Mac Management Basics 10.9
Deploying and Managing Multiple Mac Computers
## Introduction
Overview 5
Prerequisite knowledge 5

### Creating System Images
Hands-off deployment 7
Image types 8
Creating images with System Image Utility 8
Creating modular images 26
Additional resources 27

### Deployment
Local deployment 28
Deploying with NetInstall 32
Third-party deployment solutions 36
Additional resources 37

### Managing Computers with Apple Remote Desktop
Enable remote management 39
Creating Apple Remote Desktop computer lists 40
Deploying software 43
Inventory tools 46
Additional resources 48

### Policy Management
About Profile Manager 49
About configuration profiles 50
Setting up a Profile Manager server 52
Client management suites 76
Additional resources 76

### Managing Software Updates
Software update policy 77
Using the OS X Server Software Update service 78
Third-party software update service 83
Additional resources 83
Caching Software Downloads 84
   Requirements 84
   Managing the Caching service 85
   Comparing the Caching and Software Update services 87
   Additional resources 88

Additional Resources 89
   Mac Management Basics Exam 89
   OS X Training & Certification 89
   Books 90
   Support 90
Introduction

Overview
Configuring and adding a Mac to an organization’s network is simple and straightforward, but how do you handle the deployment of tens, hundreds, or even thousands of Mac computers? And once they’re deployed, how do you configure and manage them so that they can easily access resources and comply with IT policies?

The goal of this guide is to introduce you to the basic techniques for using Apple’s tools for deploying and managing Mac computers. After reading this guide and performing the outlined procedures, you’ll be familiar with the foundational Mac management concepts.

The first portion of the guide covers deploying Mac computers, focusing on methods for deploying software including creating installer packages, and using network disk images for system software deployment. Next, the guide presents solutions for managing OS X computers, including using Apple Remote Desktop and Profile Manager. The guide wraps up by describing how to use the Software Update and Caching services in OS X Server to assist with management and deployment of updates and apps.

Prerequisite knowledge
This material assumes you have a basic understanding of OS X skills and terminology. If you’re new to Mac, you should review Mac Basics online at www.apple.com/support/macbasics/.

You should also have a basic understanding of how to configure OS X, including how to connect to a network and access network services such as file servers, network printers, and directory servers. Some recommended resources for this knowledge include:

• *Mac Integration Basics*. An introduction to what you need to know to configure a Mac to work in a cross-platform environment. The guide is available online at http://training.apple.com/itpro/macinteg109 or on the iBooks Store.

• *OS X Support Essentials*. Designed to give you a tour of the breadth of functionality of OS X Mavericks and the best methods for effectively supporting users of OS X Mavericks systems, the *OS X Support Essentials 10.9* book is available from Peachpit
Press in print or digital form and as a three-day hands-on course (http://training.apple.com/pdf/mav101.pdf).
Creating System Images

This chapter covers the basics of creating images that can be deployed using the deployment methods covered in the next chapter.

While the focus is on using System Image Utility for image creation, Disk Utility could be used to create an image of a system, but it requires more preparation of the computer from which the image is being made. Also, when restoring an image, Disk Utility doesn’t create a recovery partition. As a result, Disk Utility is fine for creating an archive of a volume on a computer, but System Image Utility is better for creating images that will be deployed to multiple computers.

Hands-off deployment

Before you start creating system images, ask yourself: “Do I really need to create, manage, and deploy system images and software?”

The traditional method for deploying computers is to create system images and copy the images to every computer in the organization. While this creates consistency in system configuration, it places a burden on an IT organization to maintain a set of images, making sure they contain the latest OS updates and application versions.

Now, with the easy-to-use configuration assistant and the Mac App Store, you may find that a hands-off approach to deploying new computers might be appropriate. Instead of deploying an OS image, you can deliver new computers to the users and allow them to perform the initial configuration by downloading the software that they need — either from an internal website or the Mac App Store. Users are familiar with this approach because it’s what they do with their home computers.

If you decide that image deployment is appropriate, you should create images that minimize the need for IT involvement:

- **Minimum customizations** A deployment image should contain as few customizations as possible to protect it from constant revisions and make it as business-unit agnostic as it can be. Ideally, it contains only OS X, local settings, and keystone applications. Keystone applications are software packages that are installed on all the Mac computers in your organization.

- **Directory services** By fully using directory services, you gain centralized control over user identities and user data and provide for the delivery of a cohesive
management policy framework. You should build a script into your deployment image that binds the Mac to your directory service.

- **Client management** Using a client management system completes the minimal-touch deployment, and you should build this client management agent into your deployment image. On initial startup, the Mac contacts the client management suite and uploads its inventory information. At this point, any unit-specific software is provisioned, along with any update deltas that exist for the current deployment image. With most client management suites, optional applications are delivered to users' Mac computers via self-service software tools.


**Image types**

The two primary methods for creating deployable system images are duplicating a preconfigured Mac or building an image by combining an existing disk image or installer and installer packages.

A *disk image* (.dmg file) is a file that looks and acts like a mountable disk or volume. Disk Utility is the tool most frequently used to create disk images.

A *network disk image*, also called *network boot image*, is an image from which a client computer can start up long enough to install software contained within the image. The client can then start up from its own hard disk. The primary tool for creating installation images is System Image Utility. Usually network disk images are deployed across a network using the NetInstall service in OS X Server, but in the next chapter you'll learn a method for creating a local startup volume, such as a USB flash drive or a partition on a disk drive, from a network disk image.

Boot images and installation images are disk images. The main difference is that a .dmg file is a proper disk image and a network disk image is an .nbi folder containing files, including a .dmg disk file, to allow a computer use the folder to boot across the network.

**Creating images with System Image Utility**

Traditionally, Disk Utility has been used to create OS X system images. Although Disk Utility is still capable of creating images, you must properly prepare the systems before imaging. Disk Utility doesn’t include the OS X Restore partition as part of the imaging process.

System Image Utility is used to create network disk images. It's included with all OS X Mavericks computers at /System/Library/CoreServices. Unlike Disk Utility, System Image Utility prepares and creates the image at the same time. System Image Utility also automatically creates the OS X Restore partition.
With System Image Utility, you can create and customize three types of network disk images:

- **NetBoot** Boots a client computer to an operating system located on a server. This is done in a completely diskless boot environment or by leveraging a disk in the client to cache the operating system.

- **NetInstall** Creates a customized operating system installer that runs on a network allowing users to install Mavericks without erasing the target volume. You may define customizations to the installation process with easy-to-use Automator actions that perform tasks before or after the OS X installation process. In an environment where customizations have been used, NetInstall users are presented with the same user interface they would see if they were using the OS X Installer on the local drive. Examples of customizations include repartitioning hard drives, using predefined operating system installation choices, binding systems to directory services, renaming client systems, and installing additional software packages.

- **NetRestore** Images clients using a prebuilt image (referred to in this guide as a “prepared disk”) with block-copy Apple Software Restore (ASR). You have several options to create NetRestore sets including imaging an existing OS X computer, creating an image programmatically with a custom package set, and allowing for the arbitrary sourcing of ASR images—that is, choosing an image located on a web server or Apple file server, or using multicast ASR. With NetRestore, a single boot image can be prepopulated with predefined choices, or clients can browse for multicast ASR streams using Apple’s Bonjour browsing technology.

Although System Image Utility was designed to create images that are restored over the network (as you’ll see in the Deployment chapter), network disk images can be used to restore systems locally as well.

**Image sources**

To create an image, you must have valid OS X image sources or volumes and be logged in as an administrator user. If you download and install OS X from the Mac App Store, a valid OS X image source appears in the source pop-up menu.

You can’t create an image of the startup disk you’re running on, you must start up from a volume other than the one you’re using as the image source. For example, you could start up from an external FireWire hard disk or a second partition on the client computer’s hard disk. You can’t create the image on a volume over the network.
NetInstall from Installer

A NetInstall image takes the logic and options built into the OS X Mavericks Installer and moves them into a bootable disk image that can be used on networked client computers.

NetInstall images deployed with OS X Server are a convenient method for installing a clean version of OS X on any Mac on the network, even when the disk drive has been completely erased.

To create a NetInstall image with System Image Utility:

1. Download OS X Mavericks from the Mac App Store (do not install OS X or restart upon completion).
   An application named Install OS X Mavericks will be placed in the /Applications directory.
2. If the OS X Mavericks Installer opens, quit it.
3. Open System Image Utility (located in /System/Library/CoreServices).
4. From the Sources pop-up menu, choose Install OS X Mavericks.
5. Select NetInstall Image. This tells the image, when NetBoot loads it, to install an operating system.
6. Click Continue.
7. In the Network Disk field, enter a name for your image.
   This name identifies the image in the Startup Disk preferences pane on client computers.
8. (Optional) In the Description field, enter notes or other information to help you characterize the image.
   Clients can't see the description information.

9. If the image will be served from more than one server, select the checkbox below the description field.
   This assigns an index ID to the image for NetInstall service load balancing.

10. Click Create.

11. Read the Software Licensing Agreement and click Agree.

12. In the Save As dialog, choose where to save the image.
   If you don’t want to use the image name you entered earlier, enter a new name in the Save As field.
   If you’re creating the image on the same server that will serve it, choose a volume from the “Serve from NetInstall share point on” pop-up menu.
For this option to appear in the pop-up menu, NetInstall service must be configured on a network port and the Server app must be set to serve images from a volume. Choose a location from the Where pop-up menu or click the triangle next to the Save As field and navigate to a folder.

13. Click Save.

14. Enter an administrative password for the computer that’s generating the image and click OK.

   **Important**: Do not attempt to edit content in the image destination folder while the image is being created.

15. Once the process is complete, click Done.

   **Note**: The next chapter covers configuring the NetInstall service in OS X Server.

**NetRestore from Installer**

With NetRestore, a tool included in OS X Server, administrators can create operating system images and automations for those images, then deploy them via block-copy ASR. As with NetBoot and NetInstall, use System Image Utility to create an image, then share it for system imaging.

This section covers how to use System Image Utility and an OS X Mavericks Installer to create a bare-metal image for use with NetRestore.
To create a NetRestore image with System Image Utility:

1. Download OS X Mavericks from the Mac App Store (do not install OS X or restart upon completion).
   An application named Install OS X Mavericks will be placed in the /Applications directory.
2. If the OS X Mavericks Installer opens, quit it.
3. Open System Image Utility (located in /System/Library/CoreServices).
4. From the Sources pop-up menu, choose Install OS X Mavericks.
5. Select NetRestore Image.
6. Click Continue.
7. In the Network Disk field, enter a name for your image.
   This name identifies the image in the Startup Disk preferences pane on client computers.
8. (Optional) In the Description field, enter notes or other information to help you characterize the image.
   Clients can’t see the description information.
9. Enter the names and password that will be used to create the administrator account on the system once it has been restored:
   • Name: Enter the full administrator account name.
   • Short Name: Enter the short name for the administrator account.
   • Password and Verify: Enter and verify the password for the administrator account.

10. Click Create.
11. Read the Software License Agreement and click Agree.
12. In the Save As dialog, choose where to save the image.

If you don’t want to use the image name you entered earlier, enter a new name in the Save As field.

If you’re creating the image on the same server that will serve it, choose a volume from the “Serve from NetInstall share point on” pop-up menu.

For this option to appear in the pop-up menu, NetInstall service must be configured on a network port and the Server app must be set to serve images from a volume.

Choose a location from the Where pop-up menu or click the triangle next to the Save As field and navigate to a folder.

![Image Settings dialog](image.png)

13. Click Save.

14. Enter an administrative password for the computer that’s generating the image.

15. Once the process is complete, click Done.

**Using NetRestore from a configured computer**

NetRestore creates operating system images and automations for those images and deploys them using block-copy ASR. As with NetBoot and NetInstall, System Image Utility creates an image and shares it to facilitate system imaging.

In OS X Server, NetRestore pushes out a fully populated image, which can include applications, settings, and tools. Because the image is populated with all of this, the image first needs to be created from a volume that has been prepared, or installed, with all of those assets. In this type of environment, the prepared volume is typically one of the only steps in your imaging scheme (often followed by binding to a directory service).

NetRestore images are useful when you need to use the same software on multiple computers. If you have a classroom where all the computers need to have identical
software and configurations, you could create a NetRestore image to be deployed whenever the computers need to be refreshed to a “clean” state.

This section explains how to use System Image Utility to create a NetRestore image on a volume that has been prepared with all of the OS X Mavericks settings and applications (referred to as the “prepared volume”). In this example, the prepared volume is called Client. After creating the image, you can still add automations as postflight tasks within System Image Utility.

**To create a NetRestore image from a prepared volume with System Image Utility:**

1. Start the computer with the prepared volume in target disk mode (hold down the T key until the FireWire or Thunderbolt icon appears).
2. Use a FireWire or Thunderbolt cable to connect the computer with the prepared volume to the computer with Mavericks installed.
3. Open System Image Utility (located in /System/Library/CoreServices).
4. From the Sources pop-up menu, choose the volume that you want to use as your source for the NetRestore image.
5. Select NetRestore Image.
6. Click Continue.
7. In the Network Disk field, enter a name for your image.
   This name identifies the image in the Startup Disk preferences pane on client computers.
8. (Optional) In the Description field, enter notes or other information to help you characterize the image.
   Clients can’t see the description information.
   If the image will be served from more than one server, select the checkbox below the description field.
   This assigns an index ID to the image for NetInstall service load balancing.

9. Click Create.

10. Read the Software License Agreement and click Agree.
11. In the Save As dialog, choose where to save the image.
   If you don’t want to use the image name you entered earlier, enter a new name in the
   Save As field.
   If you’re creating the image on the same server that will serve it, choose a volume
   from the “Serve from NetInstall share point on” pop-up menu.
   For this option to appear in the pop-up menu, NetInstall service must be configured
   on a network port and the Server app must be set to serve images from a volume.
   Choose a location from the Where pop-up menu or click the triangle next to the Save
   As field and navigate to a folder.

12. Click Save.
13. Enter an administrative password for the host being used to generate the image and
    click OK.
    Important: Do not attempt to edit content in the image destination folder while the
    image is being created. Once the process is complete, click Done.

Automations with System Image Utility
Administrators often need to perform additional tasks or automations after the initial
image is built or while it’s being installed. For example, you may want to repartition a
drive before installation or repair it afterward. Workflows can handle all these tasks.

Use image workflows to create OS X NetBoot, NetInstall, and NetRestore images.
Workflows let you manually define the contents of your image in System Image Utility.

You must be logged in as an administrator user to assemble a custom workflow. An
image workflow must start with the Define Image Source action and end with the
Create Image action. Also, actions in a workflow must be connected. If not, the
workflow is invalid and the actions are not processed.
To assemble a workflow from a set of actions, drag and drop the actions from the Automator Library into the workflow sequence you want them to run. Each action in the workflow corresponds to a step you would usually perform manually.

Each action has options and settings that you can configure. System Image Utility connects these action components with the types of data that are flowing from one action to another.

You can save your assembled workflows to reuse later.

**To image OS X and automate tasks with System Image Utility:**

1. Open System Image Utility (located in /System/Library/CoreServices).
2. Choose an image source from the source pop-up menu.
3. Choose which type of image you’re creating (NetInstall, NetBoot, or NetRestore).
4. Your image type selection may vary depending on the image source you selected.
5. Click Customize for advanced image creation options.

This opens the workflow pane and Automator Library.
The Define Image Source action is the first component in the workflow and is required at the beginning of all image workflows.

6. In the Define Image Source action for your image, choose the image that you want to use as source for your workflow. This can be the Install OS X Mavericks Installer, a prepared image, or a preinstalled volume.

7. From Automator Library, choose additional actions that your customized image requires and drag them into the Workflow pane between the Define Image Source action and the Create Image action.

When you add a new action it should connect to the actions above it and below it.

Note that if an action doesn’t connect with the item above it or below it, the workflow will fail.

8. Assemble the actions in the order you like, configuring each action as you go.
Any actions that configure the network disk image must be placed between the Define Image Source action and the Create Image action.

9. If your workflow doesn’t contain a Create Image action, select the Create Image action in the Automator Library and drag it to the end of your workflow.

10. If you’re creating a NetBoot or NetRestore image, enter a name in the Installed Volume field.
   The volume that your image is installed on is renamed with this name.

11. Select the Include Recovery Partition checkbox to include the OS X recovery partition in your image.
   This option is available only with NetRestore images.

12. From the Save To pop-up menu, choose where to save the image.

13. In the Image Named field, enter the name of the image file as you would like it stored on the computer.

14. In the Network Disk field, enter a name for your image.
   This name identifies the image in the Startup Disk preferences pane on client computers.

15. (Optional) In the Description field, enter notes or other information to help you characterize the image.
   Clients can’t see the description information.

16. In the Image Index field, enter an Image ID:
   • To create an image that is unique to this server, enter an ID in the range 1–4095.
   • To create one of several identical images to be stored on different servers for load balancing, enter an ID in the range 4096–65535.

Multiple images of the same type with the same ID in this range are listed as a single image in a client’s Startup Disk preferences pane.

17. Click Save, then enter the name of your workflow in the Save As field. Choose where to save the workflow by choosing a location from the Where pop-up menu or clicking the triangle next to the Save As field and navigating to a folder.

18. Click Save.

19. To start the workflow, click Run, then authenticate if prompted.
   Important: Do not attempt to edit content in the image destination folder while the image is being created.
To restrict which computer models may start up using the network disk image:
The Filter Computer Models action limits which computer models can start up using
the network disk image. If your image contains software that has specific hardware
requirements, you can restrict the image to computer models that meet those
requirements.

1. From the Automator Library, drag the Filter Computer Models action into the workflow
   pane between the Define Image Source and Create Image actions.
2. Select the Enable checkbox for each computer model that you want to be able to start
   up using your defined image source.

   In this example, only computers that are compatible with Mavericks have been
   enabled.

   ![Filter Computer Models](image)

To set up a workflow item that partitions the target disk:
With the Partition Disk action, you can partition a computer’s drive before the image’s
software is installed. For example, you could create separate system and data
partitions.

1. From the Automator Library, drag the Partition Disk action into the workflow.
2. From the partitions pop-up menu, choose the number of partitions and enter a name
   for each.
3. Select the “Partition the disk containing volume” checkbox to limit which disks will be
   repartitioned. This feature helps reduce the dangers associated with repartitioning a
   drive, like overwriting external drives, jump drives, or computers that aren’t ready to be
   imaged.

   The checkbox labeled “Display confirmation dialog before partitioning” is another
   feature that helps decrease the risk of erasing user data. However, note that both this
   and the previous step can stop the imaging process, which may be an issue if you’re
   trying to install hundreds or thousands of systems. Use both partitioning options as
   needed.
4. Choose the format for the drives. In most cases, the default setting—Mac OS Extended
   (Journaled)—is fine.
5. Choose the minimum size for each partition. This is a sanity check so that the tool doesn't try to image 40GB to a 10GB drive and partition a chunk away for other tasks. It's better if the imaging process fails early because it keeps troubleshooting imaging issues to a minimum allowing mass deployment staff to move on to imaging the next host.

To set up a workflow item that adds a user account:

By default, an OS X computer has one user account, the primary admin account. You may want to create an additional standard account so that users can use the computer, but can't modify the system. Or you may need an additional local administrator account for troubleshooting, software updates, Apple Remote Desktop, and so on. The Add User Account action can add accounts as part of the image.

1. From the Automator Library, drag the Add User Account action into the workflow.
2. Provide a user name, short name, and password for this account and click the “Allow user to administer the computer” checkbox.
3. To create multiple accounts, drag a new Add User Account item into the workflow.
To set up a workflow item that sets the computer name:

Every computer, whether using OS X, Microsoft Windows, or Linux, needs a unique name on the network. Use the Apply System Configuration Settings action to rename the system following imaging.

1. From the Automator Library, drag the Apply System Configuration Settings action into the workflow.

2. Select the “Generate unique Computer Names starting with” checkbox and enter the prefix that imaged systems will use. Each system will begin the host name with that prefix (such as Marketing-1, Marketing-2, and so on).

Or you can pull the information from a file by selecting the “Apply Computer Name and Local Hostname settings from a file” checkbox.

If the computer running System Image Utility has been bound to a directory service like Open Directory, Active Directory, eDirectory, or some other directory service, select the “Connect computers to directory servers” checkbox. This feature adds the imaged system to the directory service as a postinstallation task.

**Note:** Most directory services require unique entries for each computer, so the binding state before imaging won’t carry through to the image unless this option is selected or a custom script is used to bind.

For prepared images, select the “Change ByHost preferences to match client after install” checkbox.
To add additional software to a System Image Utility workflow:

The most powerful feature of the Automator Library is the ability to install packages. The Add Packages action is useful if you have software that comes distributed as a package, such as software updates downloaded from Apple's Support website. However, if you know how to create your own packages, and more specifically use shell scripting to automate tasks, the Add Packages action is most beneficial to you and will help you further automate your installation process.

Note: Software installers added to System Image Utility must be in standard installer packages (.pkg) format.

1. From the Automator Library, drag the “Add Packages and Post-Install Scripts” action into your workflow.
2. Click Add (+) to add your software packages to the action.

Note: When you add multiple packages and scripts to a workflow, they install or run in the order listed in the “Add Packages and Post-Install Scripts” workflow item.

To add a configuration profile to a System Image Utility workflow:

With System Image Utility, you can add configuration profiles to your NetInstall and NetRestore workflows. By adding profiles, you can preconfigure the Mac for a number of settings and services.

You can then create configuration profiles with the OS X Server Profile Manager service (described later in the Policy Management chapter of this guide).

1. From the Automator Library, drag the Add Configuration Profiles action into your workflow.
2. Drag and drop, or use the Add (+) button, to add your configuration profiles to the action.
Note: If your workflow has packages and scripts that rely on a certificate that’s installed by a configuration profile, make sure the configuration profiles are installed in the workflow before the packages and scripts.

To configure the Enable Automated Installation workflow action:

Use the Enable Automated Installation action to set the options for automated (unattended) client installations. This action is valid only when creating NetInstall or NetRestore images.

1. From the Automator Library, drag the Enable Automated Installation action into your workflow.

2. If the image is to be installed on a specifically named volume, select “Install to the volume” and enter the name of the target volume.

3. To erase the target volume before the image is installed, select the “Erase before installing” checkbox.

   Warning: Using the Erase option removes all data from the target volume. Back up all data before using this option.

4. From the Main Language pop-up menu, choose the image language.

Creating modular images

When creating system images, the urge is to take a clean Mac, install a fresh copy of OS X and all the applications that users might need, then create a “monolithic” NetRestore image of the Mac. However, this method creates images that are difficult to maintain as the image needs to be completely rebuilt every time the OS or an app is updated.

A better approach is to create slimmer, minimal images. With the Mac App Store and the Volume Purchase Program in some regions, you could create images that contain just the operating system, and allow users to download just the apps they need. This approach saves the administrator time installing software and could save the organization money by limiting the total number of apps that need to be purchased.

At times you’ll find that required software isn’t available through the Mac App Store or you’re creating images for computers that refreshed frequently and aren’t dedicated to a single person, such as computers in a lab or classroom. For these situations, instead of creating an image from a preconfigured computer, create a customized workflow that makes a NetRestore image using the OS X Installer as the source and adds the additional software with the the “Add Packages and Post-Install Scripts” workflow item. With a modular approach, you can create customized images with updated software, including the OS, by updating the workflow and avoiding the hassle of rebuilding the master on a computer.
If you need to create installer packages to add software to an image workflow, there are a number of third-party products available to do so:

- **Composer, from JAMF software** [http://www.jamfsoftware.com](http://www.jamfsoftware.com)
  With Composer, you can inspect a computer and create a package of each application that has been installed on that system, offering a smooth transition from monolithic imaging environments to package-based imaging environments.

- **InstallEase, from Absolute Software** [http://www.absolute.com](http://www.absolute.com)
  With InstallEase, a simple snapshot-based package generation tool for OS X, you can create installer packages with minimal effort.

- **Iceberg and Packages** [http://s.sudre.free.fr/Software.html](http://s.sudre.free.fr/Software.html)
  Iceberg and Packages (under the BSD license) provide interface options for the implementation of preflight and postflight scripts, as well as features specifically used for metapackage management.

**Additional resources**


- **Leveraging NetInstall, OS X Server Essentials 10.9: Using and Supporting OS X Server on Mavericks**, Peachpit Press
After you’ve generated images and customized the automations to go into those images, the next step is to deploy them. The simplest form of deployment is to locally apply an image from one Mac to another via USB or FireWire. This process can be cumbersome, so additional techniques are introduced here to help streamline the process toward enabling a one- or zero-touch deployment.

Local deployment

Local image deployment is the simplest form of deployment for Mac computers. By taking advantage of native tools such as Apple Software Restore, Disk Utility, and target disk mode, administrators can quickly and easily test deployment images using direct connections between computers without the need to move images to production or test servers.

Local imaging techniques, however, don’t scale well and aren’t suitable for deploying a large number of Mac computers in most environments. Local deployment is typically most suitable for test environments when working out details about how the larger scale deployment process will work.

Creating a bootable installer volume

With OS X Mavericks, you can create a bootable OS X installer, which can be used to install the operating system while started from removable media, such as a USB flash drive.

To create a bootable OS X installer:

1. Use the Mac App Store to download the OS X Installer app.
2. Mount the volume you wish to convert into a bootable installer. This could be removable media, such as a USB flash drive, or a secondary internal partition.
3. Use the createinstallmedia tool to convert the volume from step two into a bootable installer based off the installer app from step one. To learn how to use createinstallmedia, execute this command in Terminal:

   `/Applications/Install\ OS\ X\ Mavericks.app/Contents/Resources/createinstallmedia`
You may need to adjust the path to the OS X Installer app in the above command.

**Note:** `createinstallmedia` is intended to be used only with the version of OS X Installer app that it came with.

### Creating a bootable disk or volume from a NetInstall image

Not all Mac computers have a fast Ethernet link to a server. You can still use your NetInstall environment to push images to these sites. However, instead of using NetBoot or NetInstall, you can use USB, FireWire, or ThunderBolt volumes.

This section explains how to use NetInstall to create a bootable drive that automatically installs a client system. Because most images are now over 6GB in size, use a drive that’s 8GB or larger.

**To create a bootable disk or volume with a network disk image:**

1. Copy a NetInstall image (.nbi folder) to the root level of a external drive.
2. Open Automator (located in `/Applications/`).
3. Create a new document.
4. In the New Document dialog, select Workflow and click Choose.

   If you created a customized image in System Image Utility, the Automator window should look familiar. That’s because System Image Utility uses Automator actions to create the customized workflow. If you select System from the left column, you’ll see the actions that are used to create the network disk image in System Image Utility.

   First you need to specify the .nbi folder that you want to make bootable.

5. In the first Actions column, select “Files & Folders.”
6. Drag the Get Specified Finder Items action from the second column to the Automator workflow area.
7. In the Get Specified Finder Items action, click Add.
8. Navigate to and select the .nbi folder that you copied to the external volume in the first step.
9. Click Add.

   Next, you need to bless the .nbi folder so that it’s bootable.

10. In the first Actions column, select System.
11. Drag the Bless NetBoot Image Folder action from the second column to below the Get Specified Finder Items action in the Automator workflow area.
12. Select the Apply Custom Label checkbox and enter a label that will appear in the list of bootable volumes.
13. Click the Run button in the upper-right corner. It should take only a few seconds for the workflow to run. The results will be displayed in the log beneath the workflow.
To create a bootable disk or volume with System Image Utility:

When creating a customized image in System Image Utility, you can add the Bless NetBoot Image Folder action to the end of the workflow.

In addition, you need to specify the external drive for the Save As value in the Create Image action.

To start up a computer with a volume containing a network disk image:

Startup Manager allows you to choose the startup volume on the fly simply by holding down the Option key while the computer is starting up.

1. Turn on, or restart, your Mac.
2. Immediately press and hold the Option key.
   After a few seconds, the Startup Manager should appear. The Startup Manager scans for available volumes.
3. Use the Left Arrow and Right Arrow keys on the keyboard to select the network disk image.
4. Press the Return key on your keyboard to start up the computer from the disk image.
Deploying with NetInstall

The NetBoot, NetInstall, and NetRestore features of OS X Server offer you alternatives for managing the operating system and application software that your Macintosh clients (or even other servers) require to start and do their work. Instead of going from computer to computer to install the operating system and application software from CDs, you can prepare an installation image that installs on each computer when it starts up. You can also choose to not install software and have client computers start up (or boot) from an image stored on the server. (In some cases, clients don’t even need their own hard disk.)

With NetBoot and NetInstall, your client computers can start from a standardized Mac OS X configuration suited to specific tasks. Because the client computers start from the same image, you can quickly update the operating system for users by updating a single boot image.

You can set up multiple NetBoot or NetInstall images to suit the needs of groups of clients or you can provide copies of the same image on multiple NetBoot servers to distribute the client startup load. You can also use a NetRestore image to quickly restore a volume.

NetInstall considerations

All systems supported by OS X Mavericks can use NetBoot to start from an OS X Mavericks network disk image.

Note: For a list of computers compatible with Mavericks, visit http://support.apple.com/kb/ht5842.

You must install the latest firmware updates on all client computers. Firmware updates are available from the Apple Support website: www.apple.com/support/.

NetInstall is supported only over physical Ethernet connections. Using Wi-Fi to boot clients using a network disk image isn’t supported by Apple and is discouraged.

Configuring a NetInstall server

NetInstall and NetRestore both rely on NetBoot to boot an operating environment that frees the internal drive for an operating system image or upgrade. NetBoot boots a Mac computer to an operating system stored within an installation image hosted on a NetInstall server.

An OS X Server can act as a NetInstall server and is covered in this section. The instructions assume you’ve already installed and are running OS X Server on an OS X Mavericks computer. If you need information about installing and configuring OS X Server, refer to the online OS X Server Help at https://help.apple.com/serverapp/mac/3.0/help/index.html or the OS X Server Essentials 10.9 book from Peachpit Press.
To configure a NetInstall server:

1. Open Server app (located in /Applications/).
2. Select NetInstall in the sidebar, then click Settings.
3. Click the Edit button to the right of “Enable NetInstall on.”
4. Make sure at least one network port is selected.
   **Note:** You should provide NetInstall services only over gigabit Ethernet ports.
5. Click OK.
6. Click Edit Storage Settings.
7. In the entry for the volume on which you want to store the NetInstall images and client data, choose “Images & Client Data” from the pop-up menu.

![Storage Settings](image)

8. Click OK.

9. Place the network disk images you created earlier in the /Library/NetBoot/NetBootSP0 directory of the volume you just selected.

10. In Server app, press Command-R to refresh the window.

   The Images list will contain the name of the network disk image you copied to NetBootSP0.

![NetInstall](image)

11. Select the image you want to use.

12. From the Action pop-up menu, choose Edit Image Settings.

13. Select the “Make available over” checkbox.
14. Choose the protocol over which you want to make the image available.

![NetInstall of OS X Mavericks](image)

15. Click OK.

16. If this is your first image, you may want to set this image as the default. If so, select the image and choose “Use as Default Boot Image” from the Action pop-up menu.

17. To start the NetInstall service, click the On/Off button in the upper-right corner.

18. To test booting a system to the image, start up the client while holding down the N key, or use the Startup Disk System Preferences on the client to select an image from the NetBoot server you just set up.

**Custom source NetRestore**

After you’ve created a network disk image and enabled it on a NetInstall server, there are a few methods you can use to have client computers boot using the image.

**To start up using the default network disk image:**

You can use the N key to start up any supported client computer from a NetInstall disk image. With this method, the client computer uses the Boot Service Discovery Protocol (BSDP) to locate a NetInstall server and starts up from the server’s default disk image. If multiple servers are present, the client starts up from the default image of the first server to respond.
When you use the N key to boot using the default NetInstall image, your computer remembers what server and image were used. The next time you hold down the N key at startup, your computer attempts to use the same server and image, even if that image is no longer specified as the default image. Holding Option-N during startup causes the computer to boot using the current default image.

**To boot using a specific network disk image:**

If your NetInstall server is hosting multiple images or you have set up multiple servers, you can use the Startup Disk in System Preferences to select a specific boot image to use.

1. Choose System Preferences from the Apple menu.
2. Click Startup Disk.
3. Click the name of the network disk image created for NetRestore.
4. Click Restart.
   The computer is booted into the NetRestore environment, where you'll see the icon for System Image Utility.
5. Click the image you want to restore, then click Continue. Or you can type the path to the image in the field provided (if that option was selected when you created the NetBoot set).

**Third-party deployment solutions**

The following is a partial list of third-party solutions for OS X deployment:

- DeployStudio— [http://www.deploystudio.com](http://www.deploystudio.com)
- Absolute Manage— [http://www.absolute.com](http://www.absolute.com)
- KACE— [http://www.kace.com](http://www.kace.com)
- LANDesk— [http://www.landesk.com](http://www.landesk.com)
- FileWave— [http://www.filewave.com](http://www.filewave.com)
Additional resources

• “Manage updates and installation: Install OS X over the network” section, OS X Server: Advanced Administration—https://help.apple.com/advancedserveradmin/mac/3.0/


• Leveraging NetInstall, OS X Server Essentials 10.9: Using and Supporting OS X Server on Mavericks, Peachpit Press
Apple Remote Desktop is an easy-to-use, powerful, open standards-based desktop management software for all your networked Mac computers. IT professionals can remotely control and configure systems, install software, offer online help to end users, create detailed software and hardware reports, and automate routine management tasks—all from a centralized location.

You can remotely manage client computers individually, but most Apple Remote Desktop features are used to manage multiple computers at the same time. For example, you can install or update the same applications on all the computers in a particular department. Or you can share your computer screen to demonstrate a task to a group of users.

To manage multiple computers with a single action, you define Apple Remote Desktop computer lists. A computer list is a group of computers that you want to administer similarly. Setting up computer lists is easy; you simply scan the network or import the identity of computers from files.

You can group and organize computers for administration. You can group computers by type (laptop, desktop), physical location (building, city), use (marketing, engineering), and so on. And one computer can belong to more than one list, giving you a lot of flexibility for multicomputer management.

After you’ve set up computer lists, you can perform most of the computer administration activities for groups of client computers.

You can also create a dedicated remote Task Server, which is a remote Mac running Remote Desktop that collects information and shares its database with authorized Remote Desktop administrators. A Task Server acts as an always-on, automated administrator installing packages and changing client settings without direct control from the Remote Desktop app. You can also use a Task Server to install packages and change settings on clients that aren't currently available on the network by holding the task in a queue until the client computer becomes available.
Enable remote management

The Apple Remote Desktop client software is built into OS X. Client computers can set local system preferences that restrict remote access to specific users and actions. Client computers must have remote management enabled to be managed. You can use remote management settings to restrict access privileges to a subset of Remote Desktop features (such as allowing report generation but not allowing observe and control), or you can set computer settings (such as showing remote management status in the menu bar or requiring a password to control the screen).

**Note:** Although the Apple Remote Desktop client software is built into OS X, the administrator app is available from the Mac App Store.

To turn on remote management on a client computer:

1. On the client computer, open System Preferences and click Sharing.
2. Select the Remote Management checkbox, then select the actions that remote users are allowed to perform and click OK.
3. Do one of the following:
   - Select “All users” to allow all users on your network to connect to your computer using Apple Remote Desktop.
   - Select “Only these users,” then click Add (+), and select the users with whom you want to share your computer using Apple Remote Desktop.
4. To change which capabilities users have when accessing your computer, click Options.

The following lists the remote management options in the Sharing pane and the Remote Desktop features that they correspond to (for example, if you want a certain administrator to be able to change computer file sharing names, you need to grant that administrator the privilege by selecting “Change settings”):

- **Observe: Control** Use these Interact menu commands: Control, Share Screen, Lock Screen, and Unlock Screen. This checkbox must be enabled to use the Upgrade Client Software and Change Client Settings features.
- **Observe: Show when being observed** Automatically change the status icon to notify the user when the computer is being observed or controlled.
- **Generate reports**  Create hardware and software reports using the Report menu; use Spotlight search.

- **Open and quit applications**  Use these Manage menu commands: Open Application, Open Items, Send UNIX Command, and Log Out Current User.

- **Change settings**  Use these Manage menu commands: Rename Computer, Send UNIX Command, and Set Startup Disk.

- **Delete and replace items**  Use these Manage menu commands: Copy Items, Install Packages, Send UNIX Command, and Empty Trash. Also delete items from report windows. This checkbox must be enabled to use the Upgrade Client Software feature.

- **Start text chat or send messages**  Use these Interact menu commands: Send Message and Chat.

- **Restart and shut down**  Use these Manage menu commands: Sleep, Wake Up, Restart, Send UNIX Command, and Shut Down. This checkbox must be enabled to use the Upgrade Client Software feature.

- **Copy items**  Use these Manage menu and Server menu commands: Copy Items, Send UNIX Command, and Install Packages. This checkbox must be enabled to use the Upgrade Client Software and Change Client Settings features.

To automatically select all access checkboxes, hold down the Option key and click any checkbox.

5. Click OK.

6. Click Computer Settings, and select options for the computer that will be shared.

### Creating Apple Remote Desktop computer lists

Apple Remote Desktop uses lists of client computers to logically organize the client computers under your control. Before you can manage any client, you need to add it to an Apple Remote Desktop computer list.

Apple Remote Desktop displays computers in lists in the main section of the Remote Desktop window. The default computer list is called the All Computers list. This is a full list of all potential clients that you’ve located and authenticated to. You can create other lists to group the computers on your network in any way you wish.

Computer lists have the following capabilities:

- You can create as many lists as you want.
- Computers can appear in more than one list.
- Lists can be made in for different types of groupings: Geographical, functional, hardware configuration, and even color.
- If you click a list name and keep the mouse over the list name, you can edit the list name.
- If you double-click the list icon, you open another window containing the computers in the list.
To add computers to the All Computers list with Apple Remote Desktop:

1. Open Remote Desktop (located in /Applications).

2. From the list on the left, click Scanner to see the computers you need to manage.

Now you can search for systems and add them to the All Computers list and a list you create.

The scanner searches with the following options:

- **Bonjour** You can use Bonjour to display a list of only the computers in your default Bonjour domain with Remote Desktop enabled. Typically this includes only your local subnet, but this can include other subnets.

- **Local Network** When you choose a local network scanner, Remote Desktop sends a subnet broadcast to computers on the same subnets as the administrator computer. All possible clients on the local subnets appear in a list on the right side of the Remote Desktop window.

- **Network Range** To locate computers by network range, you enter a beginning and ending IP address to scan, and Apple Remote Desktop queries each IP address in that range in sequence, asking if that computer is a client computer. This method works best when searching for clients outside the local subnet but on the local area network.

- **Network Address** If you know the exact IP address or fully qualified domain name of a computer, you can use that IP address or domain name to add the computer to your All Computers list.

- **File Import** You can import a list of computers into Remote Desktop by importing a file listing the computers’ IP addresses.

The list can be in text or spreadsheet file format and must contain IP addresses or fully qualified domain names (such as foo.example.com).
With File Import, you can also add ranges of IP addresses by expressing the range in the following format: xxx.xxx.xxx.xxx-yyy.yyy.yyy.yyy. For example, using a text file with “192.168.0.2-192.168.2.200” scans all IP addresses in that address range.

- **Task Server** When you view the Task Server scanner, you see all client computers that registered with the Task Server. This list includes client computers that other Remote Desktop administrators have added.

- **Directory Server** When you view the Directory Server scanner, you see all client computers that are registered with the Task Server and are in computer groups in directory servers you're bound to.

3. After the scan is complete, select one or more computers. To add multiple computers, Shift-click to select the first system in the range you want to add, then the last.

4. Drag the computers to the All Computers list.

5. Authenticate by providing a user name and password for a Remote Desktop administrator account on the computer being added.

6. Click Add.

   The computer appears in the All Computers list.

   **To create a new list of computers:**

1. From the list on the left, click All Computers.
2. Select computers to add to the list.
4. Name the computer list.

   Or you can choose File > New List to create a blank list and drag computers from the All Computers list, or from Scanner search results, to the blank list.
Listing all systems in Apple Remote Desktop helps improve IT efficiency. Support personnel can control computers remotely from their desk, so they can continue providing support to other users.

**Deploying software**

You can use Apple Remote Desktop to install software and software updates on one or more client computers without user interaction or interruption—they don't even need to be logged in. The only computer you actually have to touch is yours.

When deploying applications, consider:

- Which applications are already on systems in the environment, and what conflicts may occur due to deployment.
- Which applications can run—regardless of whether they’re actually loaded into the computer.
- Whether applications require custom packages to be deployed without prompting for serial numbers and other user choices.

You can use Apple Remote Desktop to review which applications are running on Mac computers in your network. Apple Remote Desktop can also run a report that lists applications and their versions. To see a list, open Remote Desktop, select the computers you want to review, and choose Software Version from the Report menu.

**Install software with Installer packages**

After you know which systems need software, you can deploy the software in package format with the Install feature in Apple Remote Desktop.

**To deploy software with Apple Remote Desktop:**

1. Open Remote Desktop (located in /Applications).
2. Select a computer or group of computers.
3. From the toolbar, click Install.
4. Add installer packages by either clicking Add (+) or dragging the files to the Packages list.
5. Select whether restart is necessary after installation.
6. Select whether to run the installer locally or use a task server.
7. Select whether to stop the installation on the target computers if a problem occurs.
8. Select whether to encrypt the network data.
9. Select the “Network usage” checkbox to limit bandwidth, if necessary, and enter the maximum network bandwidth you'd like the installation to use.

10. In the lower left, click Schedule to schedule installation for a later time, or click Install for immediate installation.

When installation is complete, a message appears below the toolbar.

Install software by copying
Remote Desktop makes it easy to copy items (other than the system software) on one or more client computers.

Copying files works fastest with a small number of files. For example, 10 files that are 10K each generally take longer than one file that is 100K. Consider copying a single file archive (like a .zip or .sit file) to remote computers for faster copying. Remember that OS X applications are bundles of many smaller files. Although the application you want to copy looks like a single file in the Finder, it may contain hundreds—or even thousands—of smaller files.

If a client computer is asleep when you attempt to copy items, Remote Desktop tries to wake the client. If it can't wake the client and the copy doesn't proceed, use Remote Desktop to wake the target computer, then attempt the copy again.

If you choose to copy out to many client computers simultaneously, Remote Desktop uses network multicasts to send the files. If there’s a significant number of multicast networking errors, Remote Desktop tries to copy individually to each client computer.
To copy files with Remote Desktop:

1. In the Remote Desktop window, select a computer list, then select one or more computers.

2. Choose Manage > Copy Items.

3. Add software to the “Items to copy” list.
   - Click Add (+) to browse local volumes for items to copy, or drag files and folders to the list.
   - If you want to remove an item from the list, select the item, then click Remove (–). Repeat this step until all the software you want to copy is in the list.

4. Select a destination.
   There are several preset locations in the “Place items in” pop-up menu, including the Applications folder. If you don’t see the location you want, you can specify a full pathname.

5. Select your copy options.

6. Click Copy.
   The software is copied to the indicated location. If the copy operation is unsuccessful, an error message appears in the task feedback window.
Inventory tools

With Apple Remote Desktop, you can capture data describing the attributes of client computers in the Apple Remote Desktop database, then generate reports based on the data.

You specify how often you want to capture data, the data you want to capture, and the computers you want to profile. You can collect data just before generating a report if you need up-to-the-minute information. Or you can schedule data to be collected by Remote Desktop at regular intervals and stored in its built-in Structured Query Language (SQL) database for use on an as-needed basis.

You can also specify where you want the database to reside: On the local administrator computer or on a server where the Remote Desktop administrator software is installed, so data can be captured on an ongoing basis.

Using predefined report types

Remote Desktop includes several predefined report types:

- **File Search** Use the File Search report to search client systems for specific files and folders and to audit installed applications. With this report, you can find out how many copies of a particular application are in use so you don’t violate license agreements.

- **Software Version Report** Use the Software Version report to make sure that all users have the latest application versions appropriate for their systems.

- **Software Difference Report** Use the Software Difference report to detect application versions that are out of date, nonstandard, or unacceptable. You can also learn whether a user has installed an application that shouldn’t be installed.
• **System Overview Report**  The System Overview report makes visible a wide variety of client computer characteristics. Using this report, you can review information about a client’s Wi-Fi setup, computer and display characteristics, devices, network settings, system preferences, printer lists, and key software attributes. There are numerous uses for this report, such as identifying problems or verifying system configurations before installing new software, or determining how many devices of a particular type (such as scanners) are in a particular lab.

![System Overview Report](image)

• **Administration Settings Report**  Use the Administration Settings report to determine which Remote Desktop administrator privileges are enabled or disabled in the Sharing pane of System Preferences on individual client computers.

• **Application Usage Report**  Use the Application Usage report to find out which applications have been running on your client computers and who ran those applications.

• **Hardware Reports**  Several reports provide details about particular hardware used by client computers (such as storage, USB devices, FireWire devices, memory, expansion card, and network interfaces). Use these reports to determine, for example, how much free space is left on a particular disk, which computers need more memory, and which computer has the fastest processor speed.

• **Network Test Report**  Use the Network Test report to measure and troubleshoot the communication between your administrator computer and your client computers. The Network Test report can also help with troubleshooting network hardware issues. Use this report to help identify reasons for network communication problems that could affect Remote Desktop. For example, if you’re unable to copy items to
particular client computers from the administrator computer, you may find you have a bad connection to the computers. Using this information can help you isolate the problem to a particular cable or hub.

- **User History Report**  Use the User History report to show who has logged in to a client, how the user logged in, and for how long.

**Generating your own reports**

Because the Remote Desktop database is in standard SQL format, you can also use your favorite SQL scripts to query, sort, and analyze the collected data. In addition, you can export data from the database into a file so you can import it for viewing in a different program, such as a spreadsheet application.

**Exporting reports**

After Remote Desktop generates reports, you can export them into a comma-delimited or tab-delimited text file. The file includes all columns of information in the report window, and exports the report rows in the order they’re sorted. You can feed exported reports into a database, spreadsheet, or other tool for further analysis.

**To export a report:**

1. Select the rows of the report you want to export.
2. Choose File > Export Window.
3. In the Save dialog, name the file and choose where you want to save it.
4. Choose the type of text encoding the destination application uses.
5. Choose the field separator that the destination application will use to parse the data.
6. Choose what to export. If you need to export only a portion of the report, choose Export Selected Items Only.
7. Click Save.

**Additional resources**

Policy management in OS X is a robust way of managing practically any setting in the operating system. Before OS X Lion, managed preferences was the primary way to manage Mac computers. Although OS X still support managed preferences, using configuration profiles is the preferred method as it supports both OS X and iOS devices, providing many more options (such as locking devices, performing remote wipes, and setting up 802.1X profiles).

This chapter provides an introduction to using profiles to manage devices with Profile Manager. It covers setting up and configuring the Profile Manager service on OS X Server, using Profile Manager to create profiles, and delivering and installing profiles on client computers running OS X 10.7 or later.

About Profile Manager
With Profile Manager, it’s easy to configure OS X computers and iOS devices so they use your company or school resources and have the settings your organization requires. Profile Manager is included with OS X Server, which is available from the Mac App Store.

Components of Profile Manager
With Profile Manager, you can specify how clients are configured, how to administer devices, and how to deliver the configurations to users and devices. There are three components to Profile Manager:

- **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 that you define using the administration tool. Users connect to the web-based portal using their device. After they log in, the settings that you assigned to them are available for download and installation. Users also go to this site to enroll devices for Mobile Device Management (MDM) if you’re using Profile Manager as an MDM server.

- **Mobile Device Management server** Using Profile Manager as an MDM server, you can remotely manage enrolled OS X Mavericks and iOS devices. After a device is
enrolled with Profile Manager, you can update its configuration over the network without user interaction, as well as execute tasks such as reporting and locking or wiping the device.

**Note:** Mobile device management is supported on Mac computers with OS X Mountain Lion v10.8 or later installed. However, to take advantage of all the Profile Manager features, you should update all client computers to OS X Mavericks v10.9 or later.

**Understanding user and device groups**

Each user, user group, device, and device group can have a default group of settings. This allows you to easily share base settings for devices or users that need them. For example, to configure a teacher’s iPad, create a user account for the teacher, then place that teacher in the “teachers” and “iPad” groups. This assigns the user two collections of default settings—one from each group—and you can then create additional settings tailored to the user.

Other types of user and device groups that you might find useful are “lab Mac,” “field sales iPhone,” and “student notebooks.” For the latter group, for example, the default settings might include restrictions or specific network settings.

**About configuration profiles**

Configuration profiles are XML files that load settings and authorization information onto OS X computers or iOS devices. They contain client security policies and restrictions, VPN configuration information, Wi-Fi settings, email and calendar accounts, authentication credentials that permit a computer to work with your enterprise systems, and several other types of settings.

Some VPN and Wi-Fi settings, such as 802.1X parameters, can be set only by a configuration profile. You create configuration profiles using an MDM solution such as Profile Manager.

**Note:** Although this chapter focuses on Profile Manager, management concepts covered are applicable to other MDM solutions.

Each configuration profile contains one or more payloads. A *payload* is a collection of settings in the configuration profile, such as VPN specifications. Some payloads are for use only with OS X computers, some are only for iOS devices, and some apply to both.

When you create a configuration profile, you do so for users or devices, or groups of users and devices. Profile Manager tailors the payloads depending on which you choose, and the settings apply at that level. For example, settings that apply only to users aren’t available when you’re creating a device configuration profile.

Although you can create a single configuration profile that contains all payloads for your organization, consider creating separate profiles that let you enforce policies while granting access, as well as provide updates to settings that are subject to change. For example, you might create a configuration profile that sets up a user’s
access to email but also enforces restrictions or passcode settings. To have access to messages, users must also accept your security policies.

You can distribute configuration profiles by email, on your own webpage, or by using an MDM. When users open the email attachment or download the profile using Safari on their device, they’re prompted to begin installation. You can also use Profile Manager as an MDM server to send new and updated profiles to users after they enroll their devices.

Except for passwords, users generally can’t change settings in a configuration profile. Accounts configured by a profile can be removed only by deleting the profile.

Each user, device, and group have default configuration profiles so you can quickly provide a base level of settings, then you can further assign additional configuration profiles to customize the settings to meet your organizational requirements. For example, to enforce restrictions and configure users’ devices to use your VPN, create a configuration profile with a restrictions payload and a VPN payload. Because both payloads are in the same profile, the users must install both. If they remove the configuration profile to avoid the restrictions, their VPN access is also removed.

**Basic profile categories**

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

- **User profiles**  Contain settings for individual users or user groups, such as account names, passwords, and parental controls.

- **Device profiles**  Contain settings for individual devices or device groups, such as directory bindings, energy saver, and restrictions.

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

**Distributing configuration profiles**

After you’ve defined the settings for users and their devices, you can distribute the configuration profiles to users in the following ways:

- **Manual distribution**  You can download configuration profiles (.mobileconfig files) from Profile Manager’s administration tool, then send them to your users via email or post them to a website you create. When users receive or download the profiles, they can install them on their device.

- **User self-service**  Users can download and install the settings from Profile Manager’s built-in user portal. The user portal ensures that users receive the configuration profiles that you assign to them or their group.

- **Remote device management**  You can enable Profile Manager’s MDM server, which allows you to remotely install, remove, and update configuration profiles on enrolled devices.
Setting up a Profile Manager server

OS X Server includes the Profile Manager service, which can manage both OS X and iOS devices.

To set up the Profile Manager service:

To set up Profile Manager, install OS X Server from the Mac App Store. Then, when you turn on the Profile Manager service and click Configure, the Server app guides you through the steps to set up the service, including configuring the server as an Open Directory Master.

1. In the Profile Manager pane, click On.
   Wait a moment while Profile Manager service starts.
2. Click Configure (next to Device Management).
   To use Mobile Device Management, the server must be an Open Directory Master and have valid certificates for SSL and Apple Push Notification. For information about Mobile Device Management, click Open Profile Manager and choose Help from the User menu. The Configure Device Management assistant will open to guide you through the steps needed to configure these services.
3. In Configure Device Management, click Next.
5. In the Directory Administrator dialog, enter the account information for the administrative user of the new Open Directory instance you’re creating.

6. Click Next.
7. In Organization Information, enter the name of your organization and an administrator email address for the Open Directory instance you’re creating. (Don’t include commas in your organization name.)

![Organization Information](image)

8. Click Next.

9. In Confirm Settings, review the settings to create the new Open Directory master.

![Confirm Settings](image)

10. If the settings are correct, click Set Up. If you need to make changes, click Back.

11. In Organization Information, enter any contact information that you wish to provide users, then click Next.

If you haven’t installed a code-signing certificate from a trusted authority, you’ll get a warning. You can still use the server’s self-signed certificate, but those users with devices that you wish to manage will need to take an extra step to explicitly trust your server.

13. Click Next.

To push profile changes to devices, you must configure a server to use Apple Push Notification service (APNs). This requires getting certificates for the service from Apple.

14. In “Get an Apple Push Notification Service certificate,” enter your organization’s Apple ID and password. If your organization doesn’t have an Apple ID, click “Create one now.”

15. Click Next.


At this point, you can start using Profile Manager to manage devices, but you can still make some service configurations.

17. To assign apps and books purchased through VPP, select “Assign apps and books from the Volume Purchase Program.”

For information about how to assign apps and books purchased through the VPP to users or groups, click Open Profile Manager and choose Help from the User menu.

18. To sign profiles using a certificate, select “Sign configuration profiles,” then choose a certificate from the Certificate pop-up menu.

If the certificate isn’t available in the menu, select Import from the Certificates pop-up menu and import a certificate.

19. To include configurations for services on your server in your default configuration profile, select “Include configuration for services.”

You can change the name of the configuration profile by clicking Edit next to Name.
20. To send the URL of the Profile Manager server to users so they can log in and
download the configuration profiles you assigned, click the arrow next to Visit User
Portal, then copy the URL from the browser window that opens.

For information about how users interact with Profile Manager, click Open Profile
Manager and choose Help from the User menu.

21. To specify settings and assign them to users, devices, and groups, and to manage
enrolled devices, click Open Profile Manager.

When Profile Manager opens in your web browser, log in with your administrator
name and password.

Configuring users

Before users can access most services on an OS X Server, you need to create accounts
for them on the server. These accounts can reside in a directory service or locally on
the server.

If your server is bound to a directory service, such as Microsoft Active Directory, no
further work is needed. If not, create users before setting up profiles in Profile Manager.

To add users to your OS X Server once it's running Open Directory, use the Server app.
This section covers creating users in the Server app.

Note: If the server is bound to another directory service (for example, Active
Directory), manage users there rather than from OS X Server.

To create users in OS X Server:

1. Open the Server app (located in /Applications).
2. Under Accounts on the left, select Users.
3. From the pop-up menu in the Users pane, choose Local Network Users.
4. Click the Add (+) button.
5. When prompted, enter the user details.
   • Full Name: Provide the user's first and last name.
   • Account Name: Enter the user's short name (typically first initial, last name, or
     firstname.lastname).
   • Email Address: Provide the email address to send invitations and other items for the
     user.
   • Password: Enter a password for the user.
   • Verify: Enter the password a second time to make sure it's correct.
6. Do not select the "Allow user to administer this server" checkbox.
7. For Home Folder, choose "None - Services Only."
8. Click Done to save the new user.

The new user now appears in the list of Local Network Users.
You can create groups in the same way.
Only users created in the Server app after it’s promoted to an Open Directory master can be added to that Open Directory domain. Because local and Open Directory accounts have different user IDs, promote any systems that need shared accounts to an Open Directory master before creating users.

**Manual download versus automatic push**

When you set up configuration profiles, you can choose between two distinct types: Manual download and automatic push. Both are assigned to devices either directly or through inheritance, but they’re deployed to clients in different ways.

Manual download profiles function exactly as their name implies. Users must manually install these configuration profiles on their device. These profiles are usually emailed to users, or users download them from a webpage and install them. The Profile Manager service makes these profiles available for download on the device portal page following user authentication. These profiles are static, and the payload isn’t updated unless the user downloads them again and installs an updated profile.

In contrast, automatic push profiles are distributed without user interaction following initial deployment of the profile. After a device is enrolled via the device portal page, an Apple Push Notification alerts the device of any new profiles or changes to existing profiles. Any change to the settings of an automatic push profile results in client notification.

It’s important to realize that push notification doesn’t distribute the actual profile—it alerts the device that it needs to retrieve and apply an updated configuration profile. For these notifications to work properly, you must allow the Apple Push Notification service to pass your network firewall.

For OS X computers and an 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 17.0.0.0/8 network to provide maximum flexibility in scaling the service. The entire 17.x.x.x network is safely maintained and securely controlled by Apple.

**Editing management profiles**

Apple has included the web-based Profile Manager application to facilitate the creation and delivery of configuration profiles. You can use Profile Manager to create, edit, and delete profiles as well as create device and user groups for controlling profile distribution. Users and groups from enterprise directory services (such as Active Directory) appear in Profile Manager only if the OS X Server has been properly bound.

Keep in mind that while each user, group, device, or device group can have only one profile assigned to it in Profile Manager, each device may belong to many groups. This enables the layering of settings via profile inheritance.

**General settings**

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 replaces 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.

**To edit configuration profiles:**

1. Open a web browser and navigate to https://yourserver/profilemanager (where *yourserver* is the name or IP address of your server running the Profile Manager service).

2. Authenticate as needed with administrative credentials.

3. Select the user, group, device, or device group you want to edit.
4. Click the Settings tab.

8. Click OK.

Note: When you update settings for an automatic push profile, devices receive Apple push notifications.
To create custom profile settings:

You can manage settings beyond those defined by Profile Manager. With the Custom Settings, you can add a payload with key value pairs that override settings in the corresponding preference domain.

For example, there isn’t a payload setting that corresponds to the Finder’s preference controlling the display of hard drives on the desktop.

1. Open a web browser and navigate to https://yourserver/profilemanager (where yourserver is the name or IP address of your server running the Profile Manager service).
2. Authenticate as needed with administrative credentials.
3. Select the user, group, device, or device group you want to edit.
4. Click Edit for the profile.
5. From the list of payload types, select Custom Settings.
6. Click Configure.
7. Enter the name of the identifier of the preferences set that you want to manage.
   This example uses com.pretendco.widget, which is the identifier for an in-house app at PretendCo.
8. Click Add Item.
9. Under Key, replace the New Item text with the key representing the preference you want to manage.
   In this example, the Widget preference to automatically dial phone numbers selected in the app is AutoDialNumbers.
10. From the Type pop-up menu, choose the value type for the setting.
    The AutoDialNumbers setting is Boolean.
11. Set the value.

   For the Boolean type, the value is represented by a checkbox (selected = true, unselected=false).

12. Click OK.

   The Custom Settings payload is added to the profile.

13. Click Save to save the updated profile.

14. Click Save when asked to confirm that you want to update the profile.

   An alternative to steps 7 through 11 is to click Upload File to upload a preferences file from your computer. You then delete any preference entries you don’t want to manage.

**Creating device groups**

Use device groups to easily assign profile settings for specific groups of Mac computers and quickly apply settings appropriate for each logical grouping of devices.

**To create a device group:**

1. Open a web browser and navigate to https://yourserver/profilemanager (where yourserver is the name or IP address of your server running the Profile Manager service).

2. Authenticate as needed with administrative credentials.

3. In the Profile Manager sidebar, select Device Groups.
4. Click Add (+) under the groups list to create a new device group.
5. Enter a name for the new device group.
6. Click Settings.

7. Configure the group settings and profile.
8. Click Save.

**Adding devices to a device group**

After a device has been enrolled with your Profile Manager server, you can assign the device to a group so that you can manage several devices with a common profile.

**Note:** You’ll learn about device enrollment a bit later in this chapter.

**To add devices to a device group:**

1. Open a web browser and navigate to https://yourserver/profilemanager (where yourserver is the name or IP address of your server running the Profile Manager service).
2. Authenticate as needed with administrative credentials.
3. In the Profile Manager sidebar, select Device Groups.
4. Select a device group.
5. Click Add (+) inside the Group pane on the right and choose Add Devices.
A dialog appears displaying all the enrolled devices.

6. Click the Add button for each device that you want to add to the group.
   If you want to remove a device that was added to the group, click the device’s Remove button.

7. Click Done when you’re finished adding devices.
   The device group updates to reflect the changes you made.

8. Click Save when you’re finished.

Using device placeholders

Using device placeholders, you can prepopulate device records and groups with profile settings. A placeholder record is created based on the device’s serial number, Unique Device Identifier (UDID), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID). When you enroll the matching device, it assumes the identity of the placeholder record.

If the OS X or iOS device is removed from management, or the record is deleted, the placeholder account isn’t automatically re-created.

To create a device placeholder:

1. Open a web browser and navigate to https://yourserver/profilemanager (where yourserver is the name or IP address of your server running the Profile Manager service).

2. Authenticate as needed with administrative credentials.

3. From the Library list on the left, select Devices.

4. Click Add (+) on the right and choose Add Placeholder.
5. In the Add Device dialog, choose iOS/OS X from the Device Type pop-up menu.
6. Enter a name for the device.
7. Choose a Serial Number from the Identifier Type pop-up menu and enter the serial number for the device that you’ll enroll later.

![Add Device dialog](image)

8. Click Add.

A placeholder is added to the Devices list.

![Placeholder added](image)

**To import a device list:**

Instead of adding devices to Profile Manager one at a time, you can upload a text file in comma-separated values (CSV) format.

The CSV file should have the following column headers:

<table>
<thead>
<tr>
<th>Column header</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeviceName</td>
<td>OurPhone</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>23432AABCZ5</td>
</tr>
<tr>
<td>IMEI</td>
<td>U8938932ae89ui8989eaooi78</td>
</tr>
<tr>
<td>MEID</td>
<td>1312aiu3io2o243234oo23</td>
</tr>
<tr>
<td>UDID</td>
<td>ab458782ui3972342</td>
</tr>
</tbody>
</table>

The file can be a mix of any number or type of identifiers for each device name. The DeviceName column is required for each row.

1. From the Library list on the left, select Devices.
2. Click Add (+) on the right and choose Import Placeholders.
3. Select the CSV text file, then import.
Enrolling OS X–based devices

After you've set up the Profile Manager server, you can enroll devices. When you log in to the user portal, you'll see two tabs: Devices and Profiles. The Devices pane shows the devices you've registered. You can also enroll new devices through this pane. The Profiles pane shows the download profiles available to you—the logged in user.

To enroll a Mac:

1. Open a web browser and navigate to https://yourserver/mydevices (where yourserver is the name or IP address of your server running the Profile Manager service).
2. Authenticate with a user account on the server.
   The My Devices page will appear.
3. If you're using a self-signed certificate, click the Profiles tab, then click Install for the Trust Profile.
4. Click the Devices tab.
5. Click Enroll.
   The profile downloads to the browser. The Profile pane of System Preferences automatically opens and displays information about the profile being installed.

6. Click Continue.
   You’ll be asked to confirm that you want to install the Device Enrollment profile.

7. Click Install to confirm installation.

8. Repeat this process until each profile has been installed.
   The Mac is now enrolled and appears in the Devices section of Profile Manager.

**Locking a device with the user portal**

After you’ve enrolled a device using Profile Manager, the user responsible for it can perform basic security tasks. The most basic is a remote lock, helpful when a device is misplaced or stolen.

**To remotely lock a device with the user portal:**

1. Open a web browser and navigate to https://yourserver/mydevices (where yourserver is the name or IP address of your server running the Profile Manager service).
2. Log in as the user who enrolled the device.
3. Click the Devices tab.
The Devices pane shows enrolled OS X and iOS computers.

4. Click Lock for the device you want to lock.
5. Enter the passcode code when prompted.
When you lock an OS X computer, it immediately reboots to a PIN pad. Only the PIN you created in the user portal can unlock it.

Wiping a device with the user portal

After you've enrolled a device using Profile Manager, the user responsible for it can perform basic security tasks. Remote wipe is the most intrusive action because it erases all data on the device.

Before setting up remote wipe on an OS X computer, make sure the system is using FileVault 2 to fully encrypt the hard drive. Although you can still wipe a Mac that isn’t protected by FileVault 2, the wiping process takes much longer.

For more information about FileVault 2, visit http://support.apple.com/kb/HT4790.

To remotely wipe a device with the user portal:

1. Open a web browser and navigate to https://yourserver/mydevices (where yourserver is the name or IP address of your server running the Profile Manager service).
2. Log in as the user who enrolled the device.
   The Devices pane shows enrolled OS X computers.
3. Click Wipe for the device you want to wipe.
4. Enter the passcode, then click Wipe.

5. Click OK to confirm that you want to wipe the computer.
   The Mac will be wiped, erasing all data.
   Administrators can verify that the device has been wiped in Profile Manager.

   ![Image showing the lock and wipe options]

   Note that the device entry is now a placeholder. If the device is ever reenrolled, it will automatically match up to the device’s Profile Manager entry.

   **Locking a device as an administrator with Profile Manager**

   After you’ve enrolled a device using Profile Manager, the user responsible for the device can perform basic security tasks. With Profile Manager, administrators also have the ability to perform security tasks on remote devices.

   **To remotely lock a device with Profile Manager:**

   1. Open a web browser and navigate to https://yourserver/profilemanager (where *yourserver* is the name or IP address of your server running the Profile Manager service).
   2. Authenticate as needed with administrative credentials.
3. From the Library list on the left, select Devices or Device Groups.

4. Select the device or device group you want to lock.

5. Click the Action menu (gear icon) in the device or device group pane.

6. Choose Lock.

7. Enter a lock PIN code that can be used to unlock the device.

8. Click Lock.

When you lock an OS X–based computer, it immediately reboots to a PIN pad. Only the PIN entered in Profile Manager can unlock the device.
9. To make sure the device has been locked, go to the Completed Tasks section of Profile Manager.

Wiping a device as an administrator with Profile Manager

After you've enrolled a device using Profile Manager, the user responsible for the device can perform basic security tasks. With Profile Manager, administrators also have the ability to perform security tasks on remote devices.

To remotely wipe a device with Profile Manager:

1. Open a web browser and navigate to \https://yourserver/profilemanager\ (where \yourserver\ is the name or IP address of your server running the Profile Manager service).

2.Authenticate as needed with administrator credentials.

3. From the Library list on the left, select Devices or Device Groups.

4. Select the device or device group you want to wipe.

5. Click the Action menu (gear icon) in the device or device group pane.
6. Choose Wipe.

7. Enter the passcode, then click Wipe.
   The device will be locked and wiped. All data will be lost.

8. To make sure the device has been wiped, go to the Completed Tasks section of Profile Manager.

### Removing a device from management with the user portal

Just as you can enroll, lock, and wipe a device from the user portal of Profile Manager, you can also disable remote management of a device by removing it from management.

**Note:** Removing a device from management also removes the associated profiles and any access configured by those profiles.

**To remove a device from management with the user portal:**

1. Open a web browser and navigate to https://yourserver/mydevices (where yourserver is the name or IP address of your server running the Profile Manager service).
2. Log in as the user who enrolled the device.
The Devices pane shows the OS X and iOS devices you’ve enrolled.

3. Click the Remove link in the upper right of the device entry.
4. Click OK to confirm that you want to remove the device.

The device record is removed from Profile Manager and the device is no longer considered managed.

**Removing a device from management with Profile Manager**

Users who enrolled devices can use the user portal in Profile Manager to lock and wipe devices, as well as disable remote management. With Profile Manager, administrators also have the ability to act on remote devices.

**Note:** Removing a device from management also removes the associated profiles and any access configured by those profiles.
To remove a device from management with Profile Manager:

1. Open a web browser and navigate to https://yourserver/profilemanager (where
yourserver is the name or IP address of your server running the Profile Manager
service).

2. Authenticate as needed with administrator credentials.

3. From the Library list on the left, select Devices.

4. Select the device you want to remove.

5. Click Remove (−) below the list of devices.

6. Click Unenroll to confirm that you want to remove the device from Profile Manager.
Although the device is removed from Profile Manager, a placeholder is left behind. If
the device is ever reenrolled, it will be matched to the placeholder, and any profiles
associated with the placeholder will be downloaded to the device.

7. Confirm that the device no longer appears in the Devices section of Profile Manager.

Managing profiles on client computers

After you install configuration profiles in OS X, the Profiles pane in System Preferences
appears.

You can use the Profiles pane to review which profiles are installed, add additional
profiles, and remove or verify existing profiles. You can also install configuration
profiles by double-clicking them in the Finder.

Note: Any user with administrative access can remove a device profile.
To remove a profile:

1. Open System Preferences.
2. Click Profiles.
3. Select the device profile you want to remove.
4. Click Remove (−).
   A dialog appears asking if you’re sure you want to remove the profile.
5. Click Remove to confirm that you want to remove the profile.
6. Enter an administrative user name and password, then click OK.

Forcing management profiles

You can use management profiles to enforce policy. Administrators have a few options for controlling how profiles are removed when they create the profiles in Profile Manager.

The default setting is to always allow removal. This means that users can remove user profiles that apply to them. Any user with administrative rights can remove device profiles on a Mac. However, some policies should be enforced regardless of whether the user wants to have them.

The Authorization feature secures profile removal, requiring a specific password to edit a profile. Only users with the profile password may remove it.

The Never removal setting indicates that a profile can’t be removed. The device must be wiped to remove the profile.
To change profile removal rules:

1. Open a web browser and navigate to https://yourserver/profilemanager (where yourserver is the name or IP address of your server running the Profile Manager service).

2. Authenticate as needed with administrator credentials.

3. From the Library list on the left, select Devices, Device Groups, Users, or Groups.

4. Select the device, device group, user, or group you want to edit.

5. Click Edit for the profile.
   
   The settings screen appears for the profile you chose.

6. In the General settings for the profile, change the Security settings as needed.

7. Configure the other settings that should be deployed with the profile.

8. Click OK to close the settings pane.

9. Click Save to update the profile settings.
Client management suites

The workflow that an administrative team develops for software delivery and management, patching, and remediation is often centralized around a client management suite. One of the side effects of this is that the workflow often ends up redefining the imaging workflow in a number of ways.

For available software solutions, see the following lists.

Imaging and client management

- JAMF’s Casper Suite—http://www.jamfsoftware.com
- Absolute Manage—http://www.absolute.com
- KACE—http://www.kace.com
- LANDesk—http://www.landesk.com
- FileWave—http://www.filewave.com

Client management only

- AirWatch—http://www.air-watch.com
- MobileIron—http://www.mobileiron.com
- Centrify—http://www.centrify.com
- Thursby’s ADmitMac—http://www.thursby.com
- Quest Management Xtensions (QMX)—http://www.quest.com

Additional resources

- Managing Devices with Configuration Profiles, OS X Server Essentials 10.9: Using and Supporting OS X Server on Mavericks, Peachpit Press
Managing Software Updates

The Software Update service offers ways to manage Mac software updates from Apple on your network. In an unsupervised environment, users might connect to Apple Software Update servers at any time and update their computers with software that isn’t approved by your IT group.

Using local Software Update servers, your client computers access only the software updates you permit from software lists that you control, improving your ability to manage the updates. For example, you can:

- Download software updates from Apple Software Update servers to a local server for sharing with local network clients and reduce the amount of bandwidth used outside your network.
- Direct users, groups, and computers to specific local Software Update servers using configuration profiles.
- Manage the software update packages that users can access by enabling and disabling packages at the local server.
- Mirror updates between Apple Software Update servers and your server to make sure you have the most current updates.

Software update policy

After Mac computers are deployed, developing an effective policy for managing software updates is crucial to prevent bad updates from being deployed throughout an organization, and to eliminate the need to redeploy known good systems. The policy should include fully testing updates before they’re released, releasing updates, and logging changes into your organization’s configuration management database.

Below is an example of a three-phase policy that works well for managing software updates:

- **Phase 1** After an operating system or application update is released, there should be a “cooling-off” period of seven calendar days before deploying the update. This gives the vendor time to issue patch recalls or revisions and for your organization’s IT department to perform basic functionality testing.

- **Phase 2** After the cooling-off phase, deploy the update to a pilot group to test for five business days. This group should be composed of “power users” who cover a
wide range of operational tasks and can give effective feedback. Deploying to a pilot group helps ensure that production won’t be affected if problems with the update arise.

• Phase 3 After the pilot phase is complete, the update can be delivered to all workstations and integrated into the master deployment image.

If issues arise during any phase, your policy should call for a restart of that phase. For example, if Apple releases a security update and revises it five days later, a new seven-day cooling-off period should begin.

The three-phase policy cycle minimizes the risks of widely deploying problematic updates.

Using the OS X Server Software Update service

With OS X Server, you can build a Software Update service that mirrors updates from the Apple Software Update service. This helps keep large operating system updates and software packages from increasing network traffic in environments with larger deployments and offers IT departments a built-in way to manage releases.

The Apple Software Update service runs on the Apache web server in OS X Server. The Software Update service synchronizes updates from Apple Software Update servers and stores update digests in XML files. Client computers poll the XML files to determine which updates to install, then downloads and installs them routinely.

Note that only updates marked as Enabled in the Software Update service are available for client computers to download. An administrator can disable an update, blocking its distribution until the update has been approved.

To configure the Software Update service for OS X Server:

1. Open the Server app (located in /Applications/).
2. Select Software Update in the sidebar, then click Settings.
3. Click the Settings tab.
4. Choose whether updates should be automatic or manual.

Automatic updates mirror those from Apple with no intervention. With manual updates, administrators are given the choice to release each patch provided by Apple.
5. Click the On/Off button to turn on the Software Update service and begin caching the patches from Apple.

6. Click the Updates tab.

Note: If you don’t immediately see the updates, don’t be concerned. In some cases, it can take a number of hours for them to appear.
To enable or disable a software update:

You can enable or disable software updates on your Software Update server using the Server app. When you enable updates, you make them available to your clients for downloading and installing from your Software Update server. If you disable updates, the updates might be downloaded to your server but won't be available to your clients to install.

1. In the Software Update pane, click the Settings tab.
   To manage available updates, the Software Update service must be set to Manual mode.
3. Click the Updates tab.
4. From the list of updates, select the update or updates that you want to enable or disable.
5. From the Action menu (gear icon), choose Enable or Disable.
Configuring Software Update server clients

After you've set up Software Update services, you'll want to point client computers to it. You should do this in a testing environment first and make sure that clients are updating as intended before pushing settings across your organization (whether using Profile Manager or manually changing the com.apple.SoftwareUpdate.plist file to do so).

To configure clients to use a Software Update server using Profile Manager:

The Policy Management chapter of this guide explains how to set up and use Profile Manager to manage OS X and iOS devices.

After you've set up the Profile Manager service, you can modify a profile to configure clients to use a specific Software Update server.

1. Select an existing device profile or create a new one.
2. Click Edit to add a payload to the profile.
3. From the list on the left, select Software Update.
4. Click Configure.
5. Enter the URL for your Software Update server.

   The URL should be in the form:

   `http://server.example.com:8088/catalogs.sucatalog`

   (where `server.example.com` is the actual IP address or DNS name of the host running the Software Update service).

6. Click OK.

7. Click Save, then click Save again to confirm saving the updated profile.

**To manually configure clients to use a Software Update server:**

If your client systems aren't managed, or if you want to test the functionality of the Software Update service without using a policy, use the following command to augment the default software update settings (replacing `server.pretendco.com` with the actual IP address or DNS name of the host running the Software Update service):

```bash
```

You can reset the Software Update settings to factory defaults by deleting the `/Library/Preferences/com.apple.SoftwareUpdate.plist` file and allowing the system to generate a new preferences file based on the default settings.

To point the client computer back to the Apple Software Update server, use the following command:

```bash
defaults delete /Library/Preferences/com.apple.SoftwareUpdate CatalogURL
```
Installing updates on an OS X computer with Software Update

You can check for updates manually or set your computer to check for updates automatically. These include important security updates that protect your computer from potential threats.

To check for updates manually in Software Update:

2. Select or unselect the checkboxes for available updates, then click Install.
   When the installation is complete, Software Update checks for updates again. It does this because some updates require that you’ve installed previous updates.

To set Software Update to check for updates automatically:

1. Choose Apple menu > System Preferences, and click App Store.
2. Select the “Automatically check for updates” checkbox.
3. If you want your computer to download important updates without asking, select the “Download newly available updates in the background” checkbox. When the update finishes downloading, you’re notified that it’s ready to be installed.
4. If you want to have your Mac install system files and security updates automatically, select the “Install system data files and security updates” checkbox.

Third-party software update service

Many third-party patch management solutions rely on out-of-band management for Apple-based software updates and patches.

One third-party option is an open source project called Reposado, a set of Python-based tools that replicates the Software Update service in OS X Server. Reposado downloads updates from Apple and synchronizes them to a local web server, generating the indexes and plists as needed. Reposado runs on any operating system that supports cURL, Apache (or another web server), and Python.

Another option is for the client management software to download packages from Apple and host them on staging servers. Agents running on client systems then download Apple updates from the staging servers rather than from Apple. Agents can be forced to obtain software updates from a local staging server. Both Absolute Manage and JAMF have this functionality and can be run on OS X Server, Linux Server, or Microsoft Windows Server.

Additional resources

- Implementing Software Update Service, OS X Server Essentials 10.9: Using and Supporting OS X Server on Mavericks, Peachpit Press
The Caching service speeds up the download of software distributed by Apple through the Internet. It caches all software updates, Mac App Store purchases, iBooks, iTunes U (apps and books purchases only), and Internet Recovery software that local Mac and iOS devices download.

Without any configuration, OS X and iOS devices are able to take advantage of a Caching server. When you set up a Caching server, the server registers its public IP address with Apple. When the Mac App Store, iTunes, or iBooks apps on devices that share the same public IP address make download requests, the client devices are automatically redirected to the local Caching server. When a client device leaves the network, such as when a MacBook is taken home, it reverts back to getting software directly from Apple.

Requirements

The Caching server supports clients with OS X v10.8.2 or later and iOS 7 or later, and requires that clients share the same public IP address behind a NAT.

The following figure is an example of a single subnet with a Caching server:
If your network has multiple subnets that share the same public IP address, the subnets can take advantage of the Caching server. For example, the following figure shows a network with two subnets sharing a single Caching server:

You can get the best performance from your Caching server by connecting it to your network using Ethernet. The Caching server can serve hundreds of clients at once, saturating a Gigabit Ethernet port. Therefore, in most small- to medium-scale deployments, the performance bottleneck is usually the bandwidth of your local network. To determine if your server hardware is your performance bottleneck when a large number of clients are accessing the server at the same time, check the Processor Usage graph in the Stats pane of Server app. If the processor usage is constantly at or near the maximum, you may want to add Caching servers to distribute your clients’ caching requests across multiple servers. Also, if your server is in an environment where clients download a wide variety of large amounts of content, be sure to set the cache size limit high enough. This prevents the Caching server from deleting cached data frequently, which may cause the redownloading of the same content at the expense of more Internet bandwidth consumption.

Managing the Caching service

The default location for cached content is the boot volume. You can choose an alternate location and specify how much of the volume is used by the service.

As the Caching server gets requests for content to be downloaded and cached, more of your disk space is used to store the cached content. When the disk space of the cached content reaches the maximum you specified in the Caching pane, or when the available space on the volume reaches 25GB, the Caching server deletes the least recently used cached content to make space for the next request.
To start the Caching service:
1. Open the Server app (located in /Applications/).
2. Select Caching in the sidebar.
3. Click the On/Off button to turn on the Caching service.

At this point and without any additional configuration, the Caching service starts to cache Mac App Store and iTunes downloads.

To select a volume for caching:
1. In the Caching pane, click Edit.
2. Select a storage volume.
3. Click Choose.
To delete all cached content:

1. Click Reset in the Caching pane.
2. If you're sure you want to proceed, click Reset again.

To set cache size:

In the Caching pane, use the slider to adjust the caching limit.

Comparing the Caching and Software Update services

The Software Update service and the Caching service both provide updates to software installed on Mac clients. However, the following are key differences between these services:

- The Software Update service caches only Mac updates; the Caching server can cache updates and Mac App Store purchases for Mac computers and iOS devices.
- The Software Update service requires you to manually configure clients to use only a specific software update server; the Caching server requires no client configuration. OS X and iOS devices automatically access the available Caching server on the network they're currently connected to, making the Caching server mobile-client friendly. For example, when a user is using an OS X or iOS device at work, the device uses the Caching server at work. When the same user uses the same device at home, the device automatically uses another Caching server.
- The Software Update service downloads and caches all available updates when it first starts up; the Caching service downloads and caches software based on client requests.
- The Software Update service provides client management functionality, such as the ability for administrators to restrict which updates can be seen and downloaded by clients. The Caching service doesn’t provide any client management functionality.

If you need client management functionality, use the Software Update service. Also, if you configure your client to use the Software Update service, the Software Update service takes precedence and the client can’t use the Caching service.

Important: The Caching service and Software Update service can coexist on the same server, but they don’t share cached content, which may result in additional disk space being used.

Client configuration

To access your Software Update server, you need to configure the Software Update preferences on your client computers to direct them to the server. You can manage preferences in Workgroup Manager or configuration profiles, or you can modify the preferences directly.

No client configuration on your part is required with the Caching service. On a regular basis, a Caching server registers itself and its public IP address with Apple’s software servers. When client devices attempt to access Apple’s servers, the devices are automatically directed to the Caching server associated with your public IP address.
Download management

With the Software Update service, you can select which updates are available to the client computers. This is useful for organizations that want to restrict access to new software until it has been tested for compatibility.

The Caching service doesn’t provide any control over software availability.

Note that client computers that are configured to use your Software Update server don’t access a Caching server for software updates. They do, however, still use the Caching server for other downloads, such as app purchases.

Software cached

Both services cache Apple-provided software updates, but the Caching service also caches other content downloaded using iTunes, the App Store, iBooks, or the Mac App Store, such as apps and books.

When software is cached

With the Software Update service, all updates are downloaded in advance of client computers requesting them, usually when the Software Update service is turned on and as updates become available afterward.

With the Caching service, software is downloaded and cached as client computers request it. The first computer to request an app experiences a longer download time. All computers requesting the same app afterward experience faster downloading as they get the app from the Caching server.

Additional resources


• Caching Content from Apple, OS X Server Essentials 10.9: Using and Supporting OS X Server on Mavericks, Peachpit Press
Mac Management Basics Exam
Add Apple Certified Associate - Mac Management 10.9 to your credentials. Instructions for taking the online exam are at training.apple.com/itpro/macmgmt/109exam.

OS X Training & Certification
Apple offers comprehensive certification programs for IT professionals in business, education, and other fields. Review the training and certification options below to find the path best suited to your goals.

OS X Courses
Courses are taught by Apple Certified Trainers through a worldwide network of Apple Authorized Training Centers (AATCs).

OS X Support Essentials 10.9: Provides an intensive and in-depth exploration of troubleshooting on OS X, touring the breadth of functionality of OS X systems.

OS X Server Essentials 10.9: Gives technical coordinators and entry-level system administrators the knowledge to implement an OS X Server–based system.

OS X Certifications
Apple’s OS X Certifications are designed for IT professionals who:
• Support OS X users in a business, education institution, or school district
• Manage networks of OS X systems in an organization—for example, a teacher or a technology specialist who manages classroom networks or computer labs
• Manage complex, multiplatform networks that include OS X systems
Apple Certified Associate - Mac Integration certification verifies an understanding of the different ways to integrate a Mac within a Windows or other standards-based network.
Apple Certified Associate - Mac Management certification verifies a basic understanding of the different ways to deploy and manage Mac computers.

Apple Certified Support Professional (ACSP) is next on the OS X certification path, validating basic OS X support and troubleshooting skills.

Apple Certified Technical Coordinator (ACTC) certification builds on ACSP by certifying essential OS X Server support and troubleshooting skills.

For information about all available Apple Certifications, visit training.apple.com/certification.

Books

The Apple Training Series books constitute a key part of Apple’s official curriculum, covering OS X and OS X Server. These books offer an independent approach to training and certification, guiding students step by step through real-world projects. The books are also excellent references for performing specific tasks and technologies.

There are two titles in the Apple Training Series, written for IT support and system administration personnel:

- OS X Support Essentials 10.9
- OS X Server Essentials 10.9

For more information about the books, visit Peachpit Press at www.peachpit.com/appleprotraining.

Support

In addition to the AppleCare Protection Plan, Apple provides online support at www.apple.com/support, where you can access technical articles, download manuals, and join discussion forums.

The Apple Support site also provides some online training materials for those who are new to OS X at www.apple.com/support/macbasics/.