Apple Technical White Paper

Managing OS X with Configuration Profiles

OS X Lion v 10.7.3

Table of Contents

About Configuration Profiles

Introduction

On iOS devices, preferences and preconfigured settings are managed with Mobile Device Management (MDM) technologies and configuration profiles.

Beginning with OS X Lion, Apple has brought the configuration profile and MDM technologies from iOS to OS X. Configuration profiles not only allow for the same preference policies to be deployed as the Managed Preferences system, but they also bring powerful new configuration options such as directory service binding, 802.1X configuration, and certificate distribution to Mac management.

OS X Management Changes

OS X Lion brings with it many new opportunities in the way that organizations like schools and businesses deploy and manage OS X computers. One of the most fundamental changes is in the area of management.

Changes to configuration profiles can be coordinated between an MDM server and managed OS X computers via the Apple Push Notification service (APNs), so changes to policy are quickly made on the client computers. The flexibility of many MDM solutions also allows users to enroll their own Mac into the management system. The combined use of APNs and MDM allows users or administrators to remotely lock or even wipe a lost Mac.

When planning new Mac deployments, your primary policy solution should be configuration profiles. Though you may mix policies and settings from Managed Preferences and configuration profiles on OS X computers, older Mac deployments can't use configuration profiles and are unaffected by this change.

With the addition of MDM support to OS X, Apple now offers a unified system of configuration and management for all Apple devices. As developers add support for Lion to their MDM solutions, the resources needed to manage the Mac become simplified from a hardware, software, and administrative perspective.

When integrated with an MDM server, configuration profiles can be wirelessly distributed to the Mac for completely hands-free management of your deployment. All users need to do is self-enroll their Mac for management with the MDM server, and the system will handle the rest.

Advantages

Configuration profile support in OS X allows for simplified Mac management and provides several key advantages, including:

- **Greater power and flexibility.** Profiles offer many more options than Managed Preferences did for managing your Mac deployment. All the same Managed Preferences controls, including arbitrary application control, still work with configuration profiles. The flexibility provided by Managed Preferences is still available with configuration profiles, but configuration profiles offer additional functionality over Managed Preferences. For example, you can configure 802.1X or install certificates to the keychain on a Mac.
- **Enables Mobile Device Management.** A large amount of iOS management with configuration profiles is done via MDM servers. OS X now supports MDM as well, providing the flexibility on a Mac that organizations expect for a mobile device.
- **Leverages existing file format.** Configuration profiles may be new to the Mac, but they're well understood by iOS administrators. Administrators can now apply to the Mac the expertise they've gained in iOS configuration profile creation.
- **Establishes commonality with iOS.** With the move to configuration profiles, Apple now has a common configuration technology between OS X and iOS. The file format is the same between platforms, and many of the policy keys are even shared.

Purpose

When an organization needs a streamlined process for deploying and managing a large number of OS X computers, a powerful and flexible solution is to install one or more configuration profiles onto the computers. Configuration profiles are lists of settings that you use to quickly set up OS X computers to work with information systems.

For example, you might set up a profile that configures computers to access Microsoft Exchange servers or defines how they connect to Wi-Fi and internal corporate networks. Configuration profiles also give you the ability to lock the settings.

You can use configuration profiles to set up accounts such as email, calendaring, and Exchange account settings; credentials for all those accounts; and network settings, passcode policies, and device restrictions.

Some examples of the types of settings that you can include in configuration profiles are:

- Passcode and Security policies
- Network settings including Wi-Fi, VPN, and 802.1X
- Account settings including email, LDAP, calendar, and instant messaging

- Credentials and keys
- Login items
- Dock preferences
- Parental controls
- Custom settings with key-value pairs for specific preference domains

A complete list of the available configuration profile settings is available in Appendix A.

Categories

There are two basic categories of profiles that can be installed on an OS X computer:

- **User profiles,** which contain settings for individual users or user groups, such as account names, passwords, and parental controls.
- **Device profiles,** which contain settings for individual devices or device groups, such as directory bindings, energy saver, and restrictions.

In OS X, a profile created for a device or device group is applied at the system level. A profile created for a user or user group is applied at the user level.

Types

There are three basic types of profiles that can be installed on an OS X computer: configuration profiles, managed profiles, and trust profiles.

Configuration profiles

Each user, user group, device, and device group can have a unique configuration profile with different settings. This allows organizations to quickly and easily share a basic level of settings for devices or people who need them and then further assign additional configuration profiles to customize the settings to meet the organization's requirements.

For example, to configure a teacher's MacBook Pro, you could create a user account for the teacher, then place that user in the "teachers" and "MacBook Pro" groups. This assigns two collections of default settings—one from each group—and you can then assign additional settings that are tailored to the user.

Other types of user and device groups that IT departments might find useful are "lab computers," "field sales computers," and "student computers." For example, for the field sales computers group, the default settings in the profile might include a restrictions payload and a VPN payload. Because both payloads are in the same profile, users must install both. If they remove the configuration profile to avoid the restrictions, their VPN access is also removed.

Managed profiles

Managed profiles are configuration profiles installed on devices by an MDM server. Like other configuration profiles, they can be locked to prevent end users from removing them. When you deploy managed profiles, the primary MDM profile manages anything delivered by MDM after enrollment and contains several "rights" to the system, including:

- Erase all data on this computer
- Add or remove configuration profiles
- Add or remove provisioning profiles
- Lock screen
- Query information about different settings including security, computer, network, installed applications, and installed profiles

There's no limit to the number of managed or unmanaged configuration profiles that can be installed on a device. The flexibility to install both types of profiles allows you to divide policies and settings into different profiles. For example, you may both permit end users to install multiple unlocked profiles for access to optional systems and require end users to install two locked managed profiles: one for access to the company network and another for enforcement of company security policies.

The MDM server updates and removes managed profiles. Because the primary MDM profile must be unlocked, end users can opt out of MDM at any time. If an end user decides to:

- **Opt out of MDM altogether**, removing all managed profiles and associated data, then the relationship between the MDM server and the end user's device is terminated without any notifications to the MDM server.
- **Remain under management** but remove one or more unlocked managed profiles (other than the primary MDM profile), then the device remains paired to the MDM server.

For example, if an end user removes a profile that contains Exchange settings, the MDM server removes associated profile settings from the device such as email, contacts, and calendars. Data isn't affected on the server. Any remaining unmanaged profiles are unaffected and the MDM server isn't notified that a device has opted out.

Trust profiles

Trust profiles are profiles generated by an MDM server that contain critical information, certificates, and security keys that, when installed on managed devices, help ensure that communication between the MDM server and the managed device is secure and authentic.

Structure and Format

A configuration profile is an XML file that you can use to distribute configuration information to OS X computers. These XML files store key-value pairs in a property list (.plist) format and have a .mobileconfig suffix in their filename.

Both OS X and iOS use the same file format for configuration profiles. This file, like many on OS X, contains XML information about the settings to be configured on the target devices. The data values in these configuration profiles are stored in Base64 encoding, and because these files are text files, any XML editor or text editor can read and write the .plist format.

Payloads

You can use configuration profiles to set up specific (single or multiple) settings for OS X computers. Each configuration profile contains one or more payloads, which are collections of a certain type of settings, such as settings for Wi-Fi or VPN.

When you create a new configuration profile, you can specify settings in one or more of the profile's payloads. Each payload setting field provides a brief description of its purpose and how it's used. Fields that require information are indicated with a white arrow within a red circle.

When viewing the contents of a configuration profile, you'll see that the payloads are arranged into standard key-value pairs. This allows you to read the file contents easily without extensive XML knowledge.

For example:

```
<key>PayloadType</key>
<string>com.apple.webClip.managed</string>
```

For the key named "PayloadType" the value is the string "com.apple.webClip.managed." This value indicates that the payload in this section of the configuration profile contains Web Clip information.

For more detailed information about the configuration profile format, see the example in Appendix C.

Creating Configuration Profiles

Overview

When you create a new configuration profile, you use a particular tool, discussed below, to specify settings in one or more of the profile's payloads. When using a GUI-based tool, such as Profile Manager, to create profiles, each payload setting field provides a brief description of its purpose and how it's used. In Profile Manager, required fields are indicated with a white arrow within a red circle.

Many of the payloads allow you to specify user names and passwords; if you omit this information, the end user must enter it when the profile is installed. As a best practice, payloads that include passwords should be distributed in an encrypted format to protect their contents.

Mandatory Keys

A configuration profile requires a few mandatory keys. A key is a required line of code that pertains to a specific functionality. If you decide to script your own profile, you must include the following standard keys:

- **PayloadVersion.** The PayloadVersion key describes the version of the configuration profile as a whole, not of the individual profiles within it.
- **PayloadUUID.** The PayloadUUID key is a globally unique identifier for the profile. Although its actual content is unimportant, it must be globally unique. In OS X, you can use the command `uuidgen(1)` to generate UUIDs.
- **PayloadType.** The PayloadType key supports only the value Configuration.
- **PayloadIdentifier.** The PayloadIdentifier key determines whether a new profile should replace an existing profile or be added.

Besides the standard keys, each payload type contains keys that are specific to that payload type.

For more detailed information about keys and payloads, see Appendix A.

General Settings

In addition to these mandatory keys, the General settings payload is the only required payload in a configuration profile. This payload sets the name and identifier of the configuration profile. You should use consistent naming conventions and clear descriptions with version numbers and dates to keep configuration profiles organized. It's important that you specify a unique identifier field for each configuration profile because any subsequent profile created with an identical identifier will replace the original. A good profile description is especially important for signed and

encrypted profiles, as they rely on the certificate keys of the tool that was used to create the profile.

The General settings payload is also used to specify whether end users can remove the profile after it's installed.

Multiple Payloads

A configuration profile can contain multiple payloads to configure multiple services and settings. For example, you can create separate Network payloads for both Wi-Fi and Ethernet.

Although it's possible to create a single configuration profile that contains all the payloads for a device or class of devices, creating separate configuration profiles for each type of information makes updates and distribution easier. A best practice is to group profiles that contain sensitive information, such as passwords. You might, for instance, group VPN and Wi-Fi payloads in a single configuration profile.

A timesaving best practice is to create one or more configuration profile templates and save them to a file on disk. Each template profile should define organizational policies that you want to enforce and will use again when creating other profiles.

Tools

You can create configuration profiles with a variety of tools and methods, including:

- Profile Manager, included as part of OS X Server
- Mobile Device Management (MDM) solutions from third-party providers
- Manually, by using a text editor or scripting solution

Profile Manager

Apple's MDM solution, Profile Manager, is included with Lion Server. With this software, you can create profiles for both OS X and iOS via a simple-to-use web application.

Profile Manager consists of three parts that work together to let you specify how clients are configured, how to administer devices, and how to deliver the configurations to users and devices.

Web-based administration tool

The Profile Manager web app is where you configure settings for devices, manage enrolled devices and device groups, and execute or monitor tasks on enrolled devices.

Self-service user portal

Profile Manager's user portal is an easy-to-use, secure website for distributing settings you defined with the administration tool. Users connect to the web-based portal from their OS X computer. Then, after they log in, the settings you assigned to them are available for download and installation. Users also utilize this site to enroll their OS X computers for mobile device management, if the organization is using Profile Manager as an MDM server.

Mobile Device Management server

Profile Manager also provides an MDM server so you can remotely manage enrolled computers running OS X computers and iOS devices. After a device is enrolled with Profile Manager, you can update the configuration over the network without user interaction, as well as execute tasks such as reporting or locking and wiping the device.

Important: Before you can create configuration profiles for your devices, make sure that the Profile Manager service is enabled and configured on your server. For more information on how to set up the Profile Manager service, refer to Profile Manager Help.

Third-Party MDM

You can also create configuration profiles with a third-party MDM solution. After a managed device is enrolled, it can be dynamically configured with settings and policies by the MDM server. The server sends configurations through a configuration profile to the devices and they're installed automatically.

Manually

Because configuration profiles are text-based XML files, you can use a standard text editor to manually write a configuration profile. This process can also be automated with a script. See Appendix C for a sample configuration profile in plain text.

Important: When creating profiles manually, it's important to remember which keys and payloads are mandatory as well as the structure, format, and content of the XML key-value pairs.

Securing Configuration Profiles

You can sign and encrypt configuration profiles to prevent them from being modified or viewed. You can also protect a configuration profile by locking it with a passcode so that an end user can't remove it.

Signing and Encryption

The payload data on a configuration profile can contain sensitive information such as account information and passwords. Profile Manager offers built-in security features to protect the data stored on a configuration profile.

A profile that's signed can be replaced only by another profile with the same identifier that's also signed by the same source. A profile that's encrypted guarantees data integrity and protects sensitive policy information. You can use Profile Manager to sign configuration profiles, restricting their use to a specific device and preventing anyone else from changing or seeing the settings that the profile contains.

The following security features are available when creating configuration profiles using Profile Manager:

- **None.** This option creates a plain-text .mobileconfig file that can be installed on any device. Some content in the file is disguised to prevent easy examination of the file's contents.
- **Sign Configuration Profile.**This option creates a signed .mobileconfig file that can be installed on any device as long as the profile hasn't been altered. After it's been installed, the profile can be updated only by another profile with the same identifier that's also signed by the same certificate.

Profile Manager can sign configuration profiles so devices can verify that they haven't been modified. This requires a code-signing certificate, which Profile Manager can generate for you. Alternatively, you can use a signing certificate with an established chain of trust. In the Profile Manager pane of the Server app, you can enable profile signing and select the installed code-signing certificate from the system keychain. You can then tell users to download the trust profile from the user portal to install the intermediate certificates to verify signed profiles.

As a best practice, you should sign configuration profiles, because a signed profile provides tampering detection.

Encryption

All communications between an MDM server and managed devices are encrypted. Profile Manager communicates with client devices over HTTPS using either Secure Sockets Layer (SSL) or Transport Security Layer (TLS). Configuration profiles are never transmitted in the clear from the Profile Manager server. This requirement for HTTPS communications means that the client devices must trust the Certificate Authority (CA) that issued the SSL certificates.

If you're using an SSL certificate signed by a CA that's known, then no further action is required. If you're using a self-signed certificate for Profile Manager services, then that root CA authority must be imported into the

clients before they can enroll. Profile Manager makes this process very simple.

If Profile Manager detects that it's being used with a self-signed certificate, it generates a trust profile. This profile can be downloaded from the Profile Manager administration tool, or a user can install it from the Downloads section of the My Devices user portal.

For additional security, you can enable profile code signing. This feature cryptographically signs each configuration profile with a code-signing certificate so that the device can validate that it was issued by your MDM service and that it hasn't been tampered with.

As with the SSL certificate, your client devices need to trust the CA that signed the code-signing certificate. If you have purchased a code-signing certificate, then no further action is needed. If you're using a self-signed certificate, then the users should install the Profile Manager trust profile before enrolling.

Deploying Configuration Profiles

Overview

After policies have been defined and configuration profiles have been created to enforce them, it's time to choose a deployment technique. There are several different ways to get configuration profiles installed on a Mac. Your organization should evaluate each of them to determine which method or combination of methods is appropriate.

Deploying configuration profiles to OS X computers involves two steps:

- Distributing the configuration profile, with the required root certificates and any necessary intermediate certificates, to the device
- Installing the configuration profile, with the root and intermediate certificates and user identity, onto the device

Distributing Profiles

You can download configuration profiles (.mobileconfig files) and trust profiles from Profile Manager's administration tool, then send them to users via email or post them to a website you've created. When users receive or download the file, they can install it on their OS X computer.

Manually via email

A more direct installation strategy is to email profiles directly to end users. This strategy is more common in smaller deployments or for distributing generalized policy settings such as Wi-Fi access points or Mobile Device Management (MDM) enrollment profiles. You can distribute configuration profiles as email attachments. The end user receives the email message on the OS X computer and then double-clicks the attachment to install the profile.

When distributing profiles via email, it's important to remember to not compress the file or change its file extension (.mobileconfig) so the OS X computer can recognize and install the file.

Manually via website

Because they're file based, profiles can be made available to users for download from any web or file server. In this deployment style, the standard Access Control Lists (ACLs) for the server can be used to determine which profiles a user has access to.

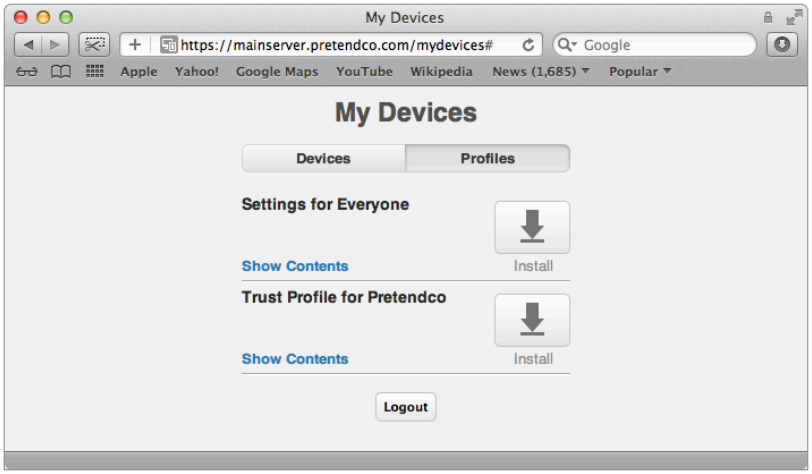
You can provide end users with a URL for a web page that contains a configuration profile. The end users can go to the web page on their OS X computer and download the profile.

When a configuration profile is ready for posting to a website, you shouldn't compress the .mobileconfig file or change its extension, or the OS X computer won't recognize or install the profile.

Manually via a self-service portal

You can use Profile Manager's built-in user portal to distribute configuration profiles to users for manual installation. When users log in, they see the profiles you assigned and can download each profile. On enrolled OS X computers, installation begins automatically.

Users can download and install the configuration profiles with the settings and the trust profiles with the certificates from Profile Manager's built-in user portal. The user portal ensures that users receive the configuration profiles that were assigned to them or their group.



Automatically via MDM

You can distribute configuration profiles to enrolled OS X computers automatically with an MDM server. For example, you can enable Profile Manager's MDM server, which allows you to remotely install, remove, and update configuration profiles and certificates on enrolled OS X computers. This allows you to automatically distribute configuration profiles to OS X computers over the network: by email, by website, and wirelessly over the air. When an end user downloads the profile from the web or opens it as an attachment in Mail, the OS X computer recognizes the .mobileconfig extension as a profile and begins installation when the user double-clicks the attached profile.

Wirelessly

Configuration profiles can be distributed wirelessly to OS X computers by using a secure enrollment and configuration process enabled by the Simple Certificate Enrollment Protocol (SCEP) to distribute encrypted

configuration profiles. This method requires some IT infrastructure but provides a highly scalable method for configuring OS X computers.

If you decide to distribute your configuration profiles wirelessly with Over-the-Air Enrollment, you should also consider an MDM solution.

Installing Profiles

The most basic delivery method is to deliver configuration profile files to users, who can install them with a double click.

To generate a configuration profile for manual installation using Apple's Profile Manager, you simply configure the desired settings and then click the Download button in the profile information screen.

When users install configuration profiles, they'll be prompted to review the profile's contents. Installation of profiles may require administrator privileges on the Mac, depending on the settings to be managed. During installation, the end user must enter necessary information (such as passwords) that wasn't specified in the profile and other information as required by the settings you specified. The user is also asked to enter passwords necessary to use certificates included in the profile.

As part of the installation process, the device retrieves Exchange policies from the server or policies from an MDM server and refreshes them. If the device or Exchange policies enforce a passcode setting, the end user must enter a passcode that complies with the policy to complete the installation.

If the installation isn't completed successfully, none of the information entered by the end user is retained.

Manually via Finder

Profiles can be installed manually by simply copying the profile to a location that the user has access to on the OS X computer, such as the Finder's Desktop, and then double-clicking the profile to install it.

After the profile is installed, the profile name will appear in the Profiles pane in System Preferences. The Profiles pane lists all user and device profiles installed on the system, including Remote Management and trust profiles. Users can review the details associated with each profile and add and remove profiles.

Automatically via Apple Remote Desktop

You may want to automatically install profiles with client management software such as Apple Remote Desktop. With built-in support for remote file copy, package installation, AppleScript, Automator Actions, and UNIX shell scripting, Apple Remote Desktop provides flexible and powerful options for installing and managing software on large numbers of OS X computers.

Automatically via System Image Utility

System Image Utility (SIU) includes support for configuration profile installation. Beginning with OS X, SIU has been expanded with an Automator action named "Add Configuration Profiles." Using this action, you can include configuration profiles to be applied in both NetInstall and NetRestore deployment images.

To use the Automator action, simply drag it from the SIU Library to a new or existing workflow. Then add your profiles and arrange them in the order you wish them to be installed. Pay close attention to the order of installation: Profiles such as root CA certificates typically should be installed before profiles containing payloads such as 802.1X and VPN settings.

Automatically via Terminal (Command-line)

Configuration profiles can be managed from the command line, or via a script, by using Terminal's `profiles` command. With this tool, you can install, query, and remove both user- and system-level configuration and provisioning profiles. This tool is simple to script with standard shell scripts, Apple Remote Desktop, or as a post-flight script within an Installer Package.

The `profiles` utility ignores the PayloadScope key that determines whether a policy should apply to the system or user domains. The `profiles` tool installs configuration profiles for the system if executed with root privileges. Running the tool as a normal user results in the policy settings being applied to the user domain.

Important: The `profiles` tool is located in the `/usr/bin` directory and should not be moved. Moving the binary may result in unexpected behavior.

To install a configuration profile called 'testfile.mobileconfig' into the current user: `profiles -I -F /testfile.mobileconfig`

To remove the configuration profile '/profiles/testfile2.mobileconfig' from the current user: `profiles -R -F /profiles/testfile2.mobileconfig`

To display information about the installed configuration profiles for the current user: `profiles -L`

To learn more about the `profiles` command, launch Terminal and type `man profiles` at the prompt.

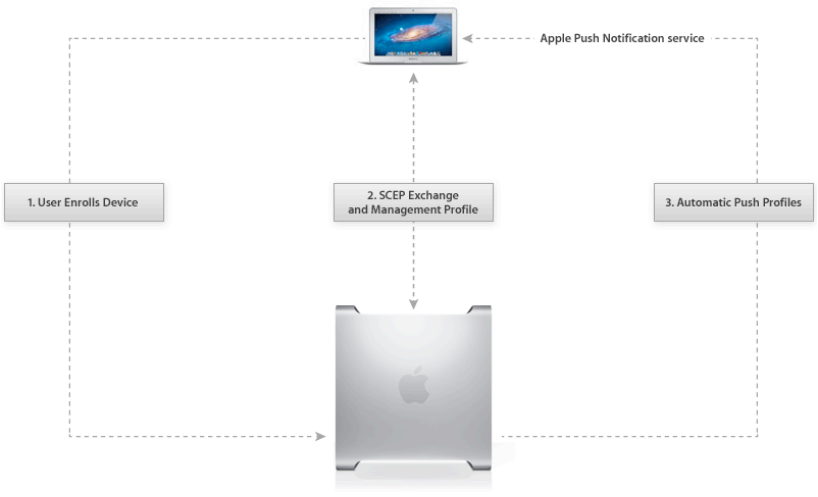
Mobile Device Management

If you require more comprehensive control and provisioning, then an MDM system may meet your organization's needs. A variety of vendors supply MDM systems that work with OS X. Profile Manager, included with OS X Server, is used as an example in this document, but the basic process and profile payload compatibility of all MDM solutions is the same.

A MDM solution allows for automated deployment of configuration profiles based on the user and device identities. This reduces the effort in deployment to simply defining the profile settings and scope. Devices may either be enrolled using an enrollment profile or by the users in a self-service portal. After enrollment, settings may be pushed to devices, hardware and software inventory is taken, and loss-prevention techniques such as remote lock and wipe are available.

MDM overview

The basic workflow of MDM is simple, with options to allow users to self-enroll devices or to provide enrollment profiles. If enrollment profiles are used, then the devices aren't associated with any particular user account. This prevents those devices from being managed with automatic push profiles that are user- or user group–based. For that reason, they're often used for shared devices such as lab workstations or kiosks.



A simplified MDM workflow

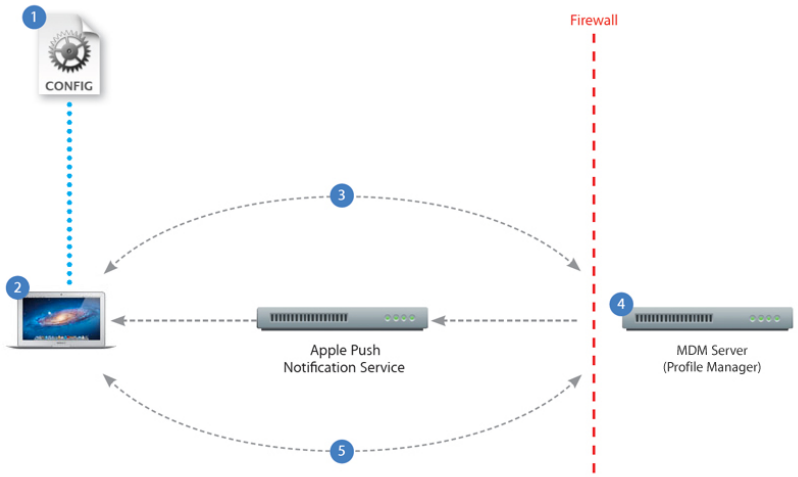
The first step in the process is for a user to enroll a device. In this example, the user can simply log in to the My Devices portal of Profile Manager and click a button to enroll the Mac.

After the user initiates the enrollment process, Safari will download an Over-the-Air Enrollment profile. This is automatically opened by the Profiles pane in System Preferences.

After the user accepts the OTA profile, a Simple Certificate Enrollment Protocol (SCEP) transaction takes place. The SCEP process securely generates a certificate to uniquely identify the client device to the MDM service.

To complete the enrollment phase, a management profile is delivered to the client. This profile places the Mac under management and immediately allows for automatic push profiles to be delivered and for remote lock and wipe. These abilities are made clear to users at the time of enrollment, and they must accept the management profile to complete the process.

After the enrollment process is complete, the MDM service will determine what, if any, profiles need to be pushed automatically to OS X computers. When an applicable configuration profile is found, a push notification for the client is created and sent. When the client receives the push notification from APNs, it contacts the MDM server over SSL and checks for any updated configuration profiles to be delivered. These profiles are then downloaded and automatically applied.



1. A Configuration Profile containing Mobile Device Management server information is sent to the computer. 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 computer being managed.
3. Enrollment takes place as the profile is installed. The server validates the computer and allows access.
4. The server sends a push notification prompting the computer to check in for tasks or queries.

5. The computer connects directly to the server over HTTPS. The server sends commands or requests information.

Enrolling devices

Before OS X computers can be configured and managed remotely, they must be individually enrolled for management with Profile Manager. Computer owners must install an enrollment profile to enroll the OS X computer with the server. You can allow users to enroll their OS X computers themselves with Profile Manager's user portal. After an OS X computer is enrolled, configuration profiles you update or send to users, devices, or device groups are installed without user interaction.

SCEP

A key part of the enrollment process is the Simple Certificate Enrollment Protocol process. When used with a MDM system, SCEP fulfills two key roles:

- It provides a conduit for certificates to be exchanged between the MDM server and the Lion client.
- It provides access to a Certificate Revocation List (CRL) so that the client can validate the credentials and certificates that are used to sign configuration profiles.

Important: For SCEP to function properly, the client needs to be able to access the server via HTTP on port 1640. Without this access, MDM won't work.

Manually downloading profiles

Manually installed profiles provide a simple way to place policies generated by Profile Manager on an OS X computer without the need for the Apple Push Notification service or even MDM enrollment. However, any changes made to these configuration profiles after they're installed won't be automatically sent to the clients.

Download profiles are often used for fairly static policy payloads such as the MDM trust profile or Wi-Fi access settings.

Assigned by groups

When creating download profiles in Profile Manager, you can assign them to devices, users, or groups of either kind. This allows you to easily define which users will have access to specific configuration profiles.

Global profiles, such as a trust profile, are available to all users.

Downloading profiles from the user portal

Profile Manager's user portal is an easy-to-use, secure website for distributing settings you define using the administration tool. Users

connect to the web-based portal from their OS X computer. When they log in to the My Devices portal page, the settings that you assigned to them are available for download and installation on the Profiles tab.

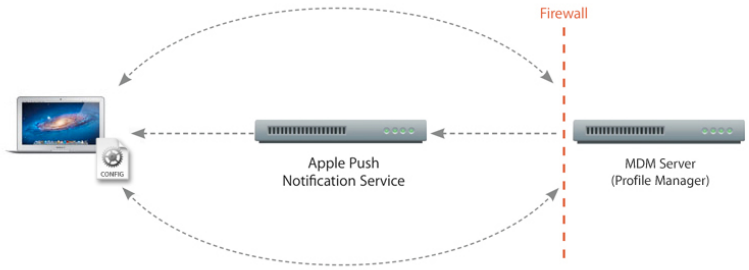
Each download profile is listed, and users can view the contents of the payload before they install them. After their choices have been made, clicking the Install button next to each profile will install it.

Important: Before you can install configuration profiles on your OS X computers using Profile Manager's user portal, you need to make sure that the Profile Manager service is enabled and configured on your server. For details on how to set up the Profile Manager service, refer to Profile Manager Help.

MDM and the Apple Push Notification service

When an MDM server wants to communicate with an enrolled OS X computer, a silent notification is sent to the computer via the Apple Push Notification service, prompting it to check in with the server. The process of notifying the computer doesn't send any proprietary information to or from the Apple Push Notification service. The only task performed by the push notification is to wake the computer so it checks in with the MDM server. All configuration information, settings, and queries are sent directly from the server to the OS X computer over an encrypted SSL/TLS connection between the computer and the MDM server. MDM requests and actions are handled 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. After the Apple Push Notification certificate is uploaded into the MDM server, computers 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 OS X computers are behind a firewall, you may need to do some network configuration for the MDM service to function properly. To send notifications from an MDM server to Apple Push Notification service, TCP port 2195 needs to be open. To reach the feedback service, TCP port 2196 needs 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 host name rather than by IP address. The push service uses a load-balancing scheme that yields a different IP address for the same host name. This host name 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 the Troubleshooting Push Notifications developer technical note TN2265 in the developer library at https://developer.apple.com/library/mac/#technotes/tn2265/_index.html.

The most flexible way to deploy settings is by automatically pushing profiles from the MDM server to the OS X computers. This allows for policies to be deployed and updated without any interaction from the user and ensures that profiles are always up to date. After an OS X computer is enrolled with your MDM service, you can automatically distribute the settings in an automatic push profile without having to manually connect each OS X computer to your MDM server.

The key to automatically pushing profiles from an MDM server, such as Profile Manager, is the Apple Push Notification service.

The Apple Push Notification service (APNs) is managed by Apple and allows MDM services to send messages, called push notifications, about configuration profile availability or changes to managed OS X computers and iOS devices. When setting up an instance of Profile Manager, the Server app on Lion Server guides you through the process of obtaining the certificates needed to use APNs.

After the device establishes communication with APNs, it will maintain the connection to listen for push notifications. Because of this, no inbound port mapping is needed.

A simplified overview of the push notification process looks like this:

1. An application that uses APNs connects to the service using its push notification service certificates.
2. After authentication, the service sends a JSON formatted property list to the APNs. The APNs will reject any notification that is larger than 256 bytes.

3. Using the device token in the notification payload, APNs locates and delivers the notification to the client.

For OS X computers and your MDM server to communicate with APNs, they need to be able to reach the Apple network on TCP ports 5223, 2195, and 2196. Apple doesn't publish a range of IP addresses for the service, so you should allow that traffic to reach the 17.0.0.0 network in order to provide maximum flexibility in scaling the service. The entire 17-net is safely maintained and securely controlled by Apple.

Profile notification

When a change is needed for the profile payload on a managed device, the MDM server will send a push notification to that particular device or group of devices. The only content in the notification payload is that the device needs to check with the MDM server for updated configuration profiles.

Important: Policy information is never transmitted in a notification message, and managed devices do NOT send any data back through APNs.

When the client receives the push notification it checks with Profile Manager via SSL for any updated settings and applies them. After the profiles have been updated, the MDM client will update its information with the server to indicate its new status.

This process is fast, secure, and completely transparent to the user.

Editing and Removing Configuration Profiles

You can update a manually installed profile by distributing a new profile to the end user as long as the unique identifier matches and the new profile (if signed) is signed by the same source.

When an updated profile is installed on the OS X computer, it compares the Identifier value with profiles that are already on the device. When the identifier on the new profile is unique, the profile is added to the device. When the identifier matches a profile already installed, information in the profile replaces the settings already on the device (except in the case of Exchange settings).

If you use an MDM solution, such as OS X Server's Profile Manager service, to manage configuration profiles, you can use it to update and remove profiles over the air.

Editing

You can use an MDM solution, such as Profile Manager, to edit existing configuration profiles. To use the updated profile to replace one that end users have already installed, you should use the same value in the Identifier field of the General settings payload.

Important: Before you can update configuration profiles on your devices with Profile Manager, you need to make sure that the Profile Manager service is enabled and configured on your server and that devices have been enrolled for management with the server. For details on how to set up the Profile Manager service and enroll devices, refer to Profile Manager Help.

Removing profiles

Profiles can be removed from OS X computers in several different ways. Users can remove profiles themselves manually by using the Profiles pane in System Preferences or by using the `profiles` command the Terminal command line application.

Profiles can also be removed remotely from managed devices using an MDM server, which sends commands through the Apple Push Notification service.

Removing profiles from devices depends on the lock status of the profile. For unlocked profiles, the user can remove profiles manually. You can also distribute a profile that's locked to a device, so that after it's installed, it can be removed only by wiping the device of all data or, optionally, by entering a passcode. Locking a configuration profile is recommended to prevent end users from deleting it from a device. The following options are available for locking:

- **Always.** This option allows the end user to remove the profile at any time.
- **With Authorization.** This option lets you specify an authorization password that permits the removal of the profile on the device.
- **Never.** This option allows the profile to be updated with a new version but not removed.

Resources

Configuration profiles reference

Profile Manager Help: About configuration profiles

Certificates

Apple Push Certificates Portal

Troubleshooting Push Notifications

Mac OS X 10.7 Help: About certificates

Mac OS X 10.7 Help: If your certificate isn't being accepted

Mail 10.7 Help: Trust a certificate

Certificate trust policies

How to request a certificate from a Microsoft Certificate Authority using the ADCertificatePayloadPlugin

OS X Server

Profile Manager Help

OS X Server: Using the Profile Manager or Wiki service with Active Directory or third-party LDAP services

OS X Server: Installing profiles that require user interaction

OS X Server Help: Provide user configuration profiles

OS X Server - Technical Specifications

OS X Server Help: About tools for client management

Well known TCP and UDP ports used by Apple software products

Appendix A: Profile Reference

User Profile Payload Reference

The following payloads can be configured for User and User Group configuration profiles on OS X computers.

General	Profile distribution type Organization Description Security
Passcode	Allow simple value Require alphanumeric values Minimum passcode length Minimum number of complex characters Maximum passcode age (in days) Auto-lock (in minutes) Maximum number of failed attempts
Email	IMAP account configuration POP account configuration SMTP account configuration
Exchange	Exchange account configuration
LDAP	Contacts LDAP configuration
CardDAV	Contacts LDAP configuration
CalDAV	Calendar server account configuration
Network	Network Interface (Ethernet or Wi-Fi) Use as Login Window (Device Profiles) SSID (Wi-Fi) Hidden Network (Wi-Fi) Auto Join (Wi-Fi) Proxy Setup (Wi-Fi) Security Type (Wi-Fi) Network Security Settings (Protocols and Trust) Accepted EAP Types (Wi-Fi)
VPN	VPN proxy settings
Certificate	X.509 certificates
SCEP	SCEP server settings
Web Clips	Web Clip payload
Security & Privacy	Usage and diagnostic information opt-out
Restrictions	Preference Pane access Application launch controls Widget launch controls Media access controls
iChat	Jabber account settings AIM account settings
Login Items	Auto-open applications Auto-open items Auto-connect network mounts

Mobility	Mobile account creation Mobile account expiry Portable home directory sync rules
Dock	Dock item settings Dock appearance setting
Printing	Printer list configuration Print job footers
Parental Controls	Content filtering Time limits
Custom	Arbitrary application preferences

Device Profile Payload Reference

The following payloads can be configured for Device and Device Group configuration profiles on OS X computers.

General	Profile distribution type Organization Description Security
Passcode	Allow simple value Require alphanumeric value Minimum passcode length Minimum number of complex characters Maximum passcode age (in days) Auto-Lock (in minutes) Maximum number of failed attempts
Network	Network Interface (Ethernet or Wi-Fi) Use as Login Window (Device Profiles) SSID (Wi-Fi) Hidden Network (Wi-Fi) Auto Join (Wi-Fi) Proxy Setup (Wi-Fi) Security Type (Wi-Fi) Network Security Settings (Protocols and Trust) Accepted EAP Types (Wi-Fi)
VPN	VPN proxy settings
Certificate	X.509 certificates
SCEP	SCEP server settings
Security & Privacy	Usage and diagnostic information opt-out
Restrictions	Preferences pane access Application launch controls Widget launch controls Media access controls
Directory	Active Directory binding settings Open Directory binding settings
Login Window	Login panel heading Login window message Login window style
Login Items	Auto-open applications Auto-open items Auto-connect network mounts

Mobility	Mobile Account creation Mobile Account expiry Portable Home Directory sync rules
Dock	Dock item settings Dock appearance setting
Software Update	Software Update Server settings
Printing	Printer list configuration Print job footers
Energy Saver	System sleep settings Display sleep settings Scheduled sleep/wake settings
Parental Control	Content filtering Time limits
Custom	Arbitrary application preferences

Appendix B: Service Port Reference

Required TCP Ports for Profile Manager

Service	TCP Ports
HTTP	80
HTTPS	443
SCEP	1640
APNs	5223, 2195, and 2196

Appendix C: Example Profiles

Example Device Configuration Profile

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN""http://
www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

    <key>PayloadDescription</key>

    <string>Sample Device configuration profile</string>

    <key>PayloadDisplayName</key>

    <string>Settings for Example Device</string>

    <key>PayloadIdentifier</key>

    <string>com.apple.mdm.mainserver.pretendco.com.
850bb6c0-45ee-012f-27bb-482a140c4fbd.alacarte</string>

    <key>PayloadOrganization</key>

    <string>Pretendco</string>

    <key>PayloadRemovalDisallowed</key>

    <false/>

    <key>PayloadScope</key>

    <string>System</string>

    <key>PayloadType</key>

    <string>Configuration</string>

    <key>PayloadUUID</key>

    <string>850bb6c0-45ee-012f-27bb-482a140c4fbd</string>

    <key>PayloadVersion</key>

    <integer>1</integer>

</dict>

</plist>
```

Example User Configuration Profile

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN""http://
www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

    <key>PayloadDescription</key>

    <string>Sample user configuration profile</string>

    <key>PayloadDisplayName</key>

    <string>Settings for User 01</string>

    <key>PayloadIdentifier</key>

    <string>com.apple.mdm.mainserver.pretendco.com.
3a3b4a60-45ec-012f-27a6-482a140c4fbd.alacarte</string>

    <key>PayloadOrganization</key>

    <string>Pretendco</string>

    <key>PayloadRemovalDisallowed</key>

    <false/>

    <key>PayloadScope</key>

    <string>User</string>

    <key>PayloadType</key>

    <string>Configuration</string>

    <key>PayloadUUID</key>

    <string>3a3b4a60-45ec-012f-27a6-482a140c4fbd</string>

    <key>PayloadVersion</key>

    <integer>1</integer>

</dict>

</plist>
```

03-29-2012