the files on the iPad can be remotely wiped the next time a mobilEcho connection is established with the server. Remote wipes are accepted by the mobilEcho application before the application password is even entered. This ensures that a wipe will occur, even if the device is in the hands of someone who cannot log into the app.



Figures 5 and 6: Settings in the mobilEcho iPad app, such as the available servers, password requirements, and caching policy can be configured by the IT administrator in the client management profile. Servers assigned by client management are not editable by the user and these servers' names or IP addresses are hidden from the user. Users can also be optionally allowed to manually configure servers from the mobilEcho app.





About GroupLogic

GroupLogic® helps enterprise and education IT organizations simply and securely integrate diverse computing platforms into enterprise environments, connecting employees and students to enterprise files, content and assets to facilitate a more productive and efficient work environment. With more than two decades of experience, GroupLogic leads the marketplace in helping IT organizations effectively and easily manage the integration of Apple products into the enterprise ecosystem. Whether IT organizations are looking to integrate existing Apple assets, purchase additional Apple hardware like Macs and iPads, or want to take advantage of the hardware costs savings that accompany the adoption of IT consumerization, GroupLogic enables IT organizations to easily and securely manage the rapid integration of diverse platforms while ensuring resources are optimized. GroupLogic enables the enterprise to focus on what is really important – competitive differentiation, improved employee productivity, mitigated risk and reduced costs. GroupLogic's proven products—ExtremeZ-IP, ArchiveConnect, and MassTransit—are in use by some of the world's most innovative companies, including Christie's, International Greetings and Omnicom Group.