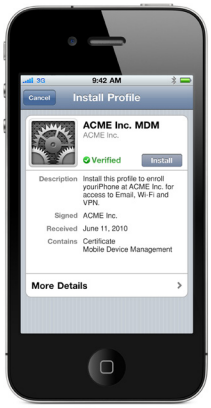
iPhone in Business
Mobile Device Management



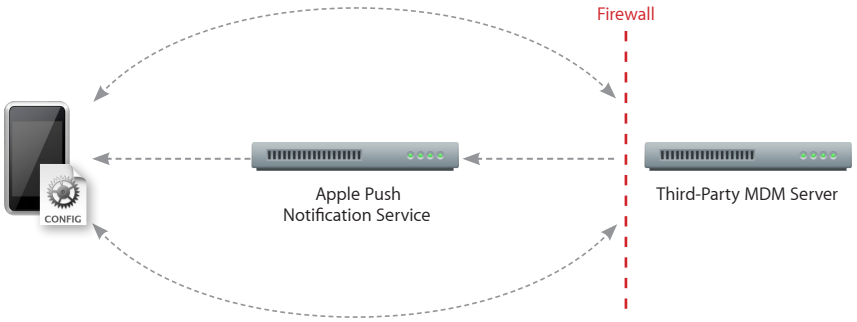
iPhone supports Mobile Device Management, giving businesses the ability to manage scaled deployments of iPhone across their organizations. These Mobile Device Management capabilities are built upon existing iOS technologies like Configuration Profiles, Over-the-Air Enrollment, and the Apple Push Notification service and can be integrated with in-house or third-party server solutions. This gives IT departments the ability to securely enroll iPhone in an enterprise environment, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely wipe or lock managed iPhone devices.

Managing iPhone

Management of iPhone takes place via a connection to a mobile device management server. As noted, this server can be built in-house by IT or purchased from a third-party solution provider. When a mobile device management server wants to communicate with iPhone, a silent notification is sent to the device prompting it to check in with the server. The device communicates with the server to see if there are tasks pending and responds with the appropriate actions. These tasks can include updating policies, providing requested device or network information, or removing settings and data.

Management functions are completed behind the scenes with no user interaction required. For example, if an IT department updates its VPN infrastructure, the mobile device management server can configure iPhone with new account information over the air. The next time VPN is used by the employee, the appropriate configuration is already in place, so the employee doesn't need to call the help desk or manually modify settings.

To illustrate the capabilities of Mobile Device Management, this document is organized into four categories of deployment: Enroll, Configure, Query, and Manage.



Enroll

The first step in managing iPhone is to enroll a device with a mobile device management server. This creates a relationship between the device and the server, allowing the device to be managed on demand without further user interaction. This can be done wirelessly or by connecting iPhone to a computer via USB.

As a scalable way to securely enroll devices in an enterprise environment, iPhone supports a process called Over-the-Air Enrollment.

Using Over-the-Air Enrollment, your enterprise can provide a secure web portal through which users can enroll their devices for management. The server can then configure managed devices with the appropriate restrictions and account access.

iPhone and SCEP
iPhone supports the Simple Certificate Enrollment Protocol (SCEP). SCEP is an Internet draft in the IETF, and is designed to provide a simplified way of handling certificate distribution for large-scale deployments. This enables over-the-air enrollment of identity certificates to iPhone that can be used for authentication to corporate services.

Process Overview

The process of Over-the-Air Enrollment involves three phases that, when combined in an automated workflow, provide a secure way to provision devices within the enterprise. These phases include:

1. User authentication
User authentication ensures that incoming enrollment requests are from authorized users and that the user's device information is captured prior to proceeding with certificate enrollment. Administrators can prompt the user to begin the process of enrollment by providing a URL via email or SMS notification.

2. Certificate enrollment
After the user is authenticated, iPhone generates a certificate enrollment request using the Simple Certificate Enrollment Protocol (SCEP). This enrollment request communicates directly to the enterprise Certificate Authority (CA), and enables iPhone to receive the identity certificate from the CA in response.

3. Device configuration
Once an identity certificate is installed, iPhone can receive encrypted configuration information over the air. This information can only be installed on the device it is intended for and contains settings for iPhone to connect to the mobile device management server.

At the end of the enrollment process, the user will be presented with an installation screen that describes what access rights the mobile device management server will have on the device. By agreeing to the profile installation, the user's device is automatically enrolled without further interaction.

Configure

Once a device is enrolled as a managed device, it can be dynamically configured with settings and policies by the mobile device management server. The server sends configurations, known as Configuration Profiles, to the device that are installed automatically.

Configuration Profiles are XML files that contain configuration information and settings that permit iPhone to work with your enterprise systems, including account information, passcode policies, restrictions, and other device settings.

When combined with the previously discussed process of enrollment, device configuration provides IT with assurance that only trusted users are accessing corporate services, and that their devices are properly configured with established policies.

And because Configuration Profiles can be signed, encrypted, and locked, the settings cannot be altered or shared with others.

Supported configurable settings

Accounts

- Exchange ActiveSync
- IMAP/ POP email
- VPN
- Wi-Fi
- LDAP
- CalDAV
- CardDAV
- Subscribed calendars

Policies

- Require passcode
- Allow simple value
- Require alphanumeric value
- Passcode length
- Number of complex characters
- Maximum passcode age
- Time before auto-lock
- Number of unique passcodes before reuse
- Grace period for device lock
- Number of failed attempts before wipe
- Control Configuration Profile removal by user

Restrictions

- App installation
- Camera
- Screen capture
- Automatic sync of mail accounts while roaming
- Voice dialing when locked
- In-application purchasing
- Require encrypted backups to iTunes
- Explicit music & podcasts in iTunes
- Allowed content ratings for movies, TV shows, apps
- Safari security preferences
- YouTube
- iTunes Store
- App Store
- Safari

Other settings

- Certificates and identities
- Web Clips
- APN settings

Query

In addition to configuring devices, a mobile device management server has the ability to query devices for a variety of information. This information can be used to ensure that devices continue to comply with required policies.

The mobile device management server determines the frequency at which it gathers information.

Supported queries

Device information

- Unique Device Identifier (UDID)
- Device name
- iOS and build version
- Model name and number
- Serial number
- Capacity and space available
- IMEI
- Modem firmware

Network information

- ICCID
- Bluetooth® and Wi-Fi MAC addresses
- Current carrier network
- SIM carrier network
- Carrier settings version
- Phone number
- Data roaming setting (on/off)

Compliance and security information

- Configuration Profiles installed
- Certificates installed with expiry dates
- List of all restrictions enforced
- Hardware encryption capability
- Passcode present

Applications

- Applications installed (app ID, name, version, size, and app data size)
- Provisioning Profiles installed with expiry dates

Manage

When a device is managed, it can be administered by the mobile device management server through a set of specific actions.

Remote wipe

A mobile device management server can remotely wipe an iPhone. This will permanently delete all media and data on the iPhone, restoring it to factory settings.

Remote lock

The server locks the iPhone and requires the device passcode to unlock it.

Clear passcode

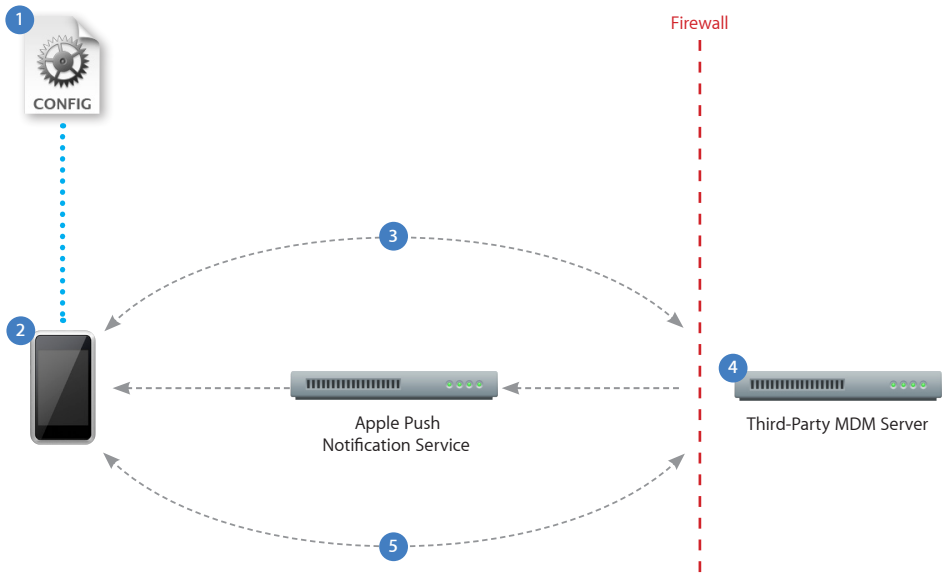
This action temporarily removes the device passcode for users who have forgotten it. If the device has a policy requiring a passcode, the user will be required to create a new one.

Configuration and Provisioning Profiles

To configure devices and provision in-house applications, mobile device management servers can add and remove Configuration Profiles and Application Provisioning Profiles remotely.

Process Overview

This example depicts a basic deployment of a mobile device management server.



1. A Configuration Profile containing mobile device management server information is sent to the device. The user is presented with information about what will be managed and/or queried by the server.
2. The user installs the profile to opt in to the device being managed.
3. Device enrollment takes place as the profile is installed. The server validates the device and allows access.
4. The server sends a push notification prompting the device to check in for tasks or queries.
5. The device connects directly to the server over HTTPS. The server sends commands or requests information.

For more information on Mobile Device Management, visit www.apple.com/iphone/business/integration

 June 2010 L419825A