Deploying iPhone and iPad
Mobile Device Management

No profiles are currently installed

Acme Inc. Configuration
Acme Inc.
✓ Verified

Description: Install this profile to enroll your iOS device at ACME Inc. to get access to Email, Wi-Fi and VPN.
Signed: iPhone Configuration Utility (8545FFEC-4B2B-4201-9A5E-F12B6B35B7D0)
Received: Mar 21, 2012
Contains: Restriction
Exchange Account
Password Policy

iPhone for Acme Inc.
Acme, Inc.
✓ Verified

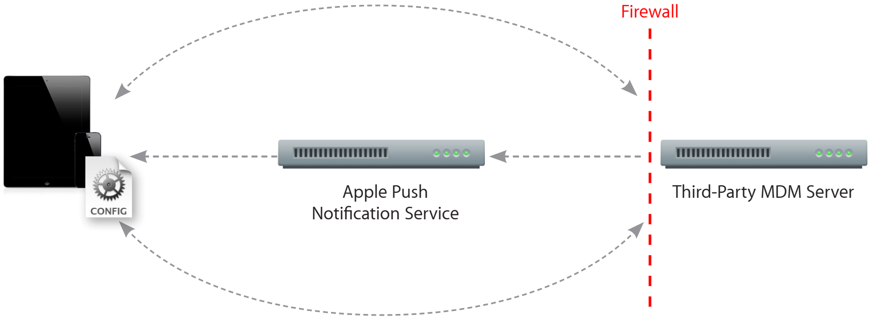
Description: Company restricted network accounts for Mail, Contacts, Calendars, Tasks and VPN. Requires a strong passcode.
Signed: iPhone Configuration Utility (492A5AE6-E58C-40FA-A6E6-ECB82D6CA773)
Received: Sep 14, 2012
Contains: Wi-Fi Network
VPN Settings
Web Clip
Restriction
Exchange Account
Password Policy

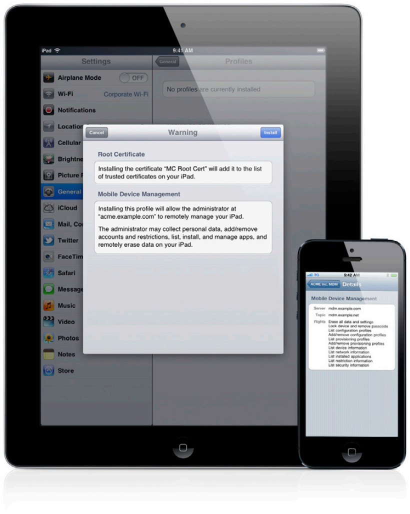
iOS supports Mobile Device Management (MDM), giving businesses the ability to manage scaled deployments of iPhone and iPad across their organizations. These MDM capabilities are built upon existing iOS technologies like Configuration Profiles, Over-the-Air Enrollment, and the Apple Push Notification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

Managing iPhone and iPad

Management of iOS devices takes place via a connection to a Mobile Device Management server. This server can be built in-house by IT or purchased from a third-party solution provider. 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.

Most management functions are completed behind the scenes with no user interaction required. For example, if an IT department updates its VPN infrastructure, the MDM server can configure iPhone and iPad 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.





No profiles are currently installed

Root Certificate

Installing the certificate "MC Root Cert" will add it to the list of trusted certificates on your iPad.

Mobile Device Management

Installing this profile will allow the administrator at "acme.example.com" to remotely manage your iPad.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPad.

Mobile Device Management

Server mdm.example.com
Topic mdm.example.net
Rights Erase all data and settings
Lock device and remove passcode
List configuration profiles
Add/remove configuration profiles
List provisioning profiles
Add/remove provisioning profiles
List device information
List network information
List installed applications
List restriction information
List security information

iOS and SCEP
iOS 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 and iPad that can be used for authentication to corporate services.

MDM and the Apple Push Notification Service

When an MDM server wants to communicate with iPhone or iPad, a silent notification is sent to the device via the Apple Push Notification service, prompting it to check in with the server. The process of notifying the device does not send any proprietary information to or from the Apple Push Notification service. The only task performed by the push notification is to wake the device so it checks in with the MDM server. All configuration information, settings, and queries are sent directly from the server to the iOS device over an encrypted SSL/TLS connection between the device and the MDM server. iOS handles all MDM requests and actions in the background to limit the impact on the user experience, including battery life, performance, and reliability.

In order for the push notification server to recognize commands from the MDM server, a certificate must first be installed on the server. This certificate must be requested and downloaded from the Apple Push Certificates Portal. Once the Apple Push Notification certificate is uploaded into the MDM server, devices can begin to be enrolled. For more information on requesting an Apple Push Notification certificate for MDM, visit www.apple.com/business/mdm.

Apple Push Notification network setup

When MDM servers and iOS devices are behind a firewall, some network configuration may need to take place in order for the MDM service to function properly. To send notifications from an MDM server to the Apple Push Notification service, TCP port 2195 needs to be open. To reach the feedback service, TCP port 2196 will need to be open as well. For devices connecting to the push service over Wi-Fi, TCP port 5223 should be open.

The IP address range for the push service is subject to change; the expectation is that an MDM server will connect by hostname rather than by IP address. The push service uses a load-balancing scheme that yields a different IP address for the same hostname. This hostname is gateway.push.apple.com (and gateway.sandbox.push.apple.com for the development push notification environment). Additionally, the entire 17.0.0.0/8 address block is assigned to Apple so firewall rules can be established to specify that range.

For more information, consult your MDM vendor or view *Developer Technical Note TN2265* in the iOS Developer Library at http://developer.apple.com/library/ios/#technotes/tn2265/_index.html.

Enrollment

Once the Mobile Device Management server and network are configured, the first step in managing an iPhone or iPad is to enroll it with an MDM server. This creates a relationship between the device and the server, allowing it to be managed on demand without further user interaction.

This can be done by connecting iPhone or iPad to a computer via USB, but most solutions deliver the enrollment profile wirelessly. Some MDM vendors use an app to kickstart this process, others initiate enrollment by directing users to a web portal. Each method has its benefits, and both are used to trigger the Over-the-Air Enrollment process via Safari.

Enrollment process overview

The process of Over-the-Air Enrollment involves phases that are combined in an automated workflow to provide the most scalable way to securely enroll devices in an enterprise environment. 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 via a web portal, email, SMS message, or even an app.

2. Certificate enrollment

After the user is authenticated, iOS 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 and iPad to receive the identity certificate from the CA in response.

3. Device configuration

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

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

Once iPhone and iPad are enrolled as managed devices, they can be dynamically configured with settings, queried for information, or remotely wiped by the MDM server.

Management

With Mobile Device Management, there are a number of functions an MDM server can perform on iOS devices. These tasks include installing and removing Configuration and Provisioning Profiles, managing apps, ending the MDM relationship, and remotely wiping a device.

Managed configuration

During the initial process of configuring a device, an MDM server pushes Configuration Profiles to iPhone and iPad that are installed behind the scenes. Over time, the settings and policies put in place at the time of enrollment may need to be updated or changed. To make these changes, an MDM server can install new Configuration Profiles and modify or remove existing profiles at any time. Additionally, context-specific configurations may need to be installed on iOS devices, depending on a user's location or role in the organization. As an example, if a user is traveling internationally, an MDM server can require that mail accounts sync manually instead of automatically. An MDM server can even remotely disable voice or data services in order to prevent a user from incurring roaming fees from a wireless provider.

Managed apps

An MDM server can manage third-party apps from the App Store, as well as enterprise in-house applications. The server can remove managed apps and their associated data on demand or specify whether the apps are removed when the MDM profile is removed. Additionally, the MDM server can prevent managed app data from being backed up to iTunes and iCloud.

To install a managed app, the MDM server sends an installation command to the user's device. Managed apps require a user's acceptance before they are installed. When an MDM server requests the installation of a managed app from the App Store, the app will be redeemed with the iTunes account that is used at the time the app is installed. Paid apps will require the MDM server to send a Volume Purchasing Program (VPP) redemption code. For more information on VPP, visit www.apple.com/business/vpp. Apps from the App Store cannot be installed on a user's device if the App Store has been disabled.

Managing supervised devices with MDM

Devices that are activated using Apple Configurator can be "supervised," enabling additional settings and restrictions to be installed. Once a device is supervised with Apple Configurator, all available settings and restrictions can be installed over the air via MDM as well. For more information on configuring and managing devices using both Apple Configurator and MDM, refer to *Deploying iPhone and iPad: Apple Configurator*.

Removing or wiping devices

If a device is found to be out of policy, lost, or stolen, or if an employee leaves the company, an MDM server can take action to protect corporate information in a number of ways.

An IT administrator can end the MDM relationship with a device by removing the Configuration Profile that contains the MDM server information. In doing so, all the accounts, settings, and apps it was responsible for installing are removed. Alternatively, IT can keep the MDM Configuration Profile in place and use MDM only to remove the specific Configuration Profiles, Provisioning Profiles, and managed apps they want to delete. This approach keeps the device managed by MDM and eliminates the need to re-enroll once it is back within policy.

Both methods give IT the ability to ensure information is only available to compliant users and devices, and ensures corporate data is removed without interfering with a user's personal data such as music, photos, or personal apps.

To permanently delete all media and data on the device and restore it to factory settings, MDM can remotely wipe iPhone and iPad. If a user is still looking for the device, IT can also choose to send a remote lock command to the device. This locks the screen and requires the user's passcode to unlock it.

If a user has simply forgotten the passcode, an MDM server can remove it from the device and prompt the user to create a new one within 60 minutes.

Supported management commands

Managed configuration

- Install Configuration Profile
- Remove Configuration Profile
- Data roaming
- Voice roaming (not available on all carriers)

Managed apps

- Install managed app
- Remove managed app
- List all managed apps
- Install Provisioning Profile
- Remove Provisioning Profile

Security commands

- Remote wipe
- Remote lock
- Clear passcode

Configuration

To configure a device with accounts, policies, and restrictions, the MDM server sends files known as Configuration Profiles to the device that are installed automatically. Configuration Profiles are XML files that contain settings that permit the device 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 and encrypted, the settings cannot be altered or shared with others.

Supported configurable items

Accounts

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

Passcode policies

- Require passcode on device
- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Time before auto-lock
- Passcode history
- Grace period for device lock
- Maximum number of failed attempts

Security and privacy

- Allow diagnostic data to be sent to Apple
- Allow user to accept untrusted certificates
- Force encrypted backups

Supervised only restrictions

- Allow iMessage
- Allow Game Center
- Allow removal of apps
- Allow iBookstore
- Allow erotica from iBookstore
- Enable Siri Profanity Filter
- Allow manual install of Configuration Profiles

Other settings

- Credentials
- Web clips
- SCEP settings
- APN settings
- Global HTTP Proxy (Supervised only)
- Single App Mode (Supervised only)

Device functionality

- Allow installing apps
- Allow Siri
- Allow Siri while locked
- Allow Passbook notifications while locked
- Allow use of camera
- Allow FaceTime
- Allow screen capture
- Allow automatic syncing while roaming
- Allow syncing of Mail recents
- Allow voice dialing
- Allow In-App Purchase
- Require store password for all purchases
- Allow multiplayer gaming
- Allow adding Game Center friends

Applications

- Allow use of YouTube
- Allow use of iTunes Store
- Allow use of Safari
- Set Safari security preferences

iCloud

- Allow backup
- Allow document sync and key-value sync
- Allow Photo Stream
- Allow shared Photo Stream

Content ratings

- Allow explicit music and podcasts
- Set ratings region
- Set allowed content ratings

Querying Devices

In addition to configuration, an MDM 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.

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
- Battery level
- Supervision status

Network information

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

Compliance and security information

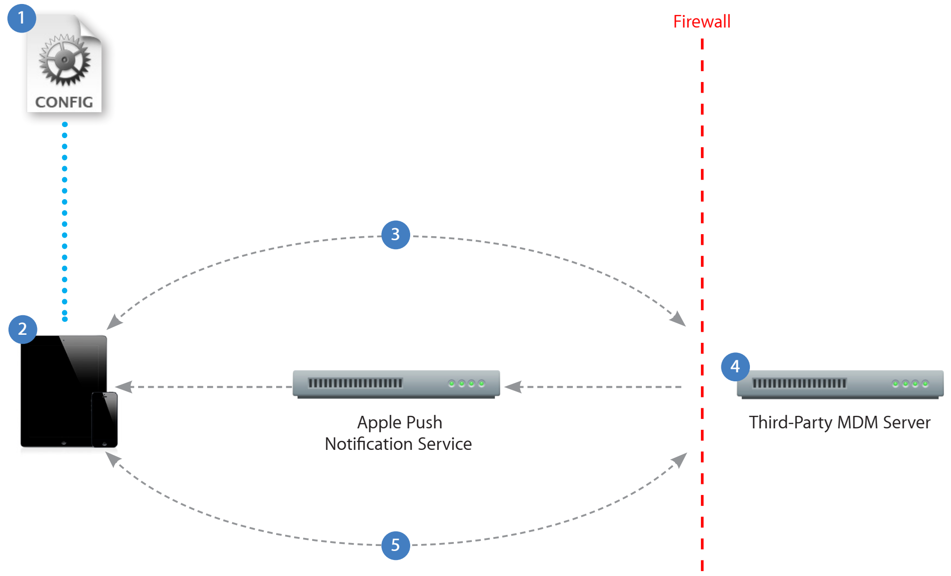
- Configuration Profiles installed
- Certificates installed with expiry dates
- List all restrictions enforced
- Hardware encryption capability
- Passcode present

Applications

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

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/business/mdm.