

7 Steps to Enable iPhones at Scale in the Enterprise

The iPhone has become a catalyst for changing the way both users and organizations think about their phones. Users want iPhones because of the exceptional experience they provide and because they support business applications. These applications include e-mail, but also broad business applications like salesforce.com and even niche business applications like medical imaging viewers. While enterprise IT's reaction may be to say "no," saying "no" is not an option. Invariably, an executive will demand an iPhone or the groundswell from users will become too loud to ignore. Enterprise IT departments need to think now about strategies to support iPhone deployments and adopt the tools necessary to support their deployment strategy.

When building an iPhone strategy, enterprise IT administrators will need to pay particular attention to how they can walk the fine line between providing end-users the tools to take full advantage of the richness of the iPhone experience, and having the processes in place to keep corporate data as secure as possible. To make iPhone deployments successful, enterprise IT should:

1. Bring iPhones under IT management
2. Connect enrolled iPhones securely to enterprise resources, including E-mail, Wi-Fi and VPN
3. Provide access to recommended enterprise applications
4. Enforce enterprise security policies to protect corporate data
5. Maintain a detailed, central inventory
6. Provide access control over iPhones connecting through ActiveSync
7. Secure lost, stolen, or retired iPhones through full and selective wipe

By developing a cohesive strategy backed by automated management tools, an enterprise can deploy iPhones in their environment at scale without placing undue strain on precious IT resources.

Task #1: Bring iPhones under IT Management

There are generally two schools of thought when it comes to connecting smartphones to enterprise management systems:

- IT should act as the gatekeeper for smartphones connecting to the enterprise by enrolling devices for users.
- End-users should enroll their devices themselves when provided with a simple process to do so, to help unburden the IT staff.

Assessing Enrollment Options

With the first model, enterprise IT first associates the phone with an authorized user account and enters the necessary information to create an entry in the inventory system. IT then completes the enrollment process on the phone or instructs the user to do so by sending the necessary instructions. This model works best:

- If phones may be shared across employees (for instance, if an iPhone or iPod touch is being used for a shift-based business application, such as in nursing or hospitality)
- In smaller companies where there are fewer users to contend with
- In support of high-touch employees, such as executives

In the second model, end-users access a web portal to request enrollment. Users then automatically receive the instructions needed to enroll the phone. This model works best for organizations that:

- Support a large number of users
- Have limited IT resources
- Have constant enrollments and changes for smartphones

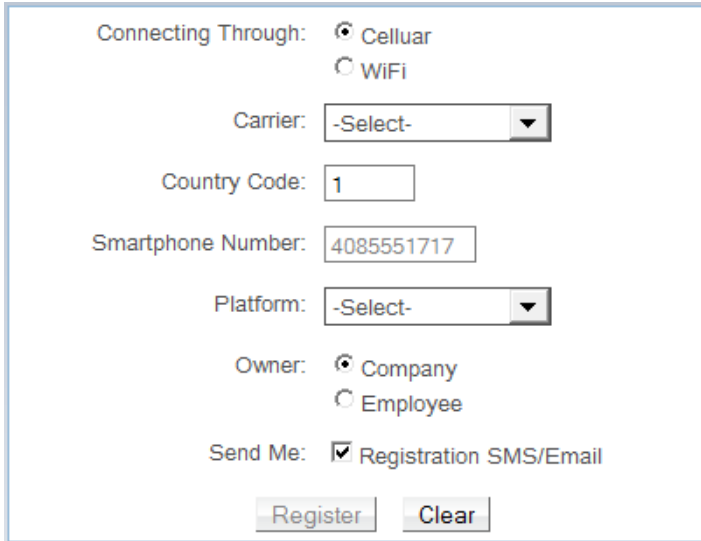
In some cases, just one of these two models will perfectly fit the organization. In most cases, a hybrid approach works best. The key is for IT to have the right tools for their own organizational model.

MobileIron's Flexible Enrollment Options

MobileIron has a flexible enrollment and access control system as part of the MobileIron Virtual Smartphone Platform. The MobileIron platform contains both a local authentication store and the ability to connect to LDAP for directory and authentication purposes.

With MobileIron, administrators define by group or individual user what rights should be assigned, including the ability to enroll phones. When a user accesses My Phone@Work, MobileIron's employee portal for smartphone management, they are given the option to enroll their phone. Users only need to know their phone number, operator, and phone type to enroll. A user is then sent a web link via SMS to begin the registration process. The remainder of the process includes downloading the MyPhone@Work Client from Apple's App Store, entering a one-time passcode they receive via email, and then starting the automated provisioning process.

Tech Tip: If IT adopts a self-service method, they should ensure that their device management system contains robust access controls that can be tied directly to the corporate directory. This will help assure that only allowed users are able to register their phones instead of the entire organization.



Connecting Through: Cellular
 WiFi

Carrier:

Country Code:

Smartphone Number:

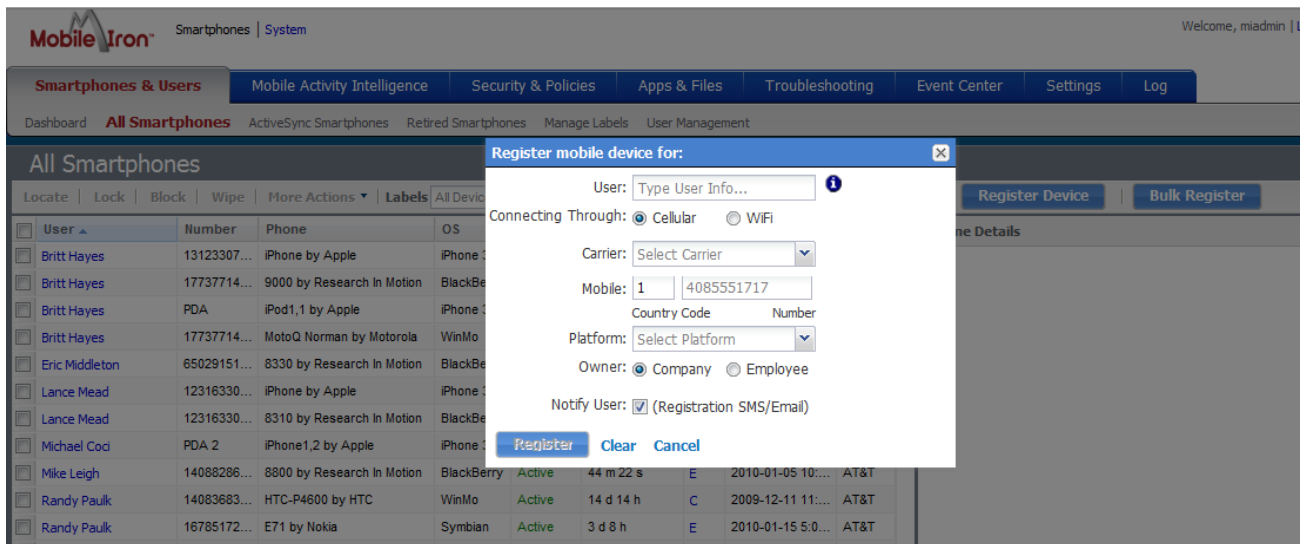
Platform:

Owner: Company
 Employee

Send Me: Registration SMS/Email

Figure 1: End-User Self Provisioning Screen

MobileIron recognizes that not all users will provision themselves or that IT may want to control the process. Therefore, the MobileIron Admin Portal enables IT to enroll phones on behalf of end users, either individually or by importing information for multiple users and phones.



MobileIron Smartphones | System Welcome, miadmin |

Smartphones & Users Mobile Activity Intelligence Security & Policies Apps & Files Troubleshooting Event Center Settings Log

Dashboard All Smartphones ActiveSync Smartphones Retired Smartphones Manage Labels User Management

All Smartphones

User	Number	Phone	OS
<input type="checkbox"/> Britt Hayes	13123307...	iPhone by Apple	iPhone
<input type="checkbox"/> Britt Hayes	17737714...	9000 by Research In Motion	BlackBerry
<input type="checkbox"/> Britt Hayes	PDA	iPod1,1 by Apple	iPhone
<input type="checkbox"/> Britt Hayes	17737714...	MotoQ Norman by Motorola	WinMo
<input type="checkbox"/> Eric Middleton	65029151...	8330 by Research In Motion	BlackBerry
<input type="checkbox"/> Lance Mead	12316330...	iPhone by Apple	iPhone
<input type="checkbox"/> Lance Mead	12316330...	8310 by Research In Motion	BlackBerry
<input type="checkbox"/> Michael Coc	PDA 2	iPhone1,2 by Apple	iPhone
<input type="checkbox"/> Mike Leigh	14088286...	8800 by Research In Motion	BlackBerry
<input type="checkbox"/> Randy Paulk	14083683...	HTC-P4600 by HTC	WinMo
<input type="checkbox"/> Randy Paulk	16785172...	E71 by Nokia	Symbian

Register mobile device for:

User:

Connecting Through: Cellular WiFi

Carrier:

Mobile:

Country Code: Number:

Platform:

Owner: Company Employee

Notify User: (Registration SMS/Email)

Figure 2: Admin Portal Registration Screen

Regardless of the method used, both enrollment and provisioning is handled over-the-air, eliminating the requirement for IT to physically touch each device.

Task #2: Connect Enrolled iPhones Securely to Enterprise Resources

Once a device is enrolled, it's important to make the device useful by allowing it to connect to enterprise resources such as e-mail, Wi-Fi, and VPN. These configurations should be:

- **Generated dynamically**, meaning that a user's credentials should be pre-populated and the right resource (e.g., server name, VPN concentrator) targeted to the right employee.
- **Handled over-the-air** to eliminate the need for enterprise IT to physically configure each iPhone (a time-consuming task even for small deployments).
- **Transmitted in a secure format**, such that when configurations are pushed over-the-air, the information within them (server names, account names, etc.) cannot be intercepted by hackers.

The MobileIron platform makes it easy to provision end-users for enterprise resources, including e-mail, Wi-Fi, and VPN. It dynamically generates configurations for iPhones based on the settings defined by an enterprise IT administrator. Administrators are able to tie settings to LDAP groups to meet the varying requirements within the organization.

For instance, suppose employees in the Americas use a VPN concentrator in a US datacenter, while employees in Europe use a VPN concentrator in the UK. In this case, the IT department could target an "America" label that provides VPN settings pointing to the US VPN concentrator and a "Europe" label that provides VPN settings that point to the UK VPN concentrator.

All configuration profiles generated by the MobileIron platform for an iPhone are delivered over-the-air using a protocol called SCEP. MobileIron's use of the SCEP protocol not only allows distribution of configurations without the need for IT to physically touch a device, but it also ensures that the configurations themselves are encrypted such that sensitive information, like server addresses and account names, are not exposed during the distribution process. The certificates used to sign and encrypt configuration profiles can also be used for authentication to back-end resources, including Exchange, Wi-Fi and VPN. Finally, because MobileIron signs all configuration profiles, any backups made with iTunes will automatically be encrypted and password protected.

Tech Tip: Use the SCEP protocol to ensure that configuration information is encrypted over-the-air, prevent configurations from being tampered with and mandate that all iTunes backups be encrypted and password protected.

Task #3: Provide Access to Recommended Enterprise Applications

While e-mail, Wi-Fi, and VPN are important attributes to provision to a user's phone, they are not the only elements an IT department should be concerned with. iPhones are essentially mini computers and have been designed to power rich applications, including business-oriented applications like medical imaging and CRM. Organizations face two main challenges in handling applications within their enterprise:

- **Communicating which of the 125,000+ applications on the Apple App Store are supported** by the enterprise and making them easily accessible. For instance, many organizations would provide support for applications like the popular CRM tool, Salesforce.com or news tools like Reuters, while they would not provide support for iPhone games.

- **Understanding how they will handle reimbursement of paid applications.** Many applications, including popular ones like QuickOffice, cost money, and IT will need to determine how to pay for those applications.



MobileIron's Application Distribution for iPhone

The MobileIron platform helps enterprises communicate to end users which App Store applications are IT supported, assists with the application reimbursement process, and makes it easy to provide direct access to web-based applications.

Through the MobileIron app, enterprise IT administrators can link to applications from the App Store and create a recommended applications list, which can be custom-tailored to an individual or group of users. When a user clicks on a recommended application, they see a description of the application and the option to download it from the App Store. Employees can participate in giving IT visibility into their application usage by marking these recommendations as applications they use. Updates to the recommended applications list can be made over-the-air to reflect changes in recommendations and in policies. For example, using the recommended applications list, IT can ensure that an executive traveling to

China is armed with the right language translation tool or currency converter just before their trip.

Managing payment for applications is also an important issue. Most organizations prefer to tie iTunes accounts to personal credit cards or corporate cards that are personally liable, and then reimburse employees for use of sanctioned applications.

To support this, the MobileIron recommended applications list can be targeted to individual users or groups, enabling IT to communicate which applications will be reimbursed by either the corporate IT or finance departments.

Employees automatically know what is supported and what is not from within their own iPhone; regular auditing against these lists can help track down sources of abuse.

MobileIron administrators can also give users easy access to web-based applications by configuring Web Clips. A Web Clip places a direct link to a website within the user's iPhone home screen. This allows an end-user to launch a web application as they would any other application.

Tech Tip: The iPhone is well known for its immersive, rich applications, but its Safari web browser makes it an ideal platform for powering web-based applications, as well. Make sure your enterprise has a strategy for deploying both types of applications to your iPhone users.

Task #4: Enforce Enterprise Security Policies

Once a user is provisioned with enterprise e-mail, Wi-Fi, VPN settings, and enterprise applications (both native and web-based), large amounts of enterprise data will now be stored on the iPhone. These data exist in multiple places including:

- The corporate e-mail box
- The browser cache
- Any application caches

Tech Tip: Because data can exist in multiple places within an iPhone, IT must have a device-wide security focus, and not just on one container, such as e-mail.

Because corporate data can exist in multiple locations, enterprises must mandate device-wide security policies. Organizations should consider enforcing the following security policies in an iPhone deployment:

- **Multi-character, complex device passwords** to ensure that unauthorized individuals cannot easily gain access to the device.
- **Device lockdown policies** that may be necessary per corporate policy, such as locking down cameras or preventing screenshots on the device.
- **Up-to-date iPhone OS software**
- **Full-device encryption** to protect all forms of corporate data.

MobileIron's Policy Management

The MobileIron platform can easily help organizations enforce strong passwords for iPhones:

- Flexible password complexity allows up to 10 characters with a minimum of up to 4 required special characters.
- The device can be wiped if the maximum number of failed login attempts has been exceeded.
- Lockdown policies can be enforced to put the iPhone in line with corporate policies. These restrictions include the ability to prevent access to the App Store and iTunes on the device, launching of the camera, etc.

As Apple adds new options to the configuration schema, the MobileIron platform will adopt these options.



Secure Configuration Management

As noted previously, the MobileIron platform delivers all configuration profiles for an iPhone over-the-air using the SCEP protocol, which ensures that sensitive corporate information is transmitted securely. In addition to encrypting all configuration data, the MobileIron platform digitally signs all configuration profiles. This means that a configuration profile cannot be tampered with, and IT is able to prevent a profile from being removed (for instance, to ensure a device-level password policy). Signed configuration profiles cannot be overwritten by programs (such as the iPhone Configuration Utility) or removed from the device unless IT approves so. MobileIron's use of SCEP also allows integration to back end certificate authorities for identity purposes.

OS and Platform Version Management

Finally, the MobileIron Client, which users install during the process of enrollment, can provide IT administrators an understanding of what devices are running older iPhone operating systems (e.g., iPhone OS 3.0 or 2.2) or are using platforms that do not support encryption (e.g., iPhone, iPhone 3G). IT administrators can reach out to these users directly from the MobileIron platform, via SMS or e-mail, to inform them that they should upgrade or use a different device. This same visibility is used to provide access control functionality, as well.

Task #5: Maintain a Detailed Central Inventory

Once users begin enrolling on the system, it's important to know what iPhones exist, who they are associated with, and whether they are owned by the user or the enterprise. Additional useful information available includes phone number, serial number, etc. As they look to keep an accurate device inventory, IT must decide:

- How to record and track inventory information
- How to keep up with the ever-increasing number of devices in the organization
- How to ensure that the information is kept up to date over time

Further, visibility into the ActiveSync environment is also crucial to the success of any smartphone deployment, especially iPhone deployments. In a recent research note, leading analyst firm Gartner Research stated that "[Exchange ActiveSync] EAS is becoming a de facto standard for push e-mail and PIM".

Gartner went on to recommend that "IT organizations should make EAS support in mobile devices a priority feature to extend the interoperability of corporate devices with multiple e-mail, calendar and contact options." With an increasing number of both e-mail platforms and devices supporting ActiveSync, organizations will need to understand how they will obtain visibility and access control over their ActiveSync e-mail systems.

MobileIron's Visibility Features

The MobileIron platform can easily provide visibility into the managed devices connecting into the organization, including iPhones, by means of the MobileIron client. The MobileIron client gathers detailed information about an individual device and reports it back to the MobileIron platform. In the case of the iPhone, reported data includes device ID, platform type (e.g., iPhone, 3G, 3GS), and OS type (e.g., iPhone OS 3.0, 3.1).

This information can be used to answer simple questions like "How many devices are in my organization?" and "What is the breakdown of iPhones versus other devices?" As mentioned previously, the information can also be used to help manage policies, such as mandating that iPhone operating systems be kept up to date.

MobileIron's visibility into enterprise devices extends into the ActiveSync environment, as well. MobileIron's Sentry functionality allows organizations to understand what devices have connected to corporate e-mail, possibly bypassing security policies, such as mandates that devices be registered with a device management system. MobileIron Sentry can integrate directly with Exchange 2007 mail servers and above, providing direct visibility from the mail server as to who is accessing push e-mail.

MobileIron Sentry can also act as an ActiveSync proxy. Clients connect to the Sentry, which relays e-mail traffic to the ActiveSync server. This method will work for:

- On-premise solutions, such as Microsoft Exchange, Lotus Notes and Novell Groupwise
- Cloud-based e-mail environments, such as Gmail and Microsoft Hosted Exchange Services, where functions such as direct query of the mailserver and remote wipe may not be readily available

In short, MobileIron delivers the most flexible means of providing visibility over the ActiveSync e-mail environment. Organizations that run a mix of e-mail environments, including both hosted and on-premise solutions, can use MobileIron Sentry to achieve complete coverage of their push e-mail environment.

Task #6: Provide Access Control over iPhones Connecting through ActiveSync

It is essential for organizations to understand who is connected to the corporate environment. However, organizations must provide access control to corporate resources, as well. Many organizations are wary about opening access to ActiveSync, despite recommendations from firms such as Gartner. Traditionally, supporting ActiveSync has meant that:

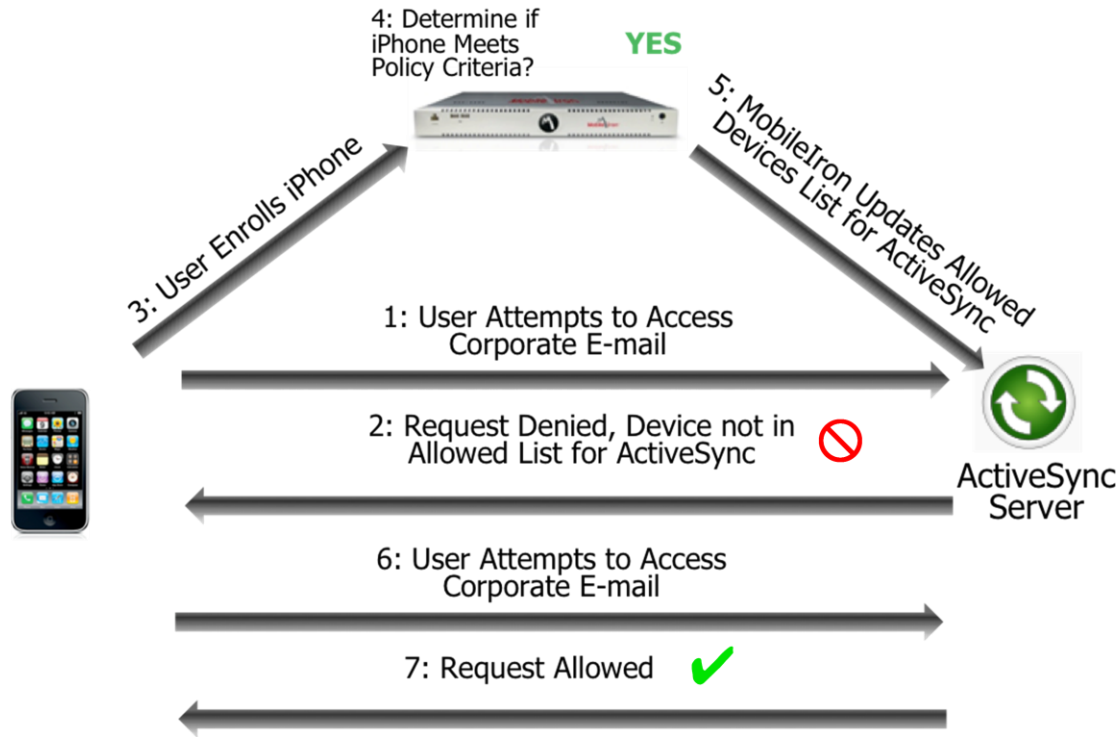
- Anyone who knows how to register their device can connect and get corporate e-mail.
- Users are able to register multiple devices, increasing the risk for loss of corporate data.

Other e-mail systems have done a good job of providing access control over corporate e-mail. With iPhones and other devices increasingly supporting ActiveSync for push e-mail, enterprises will need to look for ways to bring this functionality into ActiveSync, as well.

Tech Tip: For most organizations, the first choice for wireless email on the iPhone is the native iPhone email application, which uses ActiveSync. With an increasing number of products that support ActiveSync, IT must prioritize ActiveSync security and management instead of investing in e-mail point-products.

MobileIron's ActiveSync Management Capabilities

MobileIron's Sentry changes the ActiveSync e-mail model from one where any device can connect, to one where enterprise IT can manage the influx of devices entering the network.



With the MobileIron Sentry, enterprises can ensure that only registered devices are allowed to connect to corporate e-mail. This means that organizations are able to properly provision, secure, and manage a device before the device begins downloading corporate e-mail. The MobileIron platform can also set policies to limit the number of devices connecting to ActiveSync. This helps to prevent numerous devices from accessing corporate e-mail simultaneously and limit exposure to risk for the organization.

MobileIron's Security Features for iPhone

Once devices are provisioned, it's important to determine if they meet the correct posture in order to connect and maintain a connection to corporate e-mail. MobileIron is the first platform to be able to detect whether iPhones have been modified. Modified iPhones should be disconnected from enterprise e-mail in order to protect corporate data.

The MobileIron uses multiple proprietary methods to determine if a phone has been modified. Upon detecting a modified iPhone, the app communicates to the MobileIron platform, which can notify administrators to take action, and also disconnect the phone from corporate e-mail. This method helps to ensure that phones that pose a high security risk don't connect to the organization.

In addition to detecting modified iPhones, organizations should ensure their user base runs the latest iPhone OS software. Apple continually releases updates to the iPhone that enhance both the user experience as well as the security posture of the device. Through the MobileIron platform, IT administrators can detect if users have not upgraded their iPhone and reach out to those users and prompt them to upgrade. Administrators can also

use the MobileIron Sentry to require that users run the latest iPhone OS software from Apple before connecting to corporate resources.

Finally, the MobileIron platform can also use its inventory capabilities to set policies that require that only iPhone 3GS devices be able to connect to corporate e-mail. This access control functionality helps enterprise IT enforce policies that mandate full device encryption to protect all corporate data on the device, including e-mail, application data, and any corporate information that exists in the browser cache. Furthermore, the use of signed configuration profiles distributed by MobileIron enforces the requirement that all iTunes backups be password protected and encrypted.

Task #7: Secure Lost, Stolen, or Retired iPhones through Full and Selective Wipe

Invariably, a user will misplace their phone or someone will steal the phone. In other cases, an employee will leave the company with a personal iPhone that had been connected to the corporate network. With the multitude of situations that IT may have to contend with, it is important for IT to have the right tools to remove confidential information from a device for a given situation.

Securing Lost, Stolen, or Retired iPhones with MobileIron

If a device is lost or stolen, it's important to be able to wipe the device fully and restore it to factory defaults. The MobileIron platform can easily identify an individual iPhone and push a remote wipe command to the phone. This command causes the device to remove all information and essentially returns the device to the state it came in when it left the factory. This approach to wiping corporate information is critically important; as mentioned earlier, corporate data can exist in many places throughout the phone. It, thus, becomes important to ensure that all corporate information is wiped clean from the device.

While many use cases are served by fully wiping an iPhone, MobileIron recognizes that a "one-size-fits-all" approach does not exist. In some cases, for instance when an employee

leaves the company, the IT department may want to focus on removing e-mail from the device instead of wiping out personal information, like music or pictures of the employee's family. To this end, MobileIron can reset an ActiveSync mailbox on an iPhone and cause all of the e-mail to be removed from the device. After this command is issued, the phone is blocked from accessing the ActiveSync server to ensure that e-mail cannot be downloaded again to the device. This allows IT to begin drawing an enterprise data boundary between corporate and personal information on the phone.

Tech Tip: Because many iPhones are employee-owned, organizations need both the ability to selectively wipe the contents of the native iPhone email client as well as fully wipe the entire device.

Conclusion

Organizations across virtually every industry have found iPhones gaining traction among their employees. Many organizations are conducting pilots to determine the feasibility of supporting iPhones and have quickly found that a small, 50 user pilot balloons into hundreds or even thousands of requests from end-users for iPhone support. And while iPhones have certainly served as the catalyst for broadening the set of supported mobile devices in the enterprise, users will quickly bring in other platforms. Thus, whatever strategy an enterprise adopts should be manageable across all existing smartphone platforms. Without automated tools, any smartphone deployment, including iPhones, will become difficult to support.

MobileIron provides the broadest set of best-of-breed tools for organizations to deploy iPhones with confidence. With the MobileIron platform, organizations can:

- Register iPhones and other smartphones with IT to bring them under management
- Connect iPhones to enterprise resources, including e-mail, Wi-Fi, and VPN
- Provide access to both native and web-based enterprise applications
- Enforce enterprise security policies to protect corporate data, including mandating full device encryption on iPhones
- Maintain a detailed central inventory of all iPhones in the environment
- Provide access control over ActiveSync to prevent unregistered iPhones or iPhones out of policy from connecting
- Secure lost, stolen or retired iPhones through full and selective wipe of corporate data

To learn more about the MobileIron Virtual Smartphone Platform and how it can support iPhones in your organization, visit <http://www.mobileiron.com/iphone> or email iphone@mobileiron.com.