nWalker.org

Technology questions and answers

The Complete Guide to Profile Manager (Part 1)

In order to have easy, complete control over your devices and user accounts, OS X Server includes Profile Manager, a tool for managing Macs, iOS devices, and users on both platforms.

Profile Manager will work with iOS devices running iOS 3 or later (device enrollment is only supported on iOS 4.1 or later) and Macs running OS X Lion (10.7) or later.

Managing Devices

In order to manage devices, you must first enable Profile Manager on your server. Open Server.app and enable the Profile Manager service. The Web service is also required to run the Profile Manager server.

Now, you'll need to use the Profile Manager web interface to manage your users and devices. The Profile Manager web interface can be accessed in two different ways. In the Profile Manager section of Server.app, you can click "Open Profile Manager" in the lower right of the window. Alternatively, you can visit https://your-server-address/profilemanager. If necessary, use a server administrator account to login to Profile Manager.

Now, you'll see the Profile Manager interface, which consists of three columns. In the left column is a list of Profile Manager sections. In this column are two primary sections: Library and Activity. In the Library section, you will find all four categories: Devices for managed devices, Device Groups for groups of managed devices, Users for all of your server's users, and Groups for all of your managed groups. You can use these categories to deploy profiles, sets of configuration information, to users and devices.

Devices

One of the basic categories that you can deploy profiles to is devices. This category shows all of your managed devices at once, and you can deploy profiles to them individually from here. Devices cannot be added directly to

Profile Manager; they must be enrolled first. Device enrollment will be covered shortly. However, before a device is enrolled, you can add placeholders for expected devices.

While in the Devices category, click the plus button in the center column. Next, press “Add Placeholder”. You can give an expected device a name for management purposes here. You must also give an identification number (serial number, UDID, IMEI, or MEID), so Profile Manager can identify the device when it is enrolled.

Placeholders can also be created in bulk. Just go to the same plus icon in the center column and press “Import Placeholders”. Next, you need to import a CSV file containing device information. This CSV file (which can be exported from Excel, Numbers, or LibreOffice Calc) must be formatted as such:

- The following header rows:
  - DeviceName
  - SerialNumber
  - UDID
  - IMEI
  - MEID
- A Windows-formatted CSV (not really sure why)
  - Check your spreadsheet application for a Windows CSV export option
  - If there isn’t a Windows CSV option, follow these steps:
    - Export as a regular CSV file
    - Open the Terminal. You can find this in Applications -> Utilities -> Terminal.
    - Type in `nano FILEPATH` (if you don’t want to type the file path, you can just drag and drop the file into the terminal after typing `nano` to add the file path). Press return.
    - Press Control+O. Then, press Escape+D. Press return. Finally, press Control-X.
    - Now, your CSV file will be formatted in Windows format.

After importing your CSV file, you will get an option to create a Device Group based on this import. If you ever plan on configuring these devices as a group, you’ll want to do this. There is no reason not to do this to be safe, so I recommend it.

Device Groups

Device Groups are simply a way to group a number of devices together for management. As previously mentioned, these can be automatically created when importing device placeholders. You can also create device groups manually.

To create a device group, go to the Device Groups category and click on the plus sign in the center column. Type in a name for your device group. Click on the plus sign in the right column and click “Add Devices” or “Add Device Groups”. You can now add devices individually or filter them by name and add them to your group.

Users and Groups

Users and Groups in Profile Manager are pulled from the pre-established users and groups in Server.app. You can manage them there.

Creating a Profile

A profile is a package of settings used to configure a device or user’s account. These profiles can apply to a device, device group, user, or user group. In order to add a profile:

- Select the device, device group, user, or group that you wish to configure.
- Make sure that you are on the Profile tab.
- Under “Settings for NAME”, select “Edit”.
- From here, you can edit your profile.

How to configure a profile will be covered shortly, but first, we’ll discuss how to apply a profile to your devices.

Deploying a Profile

Now that you have a profile created, you’ll want to send it to your devices, so the settings can take effect. You can do this by either manually installing all profiles or by having profiles automatically pushed to devices.

Manual Profile Install

The first way that you can deploy profiles is by having them manually installed on each device and/or user account. In order to do this, just download each profile using the “Download” button next to “Edit” and send it (via email or some other means) to whom you want to install it. Then, the user can simply open the profile and press “Install”. However, this method is inefficient as you will need to reinstall the profile every time that you wish to change or update the profile.

Automatic Push

The best way to install profiles is through Automatic Push to devices, which only requires a one time install process. There are two ways to set up Automatic Push: via a web interface or via an Enrollment Profile.

Web Interface

To install profiles using the web interface, you must direct users on your network to a certain page to add the profile to their device. The URL for this page is https://your-server-address/mydevices. After logging in, the user can just press the blue "Enroll" button to allow the device to be managed. Then, the user will go through the Manual Profile Install procedure for their device.

Enrollment Profiles

In order to save the user from the hassle of logging in and enrolling their device, you can configure their device to be managed through an Enrollment Profile. This is a special type of profile that configures a device to be managed. Just like any other profile, you can simply email this profile to a user, so they can install it on their device.

In order to create an Enrollment Profile, go to Profile Manager and click on the plus sign in the left column. Then, select "Enrollment Profile". Give your profile a name. Enrollment Profiles only have one option: whether or not you want to restrict your profile to devices with placeholders. In order to download your enrollment profile, press the "Download" button in the lower-right corner.

Enrollment Profiles can be installed using the Manual Profile Install procedure.

Apple Configurator

Enrollment Profiles can also be installed using Apple's free Configurator tool available in the Mac App Store. However, this method only works with iOS devices and requires a wipe of all data on the device, so this is only recommended for the initial setup of a new device.

Trust Profile

Profile Manager also creates one profile that you may want to have the user install before any other profiles: the Trust Profile. Every profile created with Profile Manager is signed with a digital certificate, but most of these are signed with a certificate from your server, so you need to configure your devices to recognize your server as a Certificate Authority. In order to do this, you will need to install your Trust Profile.

The Trust Profile can be installed via the My Devices web interface or by manual install. In the My Devices interface, have the user go to the Profiles tab and install the Trust Profile. To distribute your Trust Profile by other means, you can download it by clicking on your name in the top-right of Profile Manager.

Variables

Before you start creating profiles, there is one more component that you should know about: variables. Variables allow you to have custom information for each user, so that, for example, each user will have their own username for each mail account. Every variable for Profile Manager is contained in percentage signs (%). The available variables are:

VARIABLE	DESCRIPTION	EXAMPLE	DATA SOURCE
%first_name%	The first name of the user.	Jack	Open Directory
%last_name%	The last name of the user.	Harkness	Open Directory
%full_name%	The full name of the user.	Jack Harkness	Open Directory
%short_name%	The shortened name of the user. Typically used as a username.	jharkness	Open Directory
%job_title%	The job title of the user.	Captain	Open Directory
%email%	The email address of the user.	jharkness@example.com	Open Directory
%mobile_phone%	The mobile phone number of the user.	555-555-0123	Open Directory
%guid%	The system identification number of the user.	103	Open Directory
%ProductName%	The name of the device.	MacBook Air	Device Record (Profile Manager)
%SerialNumber%	The serial number of the device.	XYZ1234AB	Device Record (Profile Manager)
%OSVersion%	The version of the operating system on the device.	10.8.1	Device Record (Profile Manager)
%BuildVersion%	The build number of the operating system on the device.	31C96	Device Record (Profile Manager)
%WIFIMAC%	The MAC address of the Wi-Fi interface of the de-	01:23:45:67:89:ab	Device Record (Pro-

	vice.		file Manager)
%IMEI%	The IMEI number of the device. Typically only found on iPhones.	AA-BBBBBB-CCCCCC-D	Device Record (Profile Manager)
%ICCID%	The ICCID number of the device's SIM card.	1234 5678 9009 8765 432	Device Record (Profile Manager)

You can place the variables in almost any field in Profile Manager. Apple also offers special variables for configuring Ethernet on an enterprise network at http://help.apple.com/profilemanager/mac/2.1/#apd073333AA-30C6-4FD2-B2E0-E0C95658A2C4.

Now, let's get into the specific settings for your profiles, starting with settings for both OS X and iOS.

OS X and iOS

These settings in Profile Manager are functional for both Mac OS X and iOS. Some specific options may be platform specific. These cases will be noted below. Also, any settings that would only reasonably apply to one user (for example, Calendar or anything else with a login) can only be managed on a per user basis for OS X and iOS or on a per device basis for iOS (as iOS devices only have one running user).

General

Profile Distribution Type
How the profile will be applied to devices. Profile Manager offers two choices: Automatic Push and Manual Download. Automatic Push will have the profile automatically applied to any managed devices that apply. Manual Download requires the user to login to Profile Manager to install the profile. The profile could also be distributed through a web page or an email message.

Organization
The name of your organization. Typically configured in the server settings and cannot be changed in Profile Manager.

Description
A description of the purpose of the profile. Displayed to the user if manually installed.

Security

Controls if the user can remove the profile. There are three possible options:

- Always: Can always be removed
- With authorization: Can be removed with a password set in Profile Manager
- Never: Requires an operating system reinstall on OS X or a device restore on iOS to remove the profile

Automatically Remove Profile
If enabled, the profile will automatically remove itself when you set it to, either on a specific date or after a certain number of days

Passcode

Allow simple value
Allows the user to use a poor passcode. For example, 1234 or 1111.

Require alphanumeric value
Requires at least one letter in the password.

Minimum passcode length
Sets the minimum number of characters in a passcode

Minimum number of complex characters
Sets the minimum number of symbols in the passcode

Maximum passcode age
Sets the number of days before a user must change his/her passcode

Maximum Auto-Lock
Sets the time after which the phone automatically locks itself

Passcode history
Sets the number of different passcodes that must be used before one can be reused. iOS only feature.

Maximum grace period for device lock
The maximum amount of time after locking the device before a passcode is required to unlock the device. iOS only.

Maximum number of failed attempts
The maximum number of incorrect passcodes that can be entered in a row before the device's data is erased

Mail

These settings allow you to configure an IMAP or POP account on your device. SMTP is used for outgoing mail.

Account Description
The name of the account. Appears in Settings on iOS, System Preferences on OS X, and in the Mail app.

Account Type
The protocol used to access the mail account. Options are POP (an older protocol) and IMAP (the current email protocol).

Display Name
The name of the user. Appears in the "From" field on outgoing email. I suggest using variables here.

Email Address
The address of the account. I suggest using variables here.

Allow messages to be moved
Allows messages from this account to be moved into another account. If unchecked, messages cannot leave folders within this account.

Allow recent addresses to be synced
Syncs the addresses that mail has been recently sent to.

Use Only in Mail
Only allows outgoing mail from official Mail app. Mail cannot be sent from any third party apps using this account.

Incoming and Outgoing Mail
Settings to access your mail server. If you leave the password blank, the user will be prompted for it. Variables are recommended for the "User Name" field.

If you use the plus (+) icon in the top right, you can add additional accounts and configure them using the same settings.

Exchange

Exchange settings are very similar to Mail settings. If you are using an Exchange server, you shouldn't have an issue filling in the account information.

Contacts

The Contacts payload allows you to configure a CardDAV account. CardDAV is primarily used by OS X Server and iCloud, so you can typically use the automatic configuration option for this.

Account Description
The name of the account. Appears in Settings on iOS, System Preferences on OS X, and in the Contacts app.

Account Hostname and Port
The address (either resolved DNS or IP address) for the CardDAV server. In the second box, input the port that the server is operating at. If you are unsure, it is probably the default, 8843.

Principal URL
A CardDAV option. If your server doesn't provide this information, you can safely leave it blank.

Account Username
The username for the server account. You'll probably want to use the username variable for this.

Account Password
The password for the server account. You'll probably want to leave this blank and allow the user to enter his/her own password.

Use SSL
Enable a secure, encrypted connection to the CardDAV server. If your server supports this, I recommend enabling this to prevent eavesdropping on the connection.

If you use the plus (+) icon in the top right, you can add additional accounts and configure them using the same settings.

Calendar

The Calendar payload allows you to configure a CalDAV account.

Account Description
The name of the account. Appears in Settings on iOS, System Preferences on OS X, and in the Contacts app.

Account Hostname and Port
The address (either resolved DNS or IP address) for the CalDAV server. In the second box, input the port that the server is operating at. If you are unsure, it is probably the default, 8843.

Principal URL
A CalDAV option. If your server doesn't provide this information, you can safely leave it blank.

Account Username
The username for the server account. You'll probably want to use the username variable for this.

Account Password
The password for the server account. You'll probably want to leave this blank and allow the user to enter his/her own password.

Use SSL
Enable a secure, encrypted connection to the CalDAV server. If your server supports this, I recommend enabling this to prevent eavesdropping on the connection.

If you use the plus (+) icon in the top right, you can add additional accounts and configure them using the same settings.

Network

Allows you to configure the network connection on the device. Supports Wi-Fi and Ethernet connections only.

Network Interface
The method of connecting to the network. Only two can be configured: Wi-Fi and Ethernet. Ethernet will only apply to OS X devices. Settings differ based on interface, so the following will be split based on the interface.

Wi-Fi settings

Service Set Identifier

Essentially, the name of the wireless network. Can be set in router settings.

Hidden Network

Your router may have the option to hide the SSID of your network from public view. Check this box if you have enabled this.

Auto Join

Check this box if you want the device to automatically connect to the wireless network if the network is in range

Proxy Setup

Some networks require a proxy to use the network. If you use a proxy, you may input the configuration information here. This setting has three choices:

- None (no proxy)
- Manual (manually enter proxy settings)
- Automatic (retrieve proxy settings from a URL)

Security Type

The type of security that your network uses for authentication. Consult your network system for your network security type.

Ethernet (available only for OS X)

Network Security Settings

The authentication protocol for the network. If you are using an enterprise-class network, you must set up your router's authentication system here.

VPN

These settings configure a VPN on your Mac or iOS device. If you are using a VPN with OS X Server, we will cover these configuration settings in the VPN chapter. If you are using another VPN, you may simply enter your VPN configuration information in this payload.

Certificate

This payload allows you to add any encryption certificates to your device. This can be internal certificates, so you can encrypt your internal sites. Or, you could use certificates for any other form of encryption that you may need. Certificates can also be used in the Network settings to access an enterprise network. These settings will probably not be used in most instances. This payload has three settings:

Certificate Name
A name of the certificate that will be displayed on the user's device.

Certificate or Identity Data
The certificate file using the X.509 standard.

Passphrase
A passphrase that encrypts the contents of the certificate. The user will be required to enter this in order to install the profile.

SCEP

Use these settings to access a SCEP server, if you have one. Most users will not be using this, so it is beyond the scope of this book.

Web Clips

A web clip is essentially a link that can be installed on a device's home screen (on iOS) or Dock (on OS X). An unlimited number of these can be added to a user's device. When managing a device, this option will be displayed under the iOS settings, as web clips can only be managed by user on OS X. Note that on OS X, the web clip will always open in the default browser.

Label
The name of the web clip. Displayed beneath the app icon on iOS and on the OS X Dock.

URL
The web address that you want to be displayed.

Removable (iOS only)
Whether or not the web clip can be removed from the device. On OS X, the web clip can always be re-

moved from the Dock.

Icon
The web clip's icon. Will be displayed on both iOS and OS X.

Precomposed Icon (iOS only)
Removes the glossy effect applied to iOS icons. Visible in icon preview in Profile Manager.

Full Screen (iOS only)
Makes the web clip a standalone application. Otherwise, the web clip will simply open in Safari.

Security and Privacy

This are some basic security settings for your users and devices.

Send diagnostic and usage data to Apple
Controls whether or not your devices automatically send anonymous data to Apple to improve iOS and OS X.

Do not allow user to override Gatekeeper setting (OS X only)
Controls whether or not the user can override OS X's Gatekeeper feature, which can restrict which types of applications can run on a system.

Conclusion

That's it for the first part of the Profile Manager guide. Part 2 and Part 3 are coming soon, so keep checking back.

This entry was posted in Mac Server Book and tagged iOS, mac, mac server, mountain lion, os x, os x server, profile manager, server on October 7, 2012.

5 thoughts on "The Complete Guide to Profile Manager (Part 1)"

Mike
December 21, 2012 at 10:54 am

Actually I'm struggling with Exchange profile variables now – even after speaking with Apple. In fact, they're waiting for me to report back to then on any progress. I'm trying to choose the correct variables for 10.8.2 Profile Manager on an OD box….

Eoin Ryan
March 9, 2013 at 8:18 am

Thanks a million – I found this really useful.

Morgan Daly
June 16, 2013 at 7:25 pm

Very cool list. Thank you.

Maybe you can help me? I have a task that I cannot cancel and I think that it's holding everything else up from working. Any ideas? I am starting to think that I might have to kill Profile Manager and start from the beginning which for 140 devices having to re-enroll will be a huge pain.

Thanks

Nathan Walker
June 17, 2013 at 12:02 pm

Glad you liked the list!

I’ve done a bit of digging and I think that I’ve found the solution to your problem. By using a Terminal command, you can completely clear out the tasks from Profile Manager. That should get you back on track.

Here are the steps:

1. Launch the Terminal. You’ll find it in the Utilities folder under Applications.

2. Copy and paste in the following command. This command accesses the database that Profile Manager stores all of its data in and erases all of the tasks.

```
sudo psql -h "/Library/Server/PostgreSQL For Server Services/Socket" -U _postgres -d device_management -c "TRUNCATE TABLE tasks;"
```

3. You will be asked for your password. Type it in and press enter.

That’s it! All of your tasks should be cleared from Profile Manager.

This method does have a few small side effects, but nothing too severe. The history of all of your completed tasks will be erased, but this isn’t too important because they’ve already been executed. Also, any profiles that were stuck in that “Active Tasks” queue will need to be pushed out again. To do this, just make a small change (like toggling a checkbox off and on) to the profile so you can save it again.

Hopefully this will solve your issue. Let me know if it works for you.

–Nathan

Morgan Daly

June 17, 2013 at 7:19 pm

Hello Nathan,

Thank you. How ever did you find this? It has worked like you said for clearing out the tasks now I just need to see if it is going to successfully push out new tasks. Fingers crossed.

I am also now leaning towards the fact that Open Directory might be corrupted at least a little. All of these profile manager problems and now failed authentications on VPN.

But thanks… I will let you know if your trick ultimately helps me to get Profile Manager working again.