Mac Management Basics 10.10

Deploying and Managing Multiple Mac Computers

01-05-2015

Contents

Introduction

Overview

This guide introduces you to creating and deploying system images for new and existing Mac computers. You'll learn how to manage Mac computers with the Apple Remote Desktop and the OS X Server Profile Manager service. You'll also learn how to streamline and manage OS X updates with OS X Server Caching and Software Update services.

Prerequisite knowledge

This guide assumes you have a basic understanding of OS X software, features, apps, and terminology. If you're new to Mac, review Mac Basics.

You should also have a basic understanding of how to configure OS X, including how to connect to a network and access network services. Network services include, but aren't limited to, file servers, network printers, and directory servers.

Additional resources

- *Mac Integration Basics* introduces how to configure a Mac for a cross-platform environment.
- *OS X Support Essentials* presents OS X Yosemite functions and tells you how to support users. The *OS X Support Essentials 10.10* book is available from Peachpit Press in print or online. You can also attend a three-day hands-on course.

Creating System Images

1

This chapter shows you how to create system images with System Image Utility. But before you learn how to create system images, you'll learn about hands-off deployment of system images, and why that might be your best choice. You'll also learn about different disk image types. After you learn how to create system images, you'll learn how to create modular images.

Consider hands-off deployment

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

Traditionally, to deploy computers, you would create system images and copy them to each computer in the organization. Deploying computers this way creates consistency in computer configurations, but it makes more work for your IT organization, which has to maintain a set of images and ensure that those images contain the latest operating system updates and apps.

Instead, Apple recommends hands-off deployment. With hands-off deployment, you can give your users their new Mac computers and allow them to perform the initial configuration by downloading the software they need. They can do this from an internal website or the Mac App Store.

If you decide to create system images and copy them to each computer in your organization, consider the following to minimize IT involvement:

- Minimize customizations to your deployment image so you won't have to revise it continually. Ideally, your deployment image should contain only OS X, local settings, and software packages that should be installed on all Mac computers in your organization.
- Make full use of directory services so you have centralized control over user identities and data. Build a script that binds each Mac in your organization to your directory services, and add it to your deployment image. Do these things to provide a cohesive data-management policy.
- Use a client management agent and build it into your deployment image. On initial startup, each Mac contacts the client management suite and uploads its inventory

information. Any unit-specific software is provisioned, along with any updates for the current deployment image. With most client-management suites, optional applications are delivered to users' Mac computers via self-service software tools.

Disk image types

Disk images are computer files that contain the structure and contents of a disk volume. They also contain an entire storage device such as a hard drive or a Universal Serial Bus (USB) flash drive. There are two types of disk images:

- A disk image is a file (with a name that usually ends with .dmg). It's also called a boot image or system image. A disk image looks and acts like an installer, mountable disk, or volume. Use Disk Utility to create disk images.
- A network disk image is a folder (with a name that ends with .nbi) containing a disk image (.dmg) file. It's also called a network boot image or system image. A client computer can start and run from a network disk image, at least long enough to install the software contained in that image. Use System Image Utility to create network disk images. Use OS X Server NetInstall to deploy network disk images across a network.

Creating network disk images

Traditionally, you would use Disk Utility to create OS X system images. Although you can still use it to create images, you must prepare systems beforehand. Also, Disk Utility doesn't include the OS X Restore partition as part of the image creation process. Go to Launchpad > Other to find Disk Utility.

Instead, use System Image Utility to create network disk images. It's included with all OS X Yosemite computers. Go to: System > Library > CoreServices > Applications.

Unlike Disk Utility, System Image Utility prepares and creates an image simultaneously. It also automatically creates an OS X Restore partition.

With System Image Utility, you can create and customize three types of network disk images: NetBoot, NetInstall, and NetRestore.

- **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 OS X Yosemite without erasing the target volume. You can 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 in which customizations are used, NetInstall users are presented with the same user interface they would see if they were using the OS X Installer on a local drive. Customization examples include repartitioning hard drives, using predefined OS installation choices, binding systems to directory services, renaming client systems, and installing additional software packages.

- **NetRestore** images clients using a prebuilt disk image with Apple Software Restore block-copy format. (Apple Software Restore is a Mac OS X application.)

  With NetRestore, you can pre-populate a single boot image with predefined choices, or clients can browse for multicast Apple Software Restore streams using the Apple Bonjour browsing technology. When you create NetRestore sets, you can:

  - Image an existing OS X computer.
  - Create an image programmatically with a custom package set.
  - Allow for the arbitrary sourcing of Apple Software Restore images. That is, you can choose an image located on a web server or an Apple file server, or use multicast Apple Software Restore.

Although System Image Utility creates images that are restored over the network, you can use network disk images to restore systems locally, too.

Obtaining valid OS X image sources or volumes

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 hard disk. You can't create an image on a volume over the network.

Creating a NetInstall image with System Image Utility

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

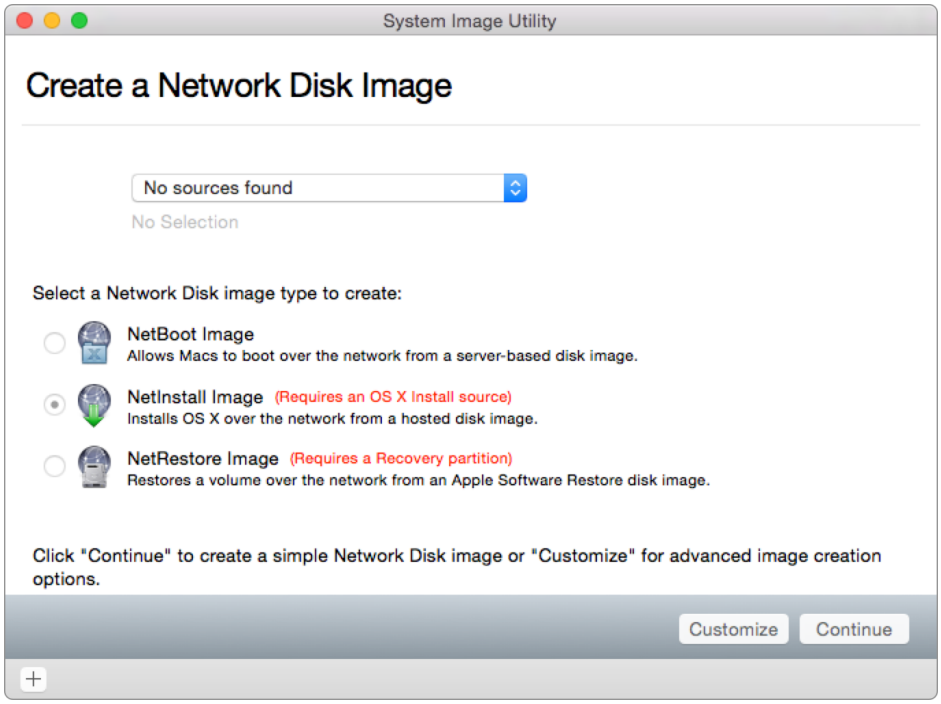
NetInstall images deployed with OS X Server are a convenient way to install a clean version of OS X on any Mac in a network, even if the disk drive was completely erased.

To create a NetInstall image with System Image Utility:

1. Download—but don't install—OS X Yosemite from the Mac App Store. Don't restart your computer after you download OS X Yosemite.

   The OS X Yosemite app is copied to /Applications/.

2. If the OS X Yosemite Installer opens, quit it.
3. Open System Image Utility from System > Library > CoreServices > Applications.



4. From the Source pop-up menu, choose Install OS X Yosemite.
5. Select NetInstall Image.

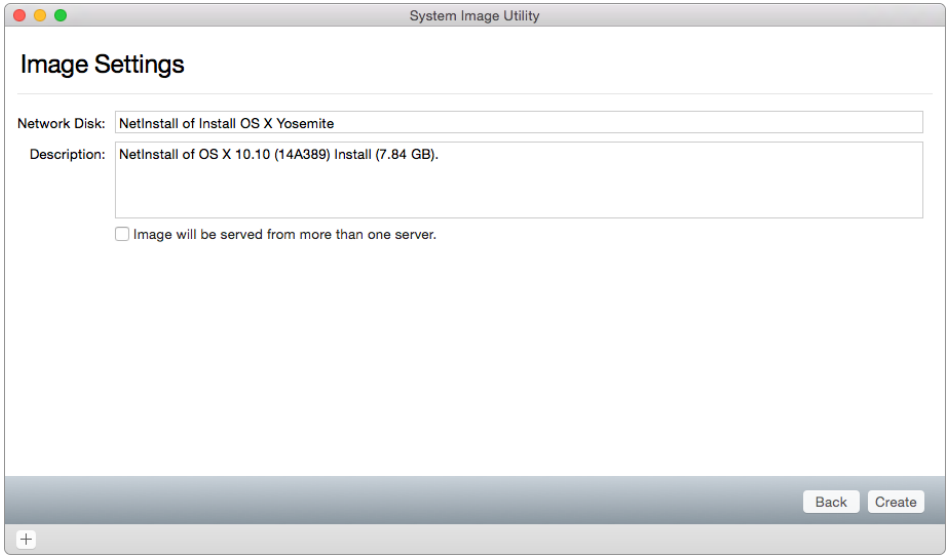
   This tells the image, when NetBoot loads it, to install an operating system.
6. Click Continue.
7. In the Network Disk field, enter a name for your image.

   This name identifies the image in the Startup Disk preferences pane on client computers.

   Optional: In the Description field, enter notes or other information that helps you characterize the image.

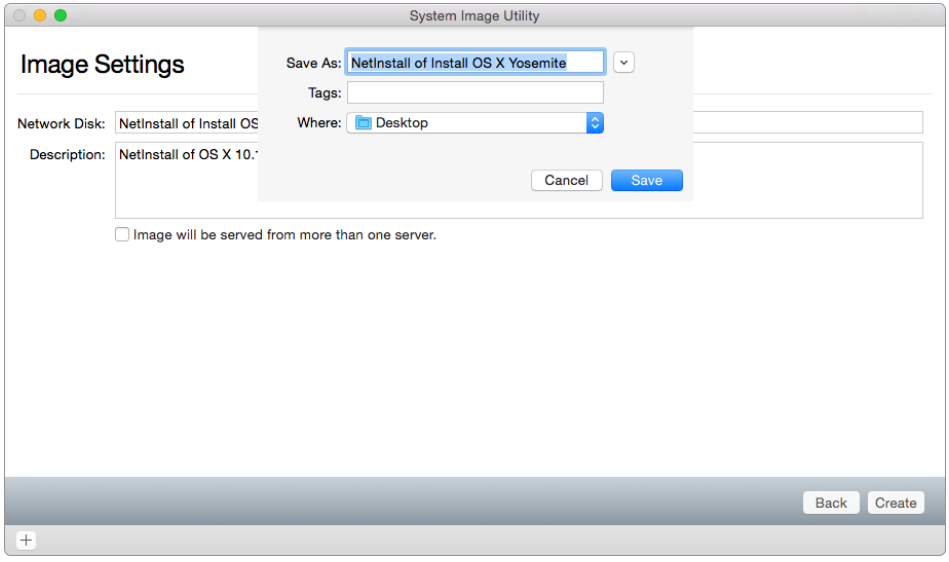
   Users of client computers can't see the description information.

8. 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 Licensing 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.

You may see 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. If you do see this pop-up menu and you're creating the image on the same server that will serve it, choose a volume from the pop-up menu.

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

12. Click Save.
13. Enter an administrative password for the computer that's generating the image and click OK.

    Important: Don't attempt to edit content in the image destination folder while the image is being created.
14. When the process is complete, click Done.

Creating a NetRestore image with System Image Utility

This section explains how to use System Image Utility to create a NetRestore image on a volume that was prepared with all of the OS X Yosemite settings and applications (called the *prepared volume*). In this example, the prepared volume is called *client*.

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

A NetRestore image restores a volume over a network from an Apple Software Restore disk image. You can restore an image to a volume in two ways with Apple Software Restore:

- You can restore an image file by file.
- You can use block copy.

You can create system images,and automations for those images, from a NetRestore image. As with NetBoot and NetInstall, use System Image Utility to create and share an image over your network.

To create a NetRestore image with System Image Utility:

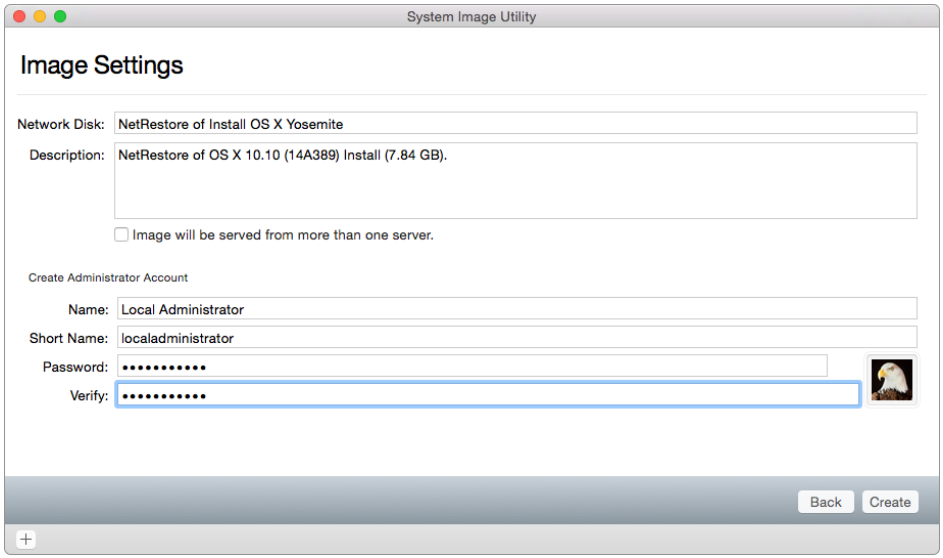
1. Download—but don't install—OS X Yosemite from the Mac App Store. Don't restart your Mac during this step.

   The Install OS X Yosemite application will be copied to /Applications/.
2. If the OS X Yosemite Installer opens, quit it.
3. Open System Image Utility. Go to System > Library > CoreServices > Applications.
4. From the Sources pop-up menu, choose Install OS X Yosemite.

   Select NetRestore Image.

5. Click Continue.

   The Image Settings pane appears.



6. In the Network Disk field, enter a name for your image.

   This name identifies the image in the Startup Disk preferences pane on client Mac computers.

   Optional: In the Description field, enter information that helps you characterize the image.

   Users of client computers can't see the description information.

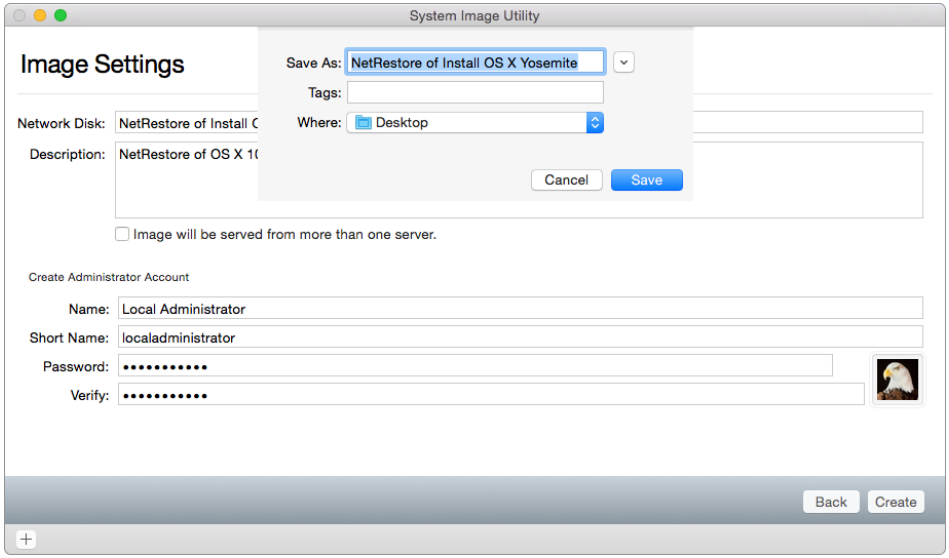
7. Enter the names and password that you'll use to create the administrator account on the system after it's restored:

   - **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.

8. Click Create.

9. Read the Software License Agreement and click Agree.

10. In the Save As dialog, choose where to save the image.



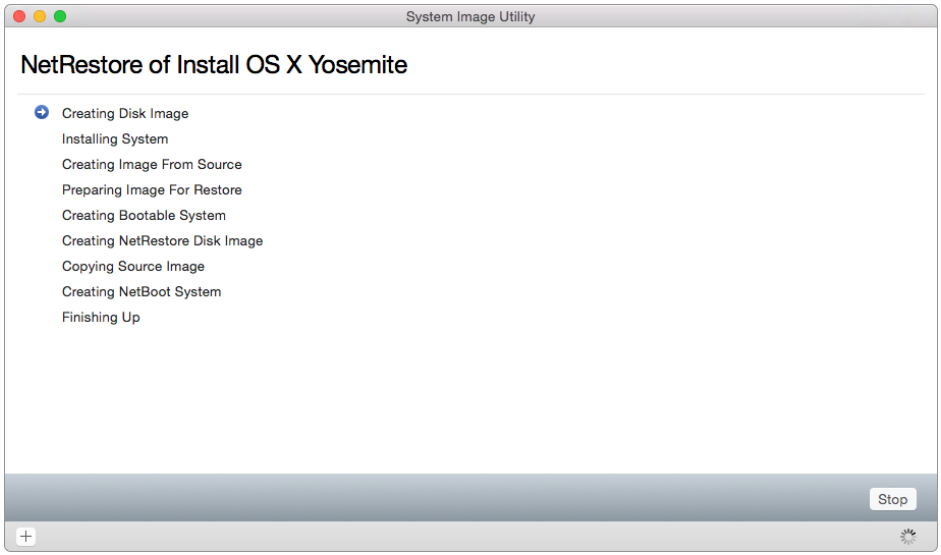
If you don't want to use the image name you entered earlier, enter a new name in the Save As field.

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 disclosure triangle next to the Save As field and navigate to a folder.

11. Click Save.
12. Enter an administrative password for the computer that's generating the image.
13. Click Create.

You see the NetRestore of *your image name* process completion.



14. When the process finishes, click Done.

NetRestore images from a configured computer

Use NetRestore images when you must use the same software on multiple Mac computers. For example, if the Mac computers in your organization must have identical software and configurations, you can create a NetRestore image that you can deploy whenever you must restore them to a "clean" state.

NetRestore creates system images and automations for those images. It deploys them using Apple Software Restore in block-copy format. 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 may include apps, settings, and tools. Because the image is populated, you must create an image from a volume that is prepared or installed with the apps, settings, and tools.

When you use NetRestore from a configured computer, you'll probably need to create an image from a volume that you prepared or installed. Next, you'll probably want to build a directory service. After you create an image, you can automate tasks within System Image Utility by creating workflows with the Automator Library.

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

1. Start the Mac with the prepared volume in two ways:

   - Start it up and immediately hold down the T key until you see the FireWire or Thunderbolt icon.

     Or

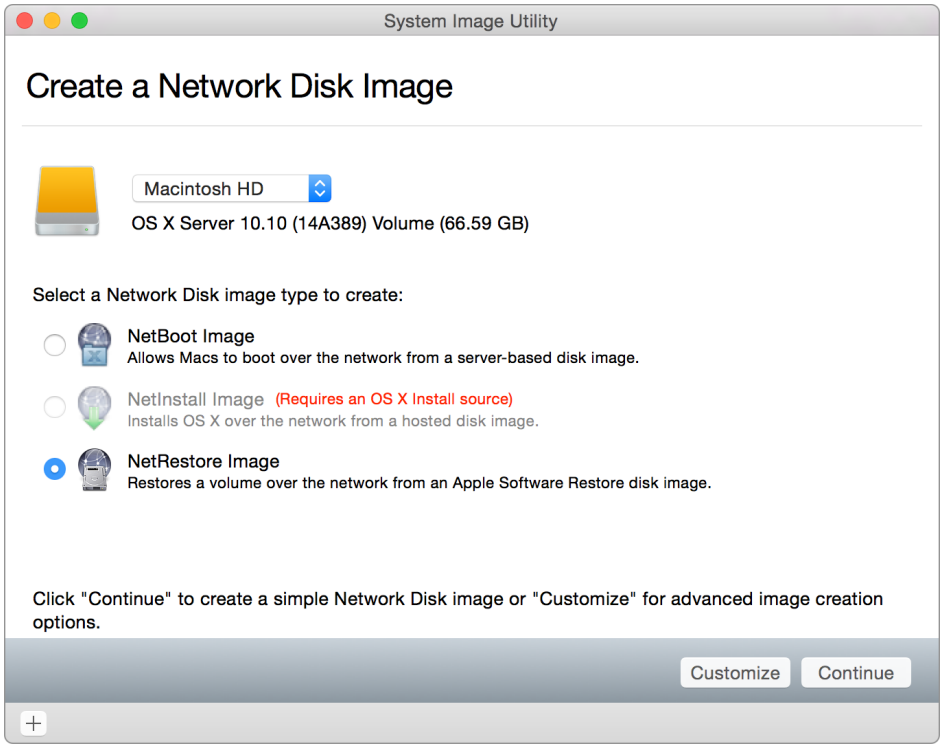
   - If the target computer is running OS X Yosemite, open System Preferences, choose Startup Disk, click Target Disk Mode, and go to step 3.

2. Restart the computer.

   It starts up in Target Disk Mode.

3. Connect the Mac with the prepared volume to the Mac with OS X Yosemite installed with a FireWire or Thunderbolt cable.

4. Go to System > Library > CoreServices > Applications and open System Image Utility.

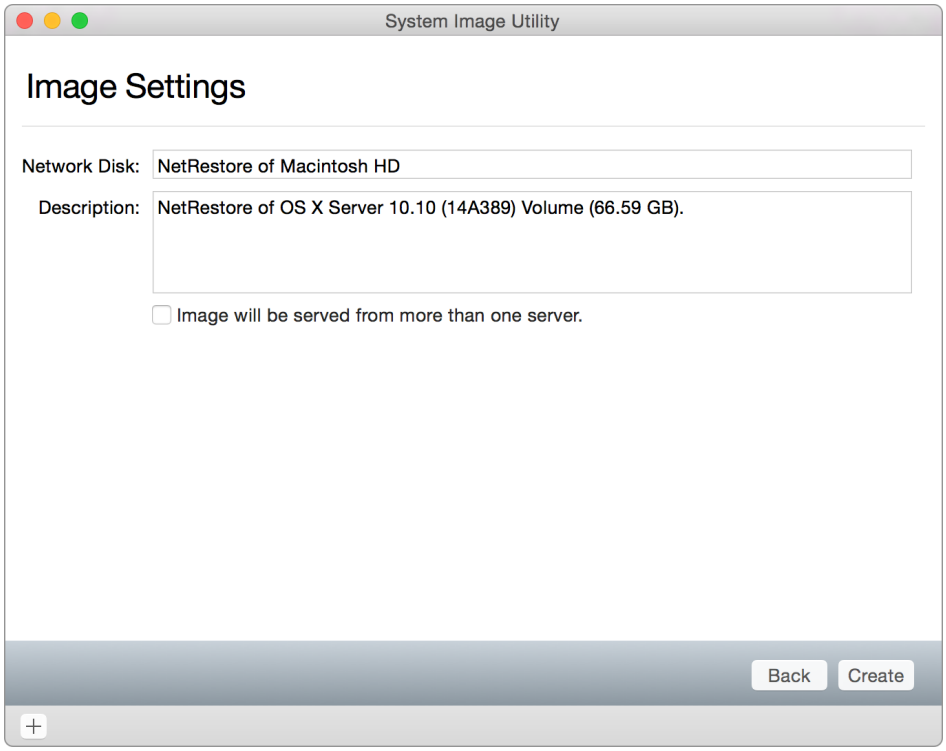


5. From the Sources pop-up menu, choose the volume that you want to use as your source for the NetRestore image.

6. Select NetRestore Image.

7. Click Continue.

   The Image Settings pane appears.



8. In the Network Disk field, enter a name for your image.

   This name identifies the image in the Startup Disk preferences pane on client Mac computers.

   Optional: In the Description field, enter notes that help you characterize the image.

   Users of client computers can't see the description information.

   If the image will be served from more than one server, select the checkbox labeled "Image will be served from more that one server."

   This assigns an index ID to the image for NetInstall service load balancing.

9. Click Create.

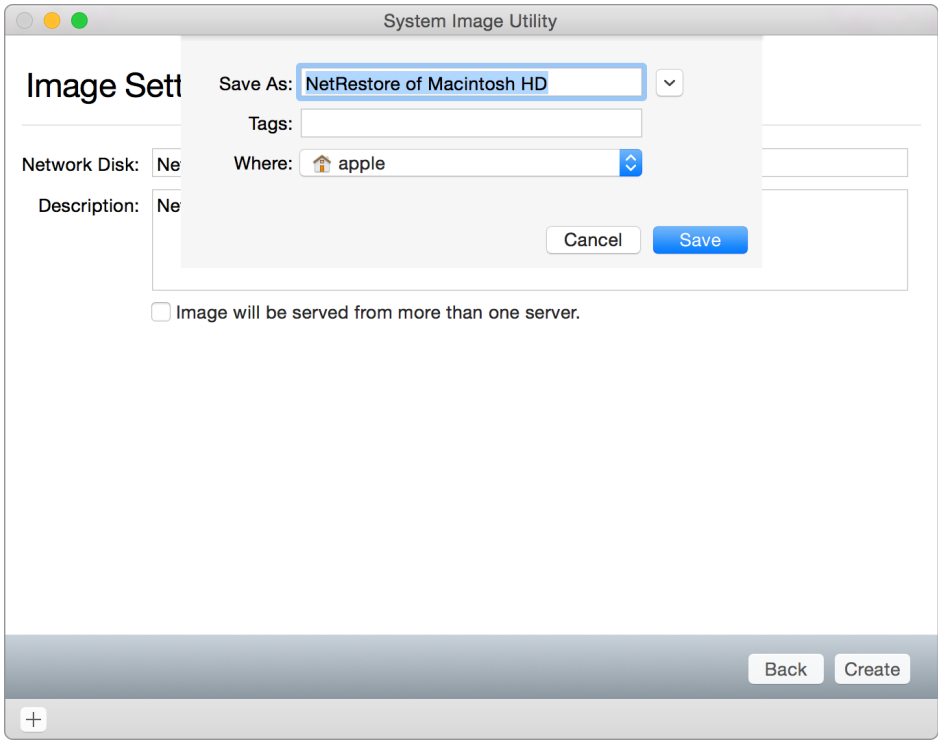
10. Read the Software License Agreement and click Agree.

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 disclosure triangle next to the Save As field and navigate to a folder.



12. Click Save.
13. Enter an administrative password for the host you're using to generate the image.
14. Click OK.

    Important: Don't attempt to edit content in the image destination folder while the image is being created.
15. When the process is complete, click Done.

Automating tasks with System Image Utility

You may need to perform additional tasks or automations after you build an initial image or while it's being installed. For example, you may want to repartition a drive before you install it, or repair it after you install it. Use Workflows for these tasks.

Use image workflows to create OS X NetBoot, NetInstall, and NetRestore images. With Workflows, you can define your image contents.

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, workflow actions must be connected. If not, the workflow is invalid and the actions aren't 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.

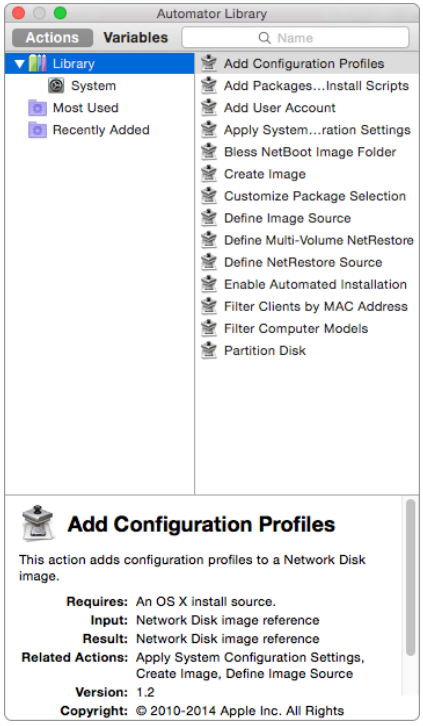
You can save your assembled workflows to reuse later.

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

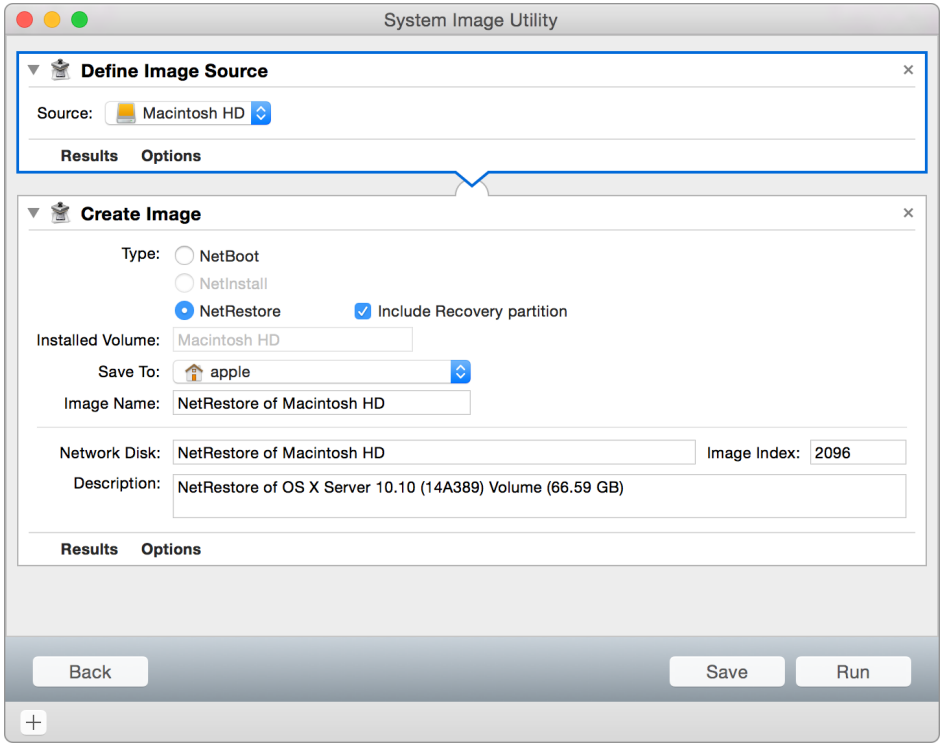
1. Open System Image Utility. Go to System > Library > CoreServices > Applications.
2. Choose an image source from the Sources pop-up menu.
3. Choose the image type you want to create (NetInstall, NetBoot, or NetRestore).

   Your image type selection may vary depending on the image source you selected.
4. Click Customize for advanced image creation options.

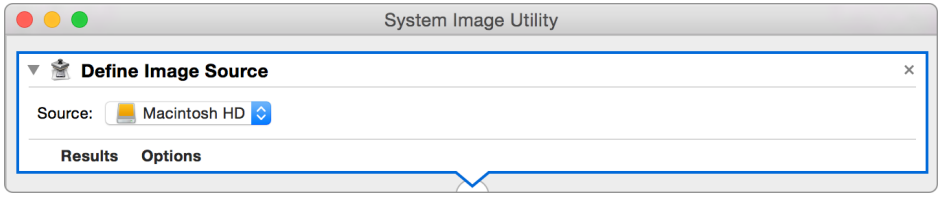
   This opens the workflow pane and Automator Library.



The Define Image Source action is the first component in the workflow and is required.



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



6. From the 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 and below it. If it doesn't, the workflow will fail. Put the actions in the order you want. Configure each action as you proceed.

   Put any actions that configure the network disk image between the Define Image Source action and the Create Image action.

7. 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.
8. Select the Include Recovery Partition checkbox to include the OS X recovery partition in your image.
9. If you're creating a NetBoot or NetRestore image, enter a name in the Installed Volume field.

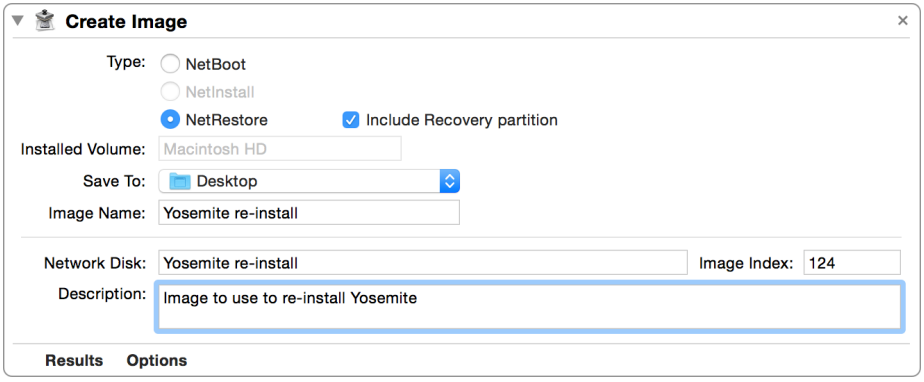
   The volume that your image is installed on will be renamed with this name.

   This option is available only with NetRestore images.
10. From the Save To pop-up menu, choose where to save the image.
11. In the Image Name field, enter the name of the image file.
12. 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.

    Optional: In the Description field, enter notes that help you characterize the image.

    Users of client computers can't see the description information.
13. In the Image Index field, enter an Image ID number:
    - 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 Startup Disk preferences pane.



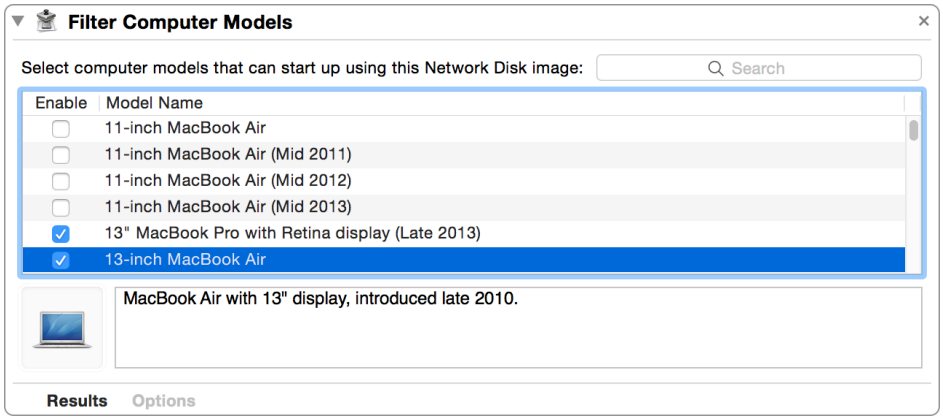
14. Click Save. Then enter the name of your workflow in the Save As field. Choose where to save the workflow by choosing a location from the Where pop-up menu or by clicking the disclosure triangle next to the Save As field and navigating to a folder.
15. Click Save.
16. To start the workflow, click Run. Then authenticate if prompted.

    Important: Don't attempt to edit content in the image destination folder while the image is being created.

To restrict which computer models can start up using a network disk image:

The Filter Computer Models action limits which Mac computers can start up using a network disk image. If your image contains software that has specific hardware requirements, you can restrict the image to Mac computers 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.

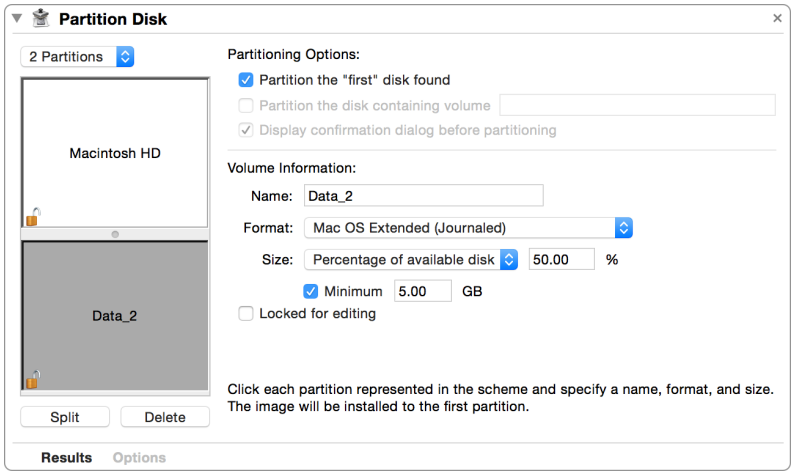


In this example, only Mac computers with13-inch displays are enabled.

To set up a workflow item that partitions the target disk:

With the Partition Disk action, you can partition a computer drive before the image software is installed. For example, you can 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 "Partition the disk containing volume" to limit which disks are repartitioned.

   This feature helps you avoid overwriting external drives, jump drives, or computers that aren't ready to be imaged. **Or**, select "Display confirmation dialog before partitioning" to avoid erasing user data.

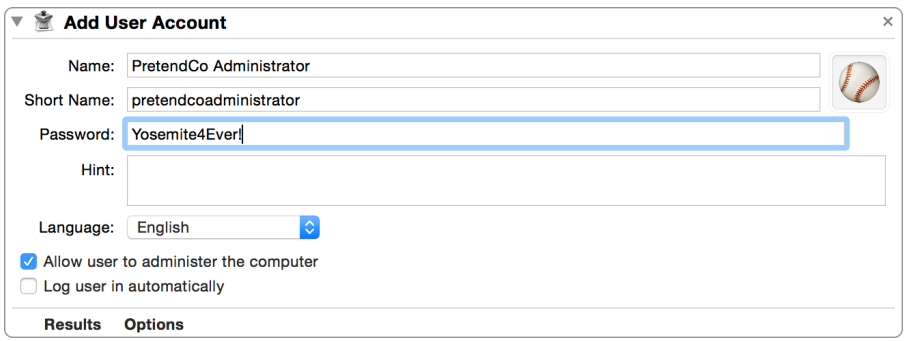
   Important: Selecting "Display confirmation dialog before partitioning" or "Partition the disk containing volume" can stop the imaging process. This may be an issue if you're trying to install hundreds or thousands of Mac computers.
4. Choose the format for the drives. In most cases, the default setting—Mac OS Extended (Journaled)—is fine.
5. Choose the minimum size for each partition. Do this so the tool doesn't try to image 40GB of data to a 10GB drive and partition a chunk away for other tasks.

   Note: It's better if the imaging process fails early, because it keeps troubleshooting imaging issues to a minimum, allowing you to move on to imaging the next host.

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

By default, an OS X Mac has one user account (the primary administrator account). You may want to create an additional standard account so users can use the Mac 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. With the Add User Account action, you can add accounts as part of the image.

1. From the Automator Library, drag the Add User Account action into the workflow.



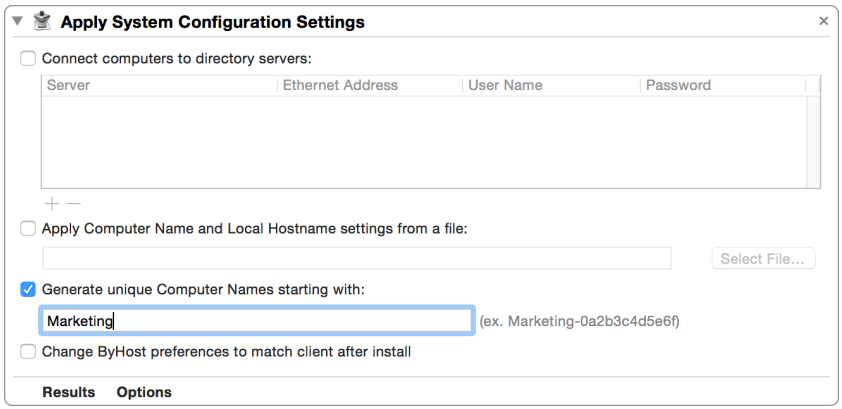
2. Provide the following:
   - Name: Enter your user name.
   - Short name: This will be populated automatically, but you can edit the short name.
   - Password: Enter a password for this account.
   - **Optional:** Hint: Enter a clue that helps you remember your password.
   - Select the checkbox labeled "Allow user to administer the computer."

3. To create multiple accounts, drag a new Add User Account action into the workflow and repeat step 2.

To set up a workflow item that sets the computer name:

Whether a computer comes with OS X, Microsoft Windows, or Linux, it must have a unique name within a network. Use the Apply System Configuration Settings action to rename a computer after it has been imaged.

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



2. Select the checkbox labeled "Generate unique Computer Names starting with," 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

Get the information from a file by selecting the checkbox labeled "Apply Computer Name and Local Hostname settings from a file."

If the computer running System Image Utility is bound to a directory service like Open Directory, Active Directory, or eDirectory, select the checkbox labeled "Connect computers to directory servers." This feature adds the imaged system to the directory service as a post-installation task.

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

For prepared images, select the checkbox labeled "Change ByHost preferences to match client after install."

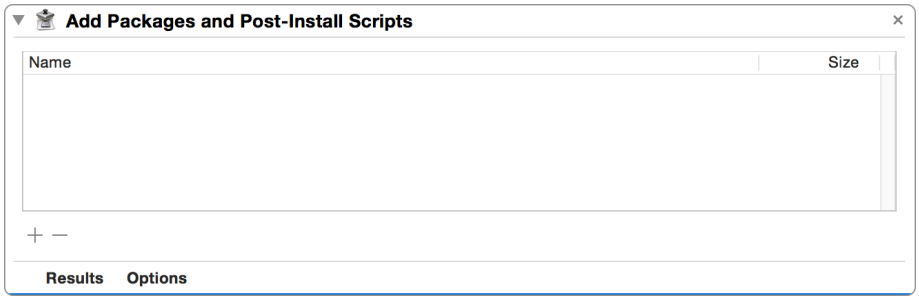
To add software packages to a System Image Utility workflow:

Use the Add Packages action within the Automator Library to install software packages such as software updates that you download from the Apple Support website.

If you know how to create your own packages and use shell scripting to automate tasks, you'll appreciate how the Add Packages action helps you further automate your installation process.

Note: Software installers that you add to System Image Utility must be in the 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.

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 a Mac for settings and services.

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 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. Enter the name of the target volume in the "Install to the volume" field.
3. To erase the target volume before the image is installed, select the "Erase before installing" checkbox.

   Warning: Selecting "Erase before installing" erases 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 you create system images, you may be tempted to take a clean Mac, install a fresh copy of OS X and all the apps that users might need, and then create a "monolithic" NetRestore image of that Mac. Doing so would create images that are difficult to maintain, because you must completely rebuild the image each time the OS or an app is updated.

Instead, create minimal images. With the Mac App Store and the Volume Purchase Program (available in some regions), you can create images that contain just the OS, and users can download just the apps they need. This approach saves you time, because you don't have to repeatedly install software. It also saves money for your organization, which won't have to buy as many apps.

Sometimes the software you need isn't available from the App Store. Or you may be creating images for computers that are refreshed frequently and aren't dedicated to a single user—for example, classroom or lab computers. In situations like these, you can create a customized workflow that makes a NetRestore image using the OS X Installer as the source, and add software with 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 must create installer packages to add software to an image workflow, consider these third-party products:

- Composer, from JAMF software: 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: With InstallEase, a simple snapshot-based package generation tool for OS X, you can create installer packages with minimal effort.
- Iceberg and Packages: Iceberg and Packages (under the BSD license) provide interface options for the implementation of preflight and postflight scripts and features you can use for metapackage management.

Additional resources

- *Supporting Mac Users: The Self-Support Model*
- *Imaging the MacBook Air: Leveraging Thunderbolt*
- Leveraging NetInstall, *OS X Server Essentials 10.10: Using and Supporting OS X Server on Yosemite*, Peachpit Press

Deploying Images

2

After you generate images and customize the automations that go into them, you deploy them. The simplest way do this is with USB or FireWire. But this method doesn't scale well, so it isn't suitable for large deployments. You can use USB or FireWire in preparing your image for large deployments.

In this chapter, you'll learn about local and large-scale deployment techniques. The chapter also introduces some third-party deployment solutions.

Deploying local images

Local image deployment is the simplest way to deploy images to Mac computers. You can use Apple Software Restore, Disk Utility, target disk mode, and direct connections between your Mac computers to help you test deployment images. This way, you don't have to move your images to production or test servers.

Creating a bootable installer volume

With OS X Yosemite, you can create a bootable OS X installer, which you can use to install OS X from removable media.

To create a bootable OS X installer:

1. Download the Install OS X Yosemite app from the App Store.
2. Mount the volume that you want 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 (a program within the Install OS X Yosemite app) to convert the volume from step 2 into a bootable installer based on the Install OS X Yosemite app from step 1.

   Note: Use the createinstallmedia tool only with the Install OS X Yosemite app version that it came with.

   Enter the following at the Terminal prompt. You may need to adjust the path to the Install OS X Yosemite app.

   /Applications/Install\ OS\ X\ Yosemite.app/Contents/Resources/createinstallmedia

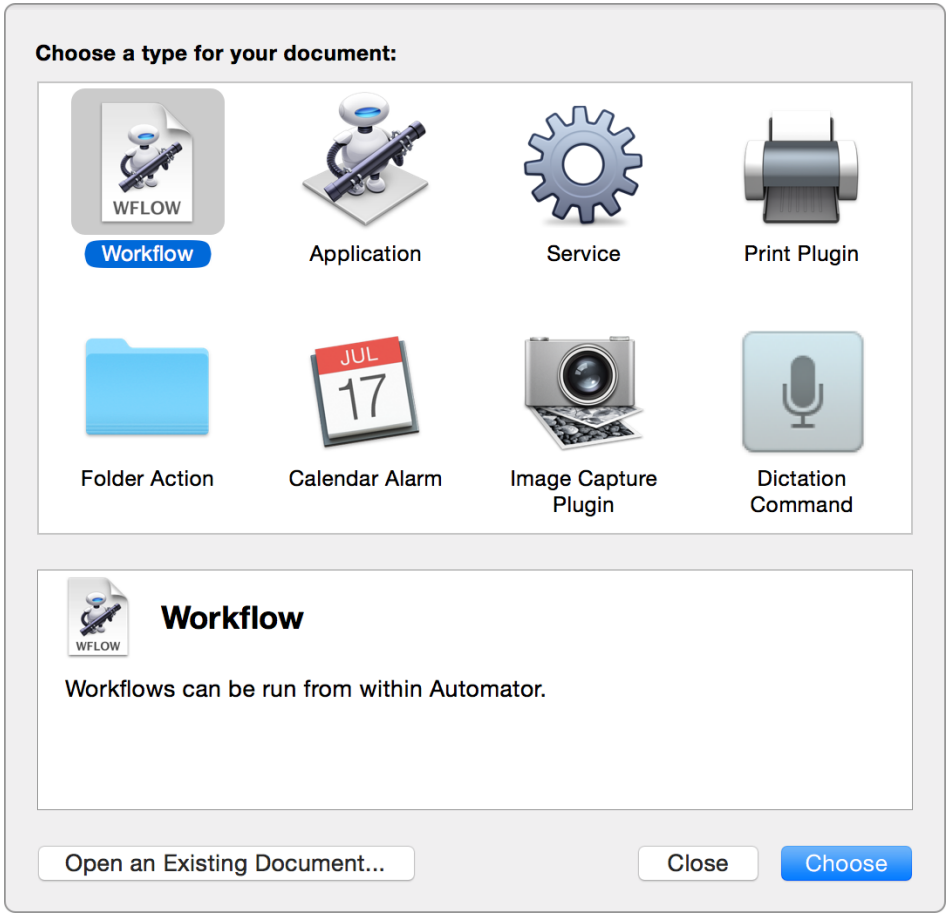
Using a network disk image to create a bootable disk or volume

If the Ethernet connection on the Mac computers is slow, use your NetInstall environment and USB, FireWire, or Thunderbolt volumes to push images.

This section explains how to use NetInstall to create a bootable drive that automatically installs a client system. Because most images now have more than 6GB of data, use a drive that's at least 8GB.

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

1. Copy a NetInstall image (.nbi folder) to the root of an external drive.
2. Open Automator from /Applications/.
3. Create a new document.

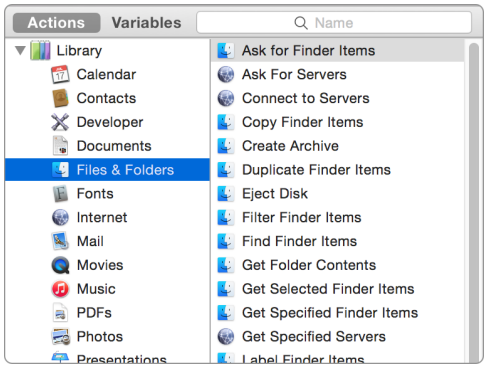


4. In the "Choose a type for your document" pane, select Workflow and click Choose.

   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 a customized workflow. You can also use the Bless NetInstall Image action when you create a customized workflow. If you select System from the left column, you'll see the actions for creating the network disk image in System Image Utility.

5. Specify the .nbi folder that you want to make bootable.

6. In the first Actions column, select "Files & Folders".



7. Drag the Get Specified Finder Items action from the second column to the Automator workflow area.

8. In the Get Specified Finder Items action, click Add.

9. Navigate to and select the .nbi folder that you copied to the external volume in step 1.

10. Click Add.

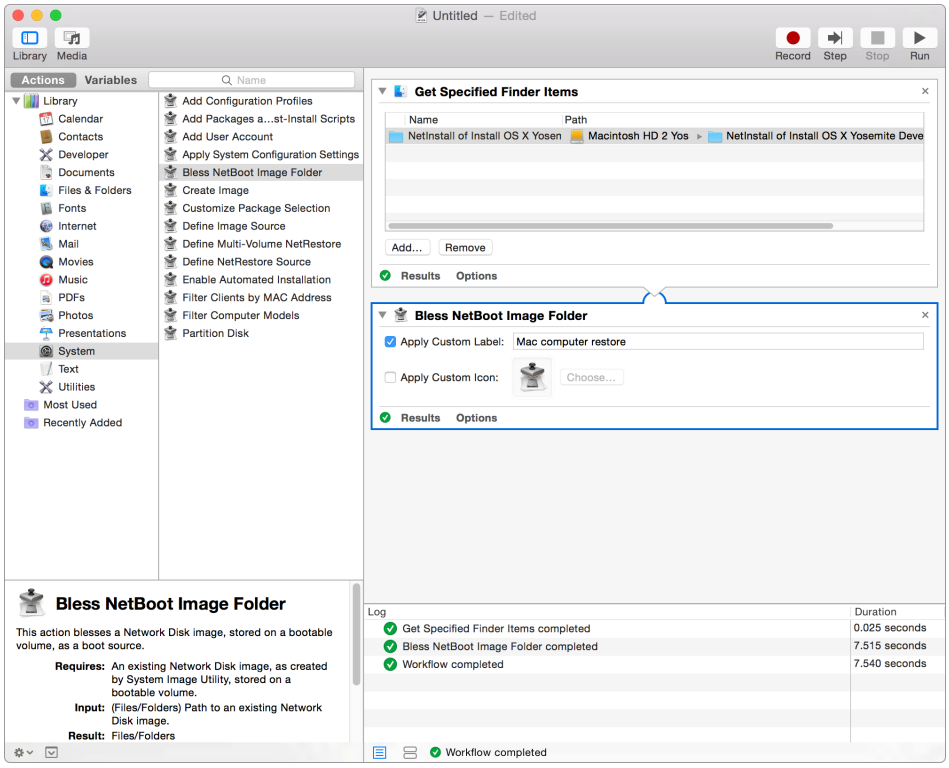
11. Bless the .nbi folder so it's bootable.

12. In the Actions column, select System.

13. Drag the Bless NetBoot Image Folder action from the second column to below the Get Specified Finder Items action in the Automator workflow area.

14. Select the Apply Custom Label checkbox, and enter a label that will appear in the list of bootable volumes.

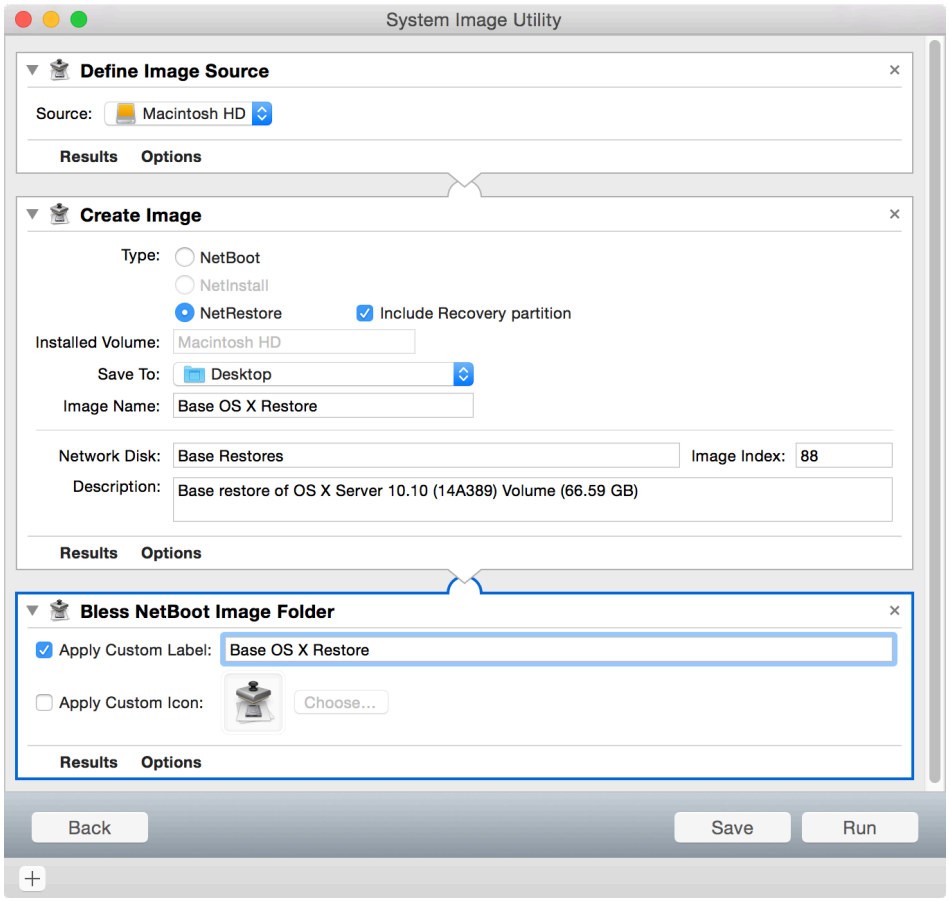
15. Click the Run button in the top-right corner.



It should take a few seconds for the workflow to run. The log beneath the workflow displays the results.

To create a bootable disk or volume with System Image Utility:

1. If you create a customized image in System Image Utility, add the Bless NetBoot Image Folder action to the end of the workflow.
2. Specify the external drive in the Save To pop-up menu in the Create Image action.



To start up a computer with a volume that contains a network disk image:

1. Turn on or restart your Mac.
2. Immediately hold down 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 images with NetInstall

Use NetBoot, NetInstall, and NetRestore to manage the operating system and apps that your Mac clients (or even other servers) require to start and do their work. Instead of going from one computer to another to install the operating system and apps from CDs, you can prepare an installation image that installs on each computer when it starts up. You can also have clients start up (or boot) from an image stored on a server. In some cases, clients don't even need their own hard disks.

With NetBoot and NetInstall, your clients can start from a standardized Mac OS X configuration suited to specific tasks. Because the clients 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 that serve the needs of client groups, 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.

Mac computers with OS X Yosemite can use NetBoot to start from an OS X Yosemite network disk image. For a list of Mac computers that work with OS X Yosemite, visit:

http://support.apple.com/en-us/HT201475

You must install the latest firmware on all client Mac computers. Firmware updates are available from the Apple Support website.

NetInstall is supported only over physical Ethernet connections. Apple doesn't support —and discourages—using Wi-Fi to boot clients with a network disk image.

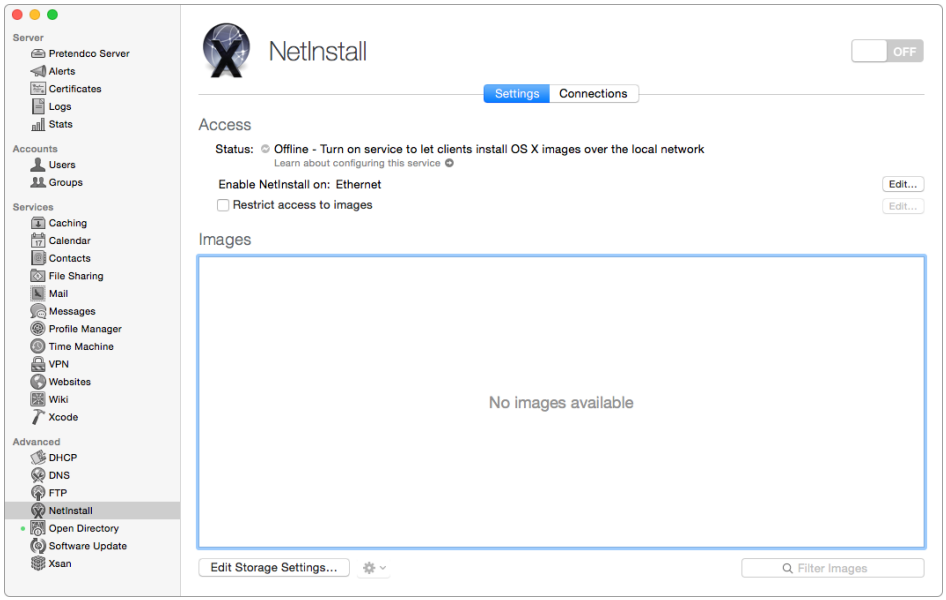
Configuring a NetInstall server

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

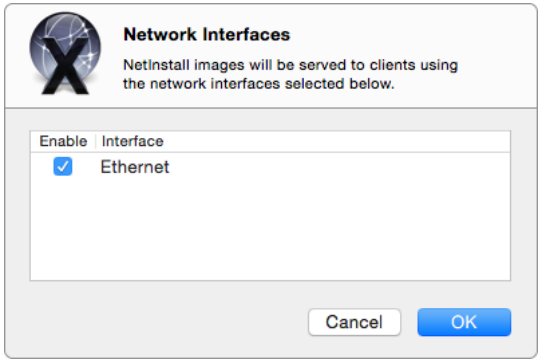
This section explains how to configure an OS X server to act as a NetInstall server. The instructions assume you already installed and are running OS X Server on an OS X Yosemite computer. For information about installing and configuring OS X Server, see the *OS X Server Essentials 10.10* book from Peachpit Press, or refer to Server Help.

To configure a NetInstall server:

1. Open Server app from /Applications/.
2. Select NetInstall in the sidebar. Then click Settings.

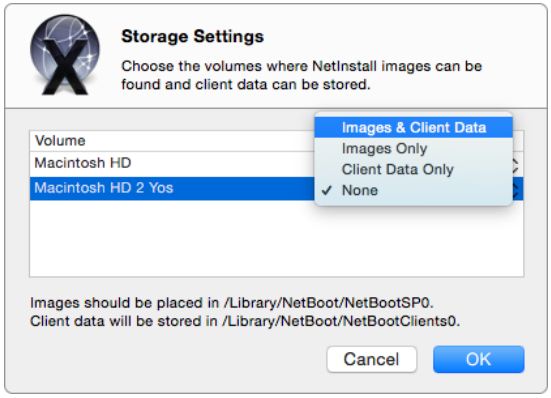


3. Click the Edit button to the right of "Enable NetInstall on."

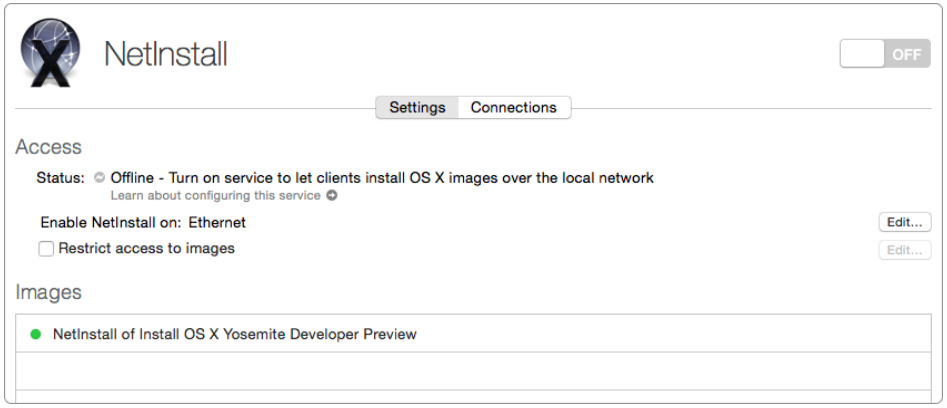


4. Make sure that at least one network port is selected.
5. Click OK.
6. Click Edit Storage Settings.

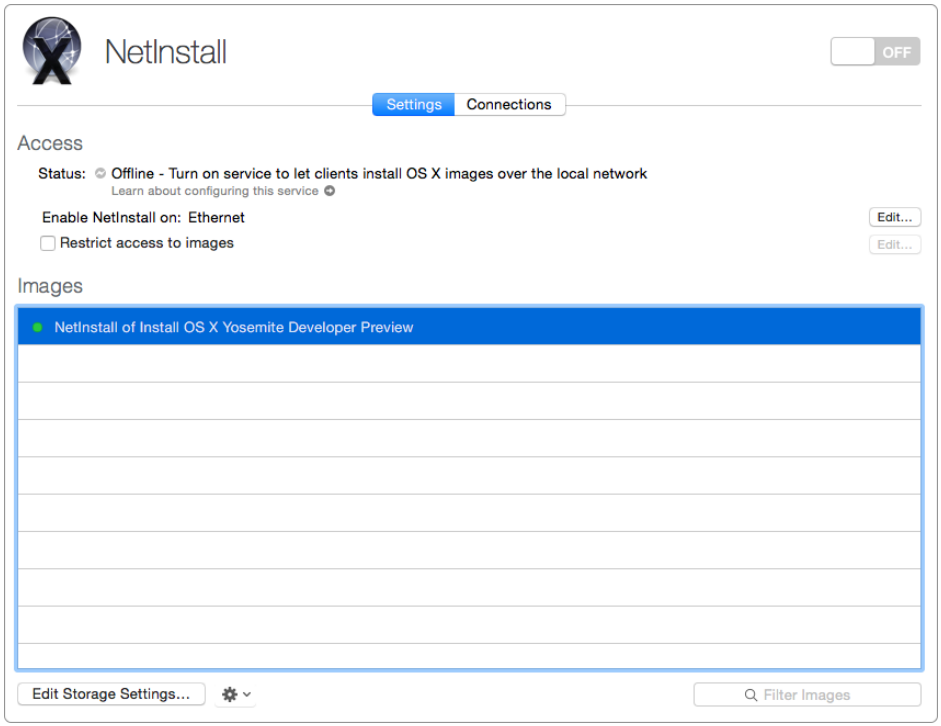
7. In the entry for the volume that you want to store the NetInstall images and client data on, choose “Images & Client Data” from the pop-up menu.



8. Click OK.
9. Put the network disk images you created earlier in the exercise in the /Library/NetBoot/NetBootSP0 directory of the volume you just selected.
10. In Server app, press Command-R to refresh the window.

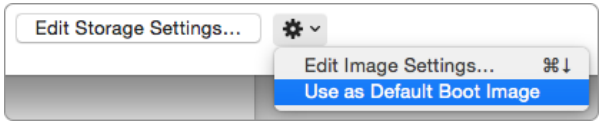


The Images list shows the network disk image name that you copied to NetBootSP0.



11. Select the image that you want to use.
12. From the Action pop-up menu, choose Edit Image Settings.

    This is the default setting.
13. Select the "Make available over" checkbox.
14. Choose the protocol that you want to use to make the image available.
15. Click OK.
16. If this is your first image, you may want to set it as the default. If so, select the image and choose "Use as Default Boot Image" from the Action pop-up menu.



17. Click the on/off switch for the NetInstall service to turn it on.
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.

Starting up Mac computers from NetInstall disk images

After you create a network disk image and enable it on a NetInstall server, you can boot client Mac computers from the image in two ways:

- Boot from a default network disk image
- Boot from a specific network disk image

To boot using the default network disk image:

Use the N key to boot any supported client computer from a NetInstall disk image. When you use the N key, the client Mac uses the Boot Service Discovery Protocol (BSDP) to locate a NetInstall server and boots from the server 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 Mac remembers which 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 down Option-N during startup causes the Mac to boot using the current default image.

To start up using a specific network disk image:

If your NetInstall server is hosting multiple images or you 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

   Type the path to the image in the provided field.

   The field will appear if you selected that option when you created the NetBoot set.

Third-party deployment solutions

Here's a partial list of third-party solutions for OS X deployment:

- DeployStudio
- JAMF's Casper Suite
- Absolute Manage
- KACElivepage.apple.com
- LANDESK
- FileWave

Additional resources

- "Manage updates and installation: Install OS X over the network" section, *OS X Server: Advanced Administration*
- *OS X Education Deployment Guide*
- *OS X Server Essentials 10.10: Using and Supporting OS X Server on Yosemite*, Peachpit Press

Managing Mac Computers with Apple Remote Desktop

3

Apple Remote Desktop is an open standards–based desktop management software utility for your networked Mac computers. You 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 get Apple Remote Desktop from the Mac App Store.

You can remotely manage client computers individually, but most 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 Remote Desktop computer lists. A computer list is a group of computers that you want to administer similarly. Scan your network or import the identity of computers from files to create a computer list.

You can group and organize computers for administration. You can group them 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 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.

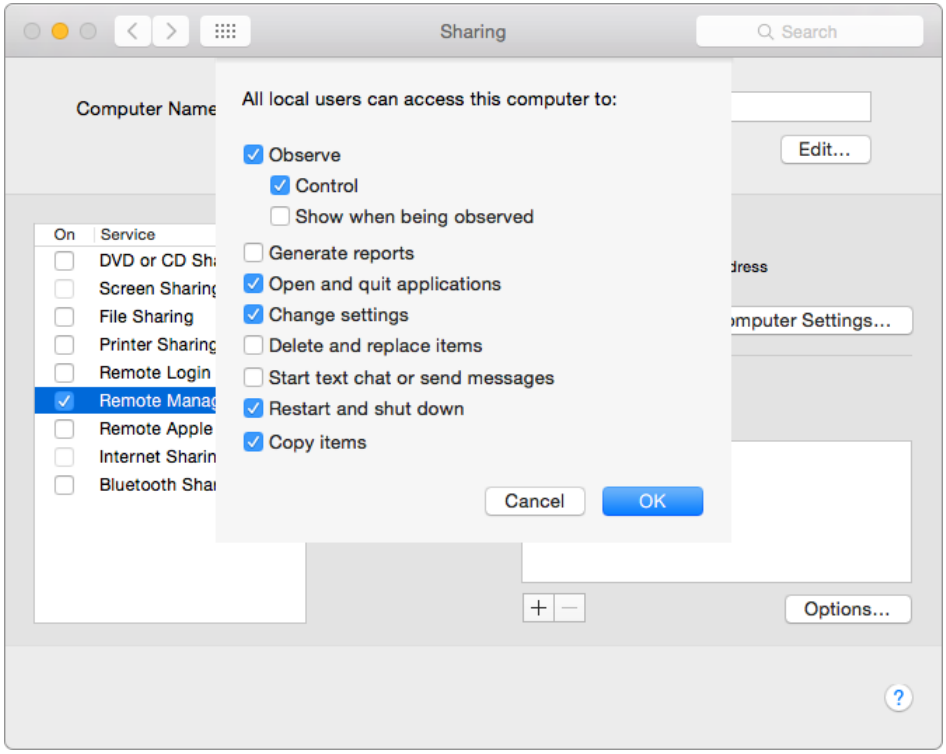
Enabling remote management

The Remote Desktop client software is built into OS X. The administrator app (also called Apple Remote Desktop) is available from the Mac App Store.

Client computers can set local system preferences that restrict remote access to specific users and actions. Remote management must be enabled on client computers. 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).

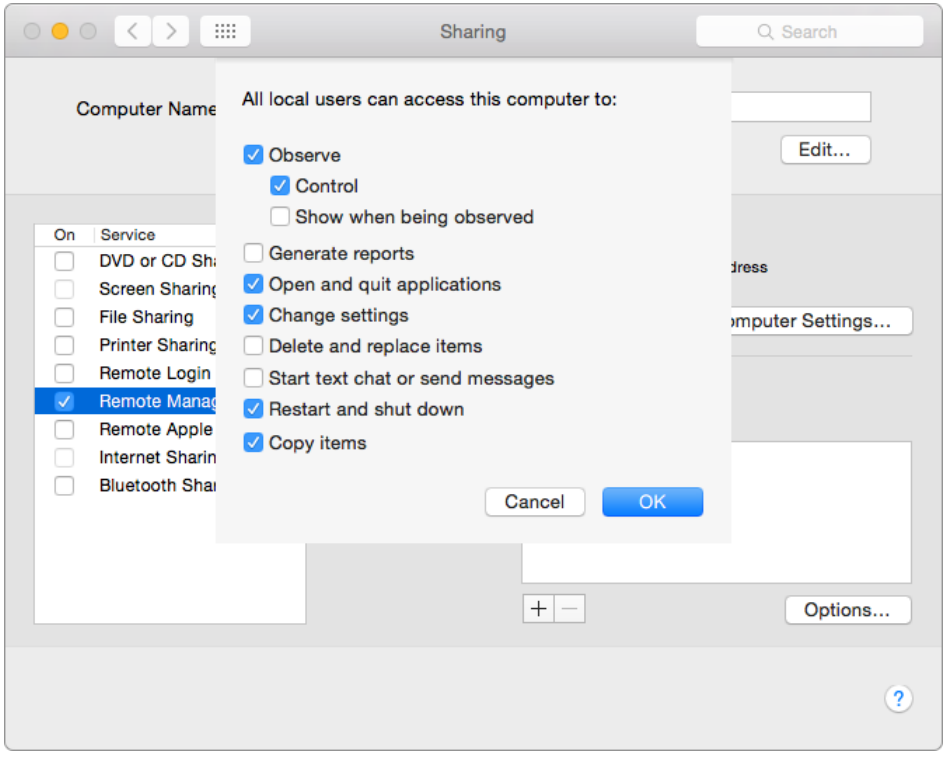
To turn on remote management on a client computer:

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 Remote Desktop.
   - Select "Only these users"; then click Add (+), and select the users with whom you want to share your computer using Remote Desktop.
4. To change which capabilities users have when accessing your computer, click Options.



Here are the Sharing pane Remote Management options 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 select Change settings.)

- **Observe: Control** Use these Interact menu commands: Control, Share Screen, Lock Screen, and Unlock Screen. You must enable this checkbox if you want 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. You must enable this checkbox 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. You must enable this checkbox 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. You must enable this checkbox to use the Upgrade Client Software and Change Client Settings features.

To automatically select all access checkboxes, hold down the Option key and select 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

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

Remote Desktop displays computers in lists in the main section of the Remote Desktop window. The default computer list, called All Computers, lists potential clients that you've located and authenticated. You can create other lists to group Mac computers in your network in any way you wish.

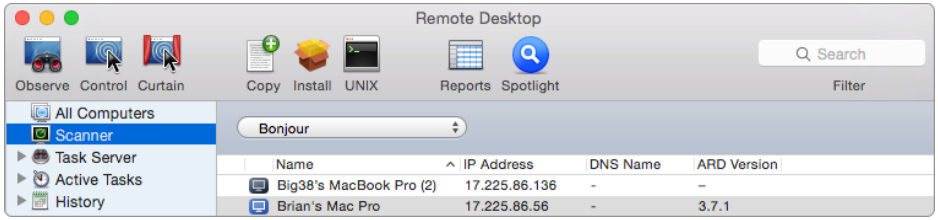
Computer lists have the following capabilities:

- You can create as many lists as you want.
- A computer can appear on more than one list.
- You can create list types (for example, geographical, functional, hardware, or configuration).
- If you click a list name and hold the pointer over it, you can edit the list name.
- If you double-click the list icon, you open another window containing the computers in the list.

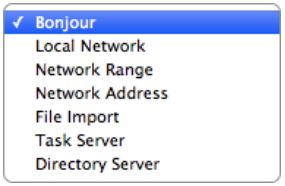
To add computers to the All Computers list with Remote Desktop:

1. Open Remote Desktop from /Applications/.

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



3. Search for systems and add them to the All Computers list and a list you create.



The scanner searches with the following options:

- **Bonjour** 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 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, enter a beginning and ending IP address to scan, and 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 it 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 computer 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).

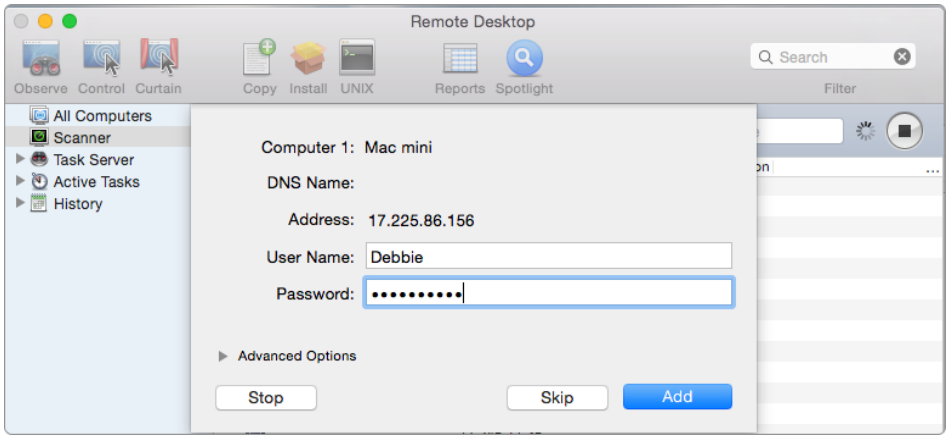
With File Import, you can also add ranges of IP addresses by expressing the range in the following format:

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.

4. 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.
5. Drag the computers to the All Computers list.
6. Authenticate by providing a user name and password for a Remote Desktop administrator account on the computer being added.



7. 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.
3. Choose File > New List From Selection.
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 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

Use Remote Desktop to install software and software updates on one or more client Mac computers without user interaction or interruption. Your users don't need to be logged in. The only computer you use is yours.

When you deploy apps, consider which apps:

- Are already on systems in the environment, and what conflicts may occur due to your deployment.
- Can run (whether or not they're on a Mac).
- Require that you deploy custom packages that don't prompt you to enter serial numbers or other user information.

Use Remote Desktop to view apps that are running on Mac computers in your network. You can run a report that lists apps and their versions.

To see a list of apps and their versions with Remote Desktop:

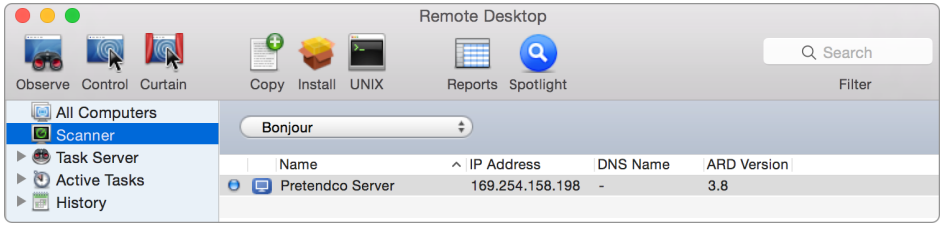
1. Open Remote Desktop.
2. Select the Mac computers that you want to review.
3. Choose Software Version from the Report menu.

Installing software with installer packages

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

To deploy software with Remote Desktop:

1. Open Remote Desktop from /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 to 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.

Installing software by copying

You can use Remote Desktop to copy items (other than the system software) to one or more client computers.

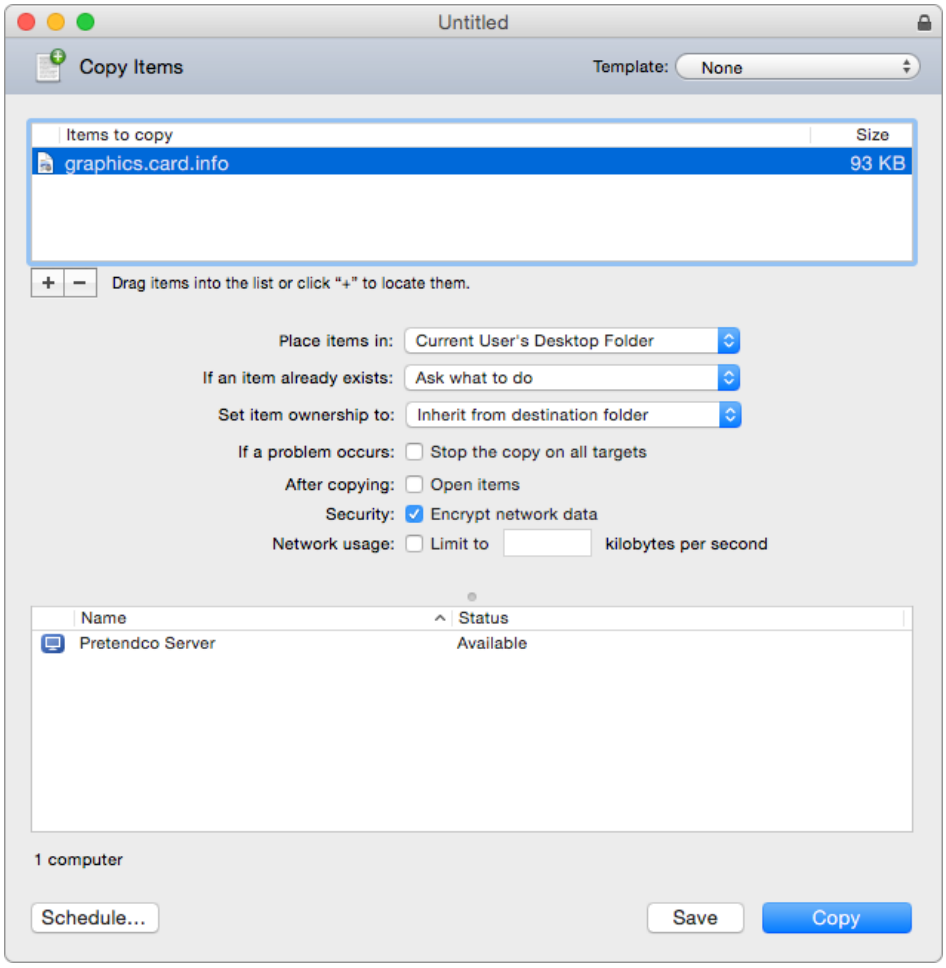
Copying files works fastest with a small number of files. For example, 10 files that are 10K each generally take longer than one 100K file. Consider copying a single file archive (like a .zip or .sit file) to remote computers for faster copying. Remember that OS X apps are bundles of smaller files. Although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

Creating reports

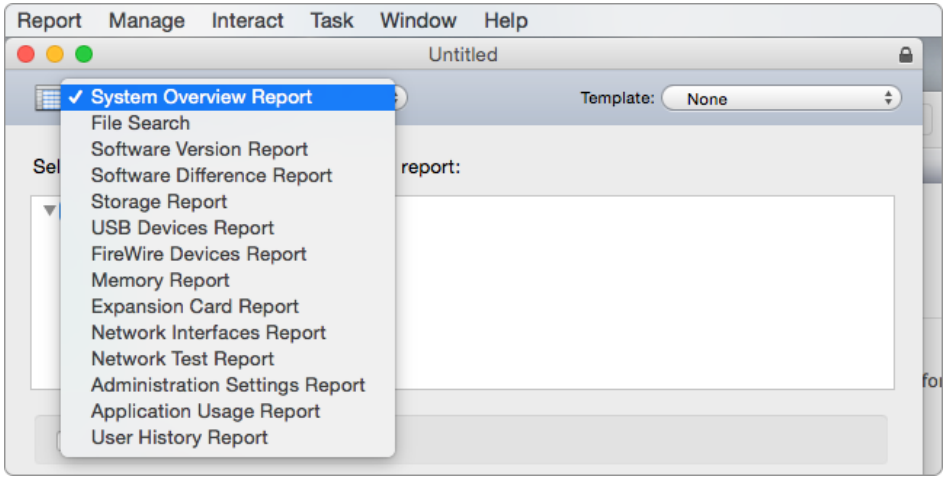
With Remote Desktop, you can capture data describing the attributes of client computers in the Remote Desktop database, then generate reports based on the data.

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. Remote Desktop stores data in its built-in Structured Query Language (SQL) database so you can use it when you need it.

You can also specify where you want the database to reside. You can put the database 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 many predefined report types.



- Use the **System Overview Report** to view client computer characteristics. It shows you client Wi-Fi setup, computer and display characteristics, devices, network settings, system preferences, printer lists, and key software attributes. Use this report to identify problems or to verify system configurations before you install software, or to determine which devices (such as scanners) are in a lab.
- 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.
- Use the **Software Version Report** to make sure that all users have the latest application versions appropriate for their systems.

- 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.
- Use the **Storage Report** to get information about the internal storage devices of client computers.
- Use the **USB Devices Report** to get information about USB devices that are connected to your client computers.
- Use the **FireWire Devices Report** to get information about client device speeds, software versions, manufacturer, model, and firmware version.
- Use the **Memory Report** to learn about installed memory on your client computers.
- Use the **Expansion Card Report** to get information about your client computer expansion cards.
- Use the **Network Interfaces Report** to get exhaustive information about your client computer network.
- 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 you troubleshoot 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 that you have a bad connection to the computers. Using this information can help you isolate the problem to a particular cable or hub.
- 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.
- Use the **Application Usage Report** to find out which applications are running on your client computers and who is running them.
- Use the **User History Report** to see who logged in to a client, how they logged in, and for how long they were logged in.

Generating customized reports

The Remote Desktop database is in standard SQL format, so you can use your favorite SQL scripts to query, sort, and analyze 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 that 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.

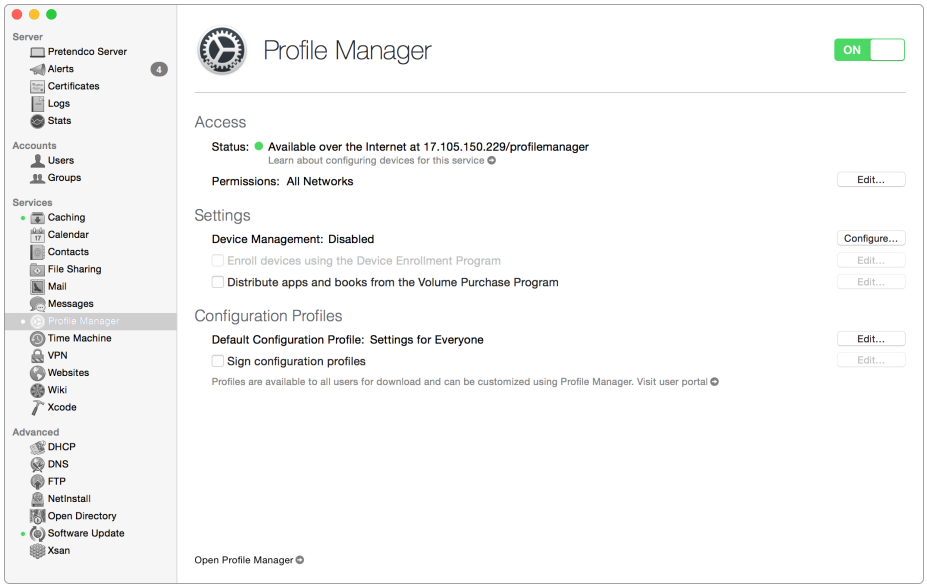
Additional resources

- *Remote Desktop Help*
- *Apple Remote Desktop*

Managing OS X Devices with Profile Manager

4

You can use Profile Manager, which is included in OS X Server. Use Profile Manager to configure and distribute settings to your OS X and iOS devices. Profile Manager helps you provide the settings, apps, and books that your organizational needs. With Profile Manager, you can specify how clients are configured, how to administer devices, and how to deliver the configurations to users and devices.



Before OS X Lion, managed preferences was the primary way to manage Mac computers. OS X Yosemite supports managed preferences, but you should use Profile Manager to create configuration profiles that support both OS X and iOS devices. Configuration profiles also provide more options (such as locking devices, performing remote wipes, and setting up 802.1X profiles).

Note: Some Profile Manager features are only available only with Mac computers that run OS X Mavericks v10.9 or later and iOS devices that run iOS 7 or later.

Profile Manager components

Profile Manager has three components: an administration web app, a Mobile Device Management (MDM) server, and the user portal.

- Use the Profile Manager **administration web app** to configure settings for devices, to manage enrolled devices and device groups, and to execute or monitor tasks on enrolled devices.
- Use Profile Manager as an **MDM server** to remotely manage enrolled OS X and iOS devices. After a device is enrolled with Profile Manager, you can update its configuration over the network without user interaction. You can also remotely lock or wipe a device.

  Note: Mobile Device Management is supported on Mac computers with OS X Mountain Lion v10.8 or later. To use all Profile Manager features, though, update all client computers to OS X Mavericks v10.9 or later.
- After you configure settings, you can use the Profile Manager **user portal** secure website to distribute them. Your users can access the portal to download and install your settings. They can also enroll their devices if you're using Profile Manager as an MDM server.

Configuration profiles

Configuration profiles are XML files that load settings and authorization information onto Mac 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 *only* be set by a configuration profile. You create configuration profiles using an MDM solution such as Profile Manager. Although this chapter focuses on Profile Manager, the management concepts covered apply to other MDM solutions.

Each configuration profile contains one or more payloads. A payload is a collection of settings in a configuration profile. VPN specifications are an example of a setting. Use payloads for Mac computers, iOS devices, or both.

You can create configuration profiles for users, devices, and 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. For example, you might create a configuration profile that sets up users' access to email but also enforces restrictions or passcode settings. To have access to messages, users must also accept your security policies.
- Provide updates to settings that are subject to change.

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

Users generally can't change settings in a configuration profile, except for passwords. Accounts configured by a profile can be removed only by deleting the profile.

Each user, device, and group has 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 user 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.

You can install two types of profiles on a Mac:

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

Payloads

The General settings payload is the only required payload in a configuration profile. It sets the name and identifier of the configuration profile. Use consistent naming conventions and clear descriptions with version numbers and dates to keep configuration profiles organized. Specify a unique identifier field for each configuration profile, because any subsequent profile created with the same identifier replaces the original one. A good profile description is especially important for signed and encrypted profiles, because they rely on the certificate keys of the tool that was used to create the profile.

Manual download versus automatic push for profiles

When you set up configuration profiles, you can choose between two distinct types: manual download or 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 web page 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, a

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.

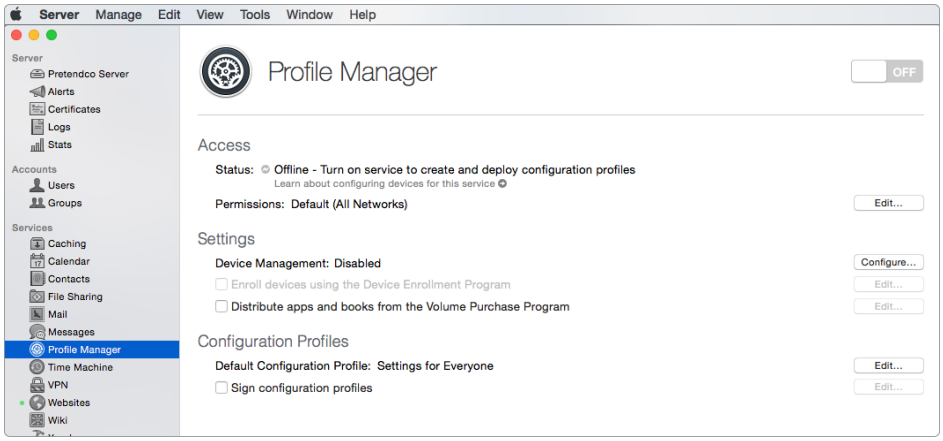
The push notification doesn't distribute the actual profile. It alerts the device that it needs to retrieve and apply an updated configuration profile. For these notifications to work properly, you must allow the Apple Push Notification service to pass your network firewall.

For OS X computers and an MDM server to communicate with the Apple Push Notification service, 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.

Setting up a Profile Manager server

To set up a Profile Manager server:

1. Open the Server app.



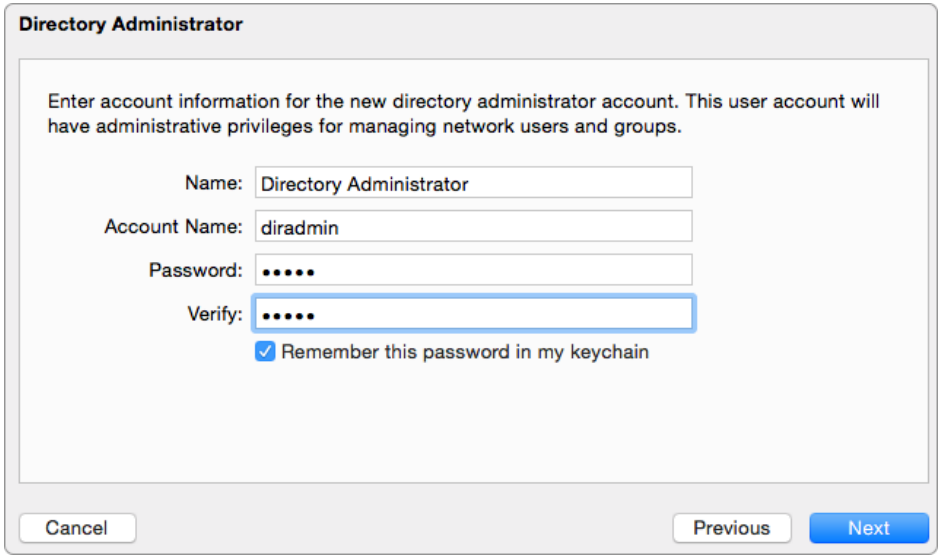
2. Select Profile Manager from the menu on the left.
3. In the Profile Manager page, click the on/off switch to turn on Profile Manager.

   Wait a moment while Profile Manager service starts.
4. Click Configure (to the right of Device Management).

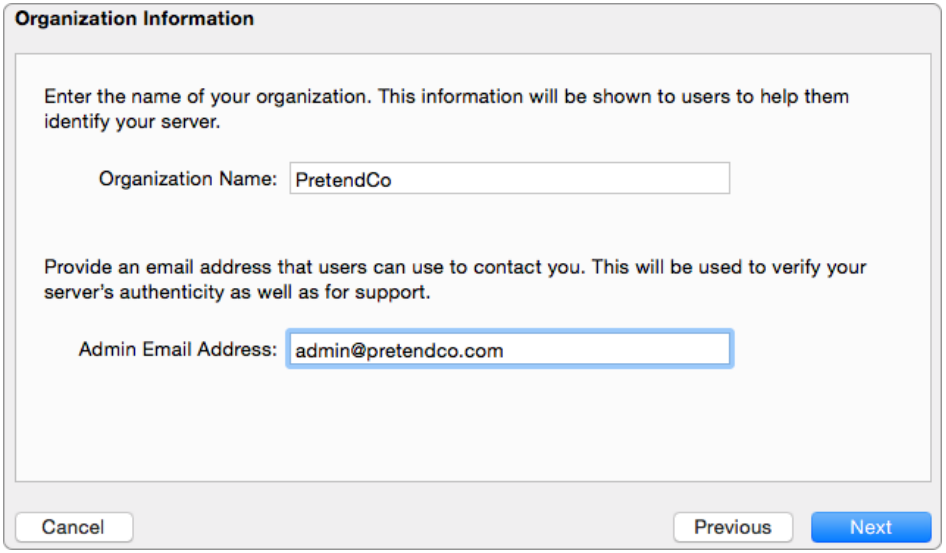
   The Server app guides you through the steps to set up the service, including configuring the server as an Open Directory Master.

   To use Mobile Device Management, the server must be an Open Directory Master and have valid certificates for SSL and the Apple Push Notification service. 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.

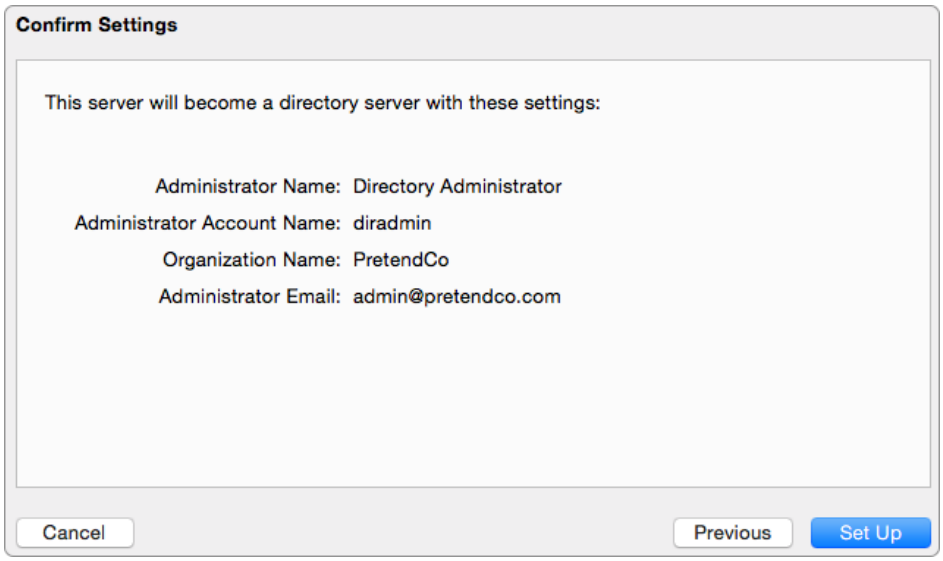
5. In the Configure Device Management dialog, click Next.
6. In the "Configure Network Users and Groups" dialog, click Next.
7. In the Directory Administrator dialog, enter the account information for the administrative user of the new Open Directory instance you're creating.



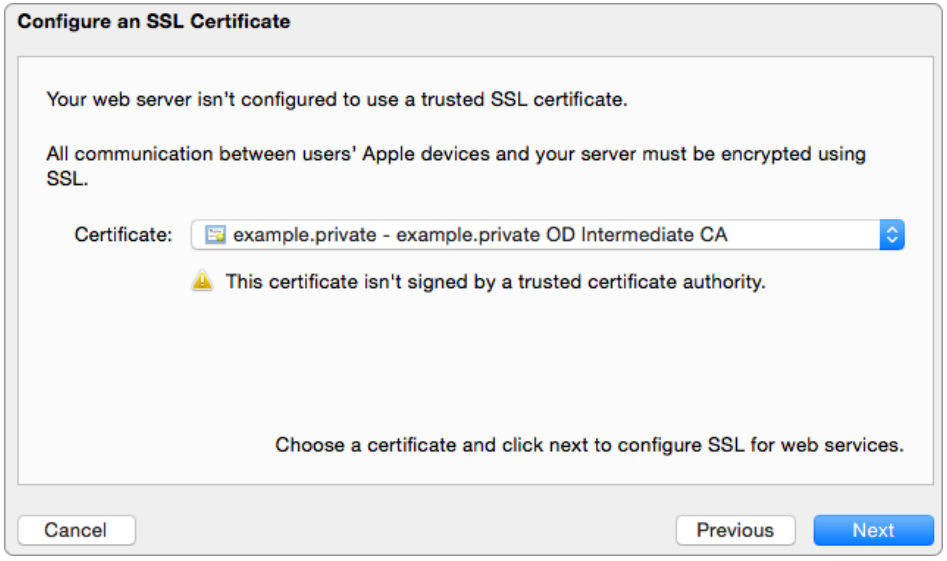
8. Click Next.
9. In the Organization Information dialog, enter the name of your organization and an administrator email address for the Open Directory instance you're creating. (Don't include commas in your organization name.)



10. Click Next.
11. In the Confirm Settings dialog, review the settings to create the new Open Directory Master.



12. If the settings are correct, click Set Up. If you need to make changes, click Back.
13. In the Organization Information dialog, enter any contact information that you want to provide users. Then click Next.
14. In the "Configure an SSL Certificate" dialog, choose your code-signing certificate from the Certificate pop-up menu.



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 want to manage will need to take an extra step to explicitly trust your server.

15. Click Next.

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

16. In the "Get an Apple Push Notification service certificate" dialog enter your organization's Apple ID and password. If your organization doesn't have an Apple ID, click "Create one now."

17. Click Next.

18. In the Confirm Settings dialog, click Finish.

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

    To assign apps and books purchased through the Volume Purchase Program (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.

    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.

    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.

    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.

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

19. 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 OS X Server, you must 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 it isn't, add users before setting up profiles in Profile Manager.

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

1. Open the Server app from /Applications/.
2. Select Users from the Accounts list on the left.
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.

   Make sure the "Allow user to administer this server" checkbox is deselected.
6. Choose "None - Services Only" from the Home Folder pop-up menu.
7. 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 adding users.

Creating user and device group default settings

You can create default settings for any user, user group, device, or device group, and share those settings with devices or users that need them.

Note: The following process is an example only. Exact steps for your process may differ.

To create defaults for and configure a teacher's iPad:

1. Create a default-settings group called "teachers."
2. Create a default-settings group called "iPad."

3. Create a user account for a teacher.
4. Put the teacher's user account into the "teachers" and "iPad" default settings groups.

   This assigns the teacher two collections of default settings—one from each group.

   Optional: Create additional settings tailored for the teacher.

Editing management profiles

Use Profile Manager to create, edit, and delete configuration profiles as well as to 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 was properly bound.

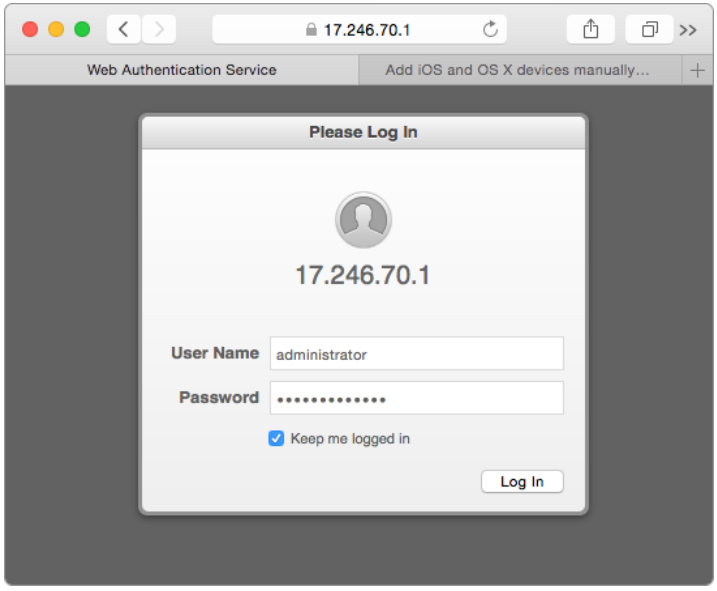
Although each user, group, device, or device group can have only one management profile assigned to it in Profile Manager, each device can belong to many groups. This enables the layering of settings via profile inheritance.

Use the General settings payload to specify whether users can remove a profile after it's installed.

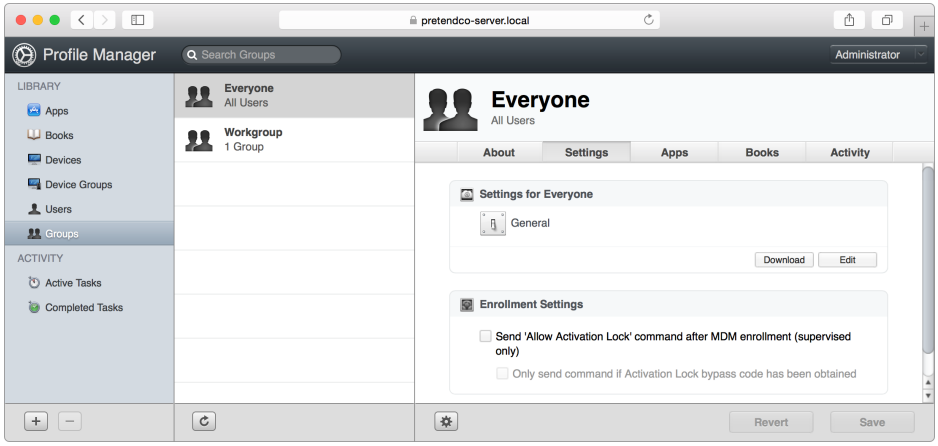
To edit configuration profiles:

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

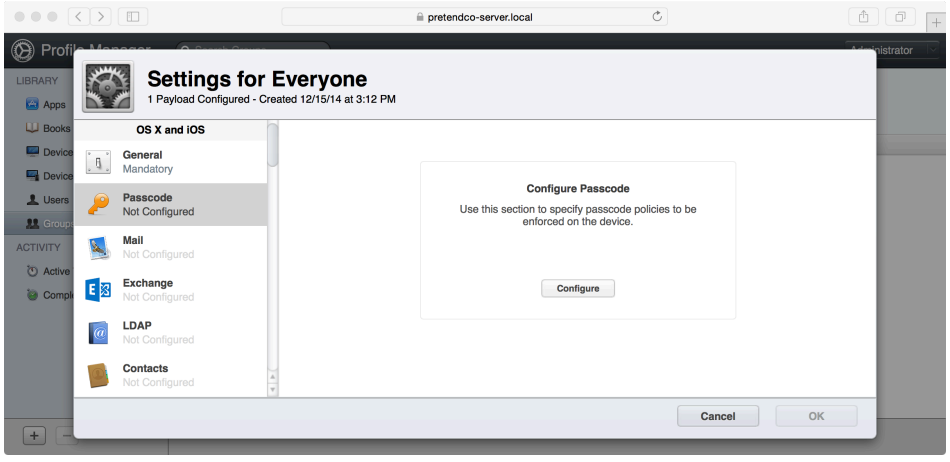
   https://*yourserver*/profilemanager
2. Authenticate as needed with your administrator credentials.



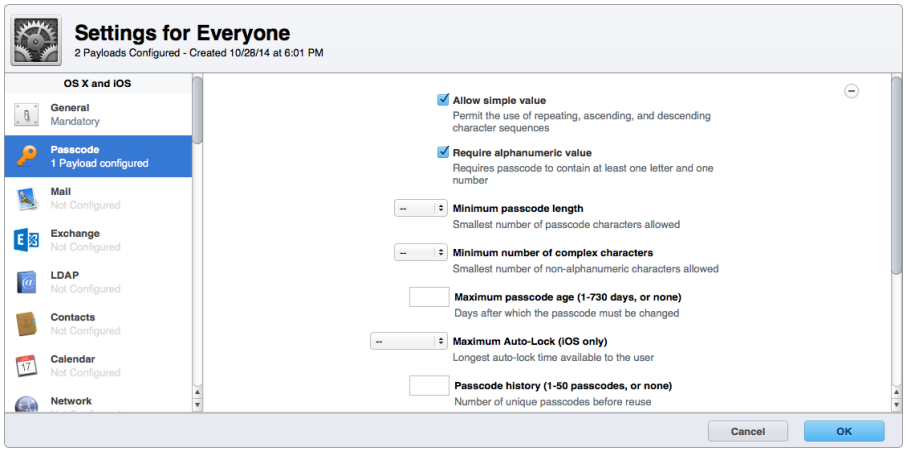
3. Click Log In.
4. Select the user, group, device, or device group that you want to edit.
5. Click the Settings tab.



6. Click Edit for the profile.
7. Select a settings category from the list on the left.



8. Click Configure.



9. Click OK.
10. Click Save to update the profile settings.
11. Click Save when asked to confirm that you want to save the settings.

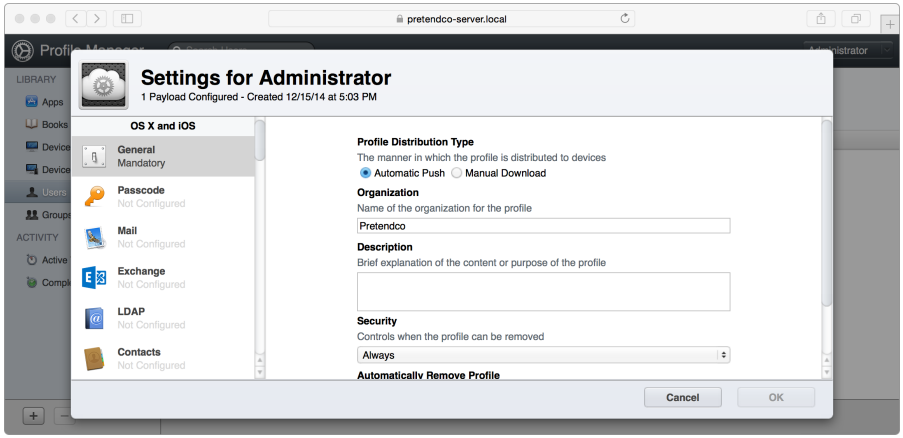
    When you update settings for an automatic push profile, devices receive Apple push notifications.

    To create custom profile settings:

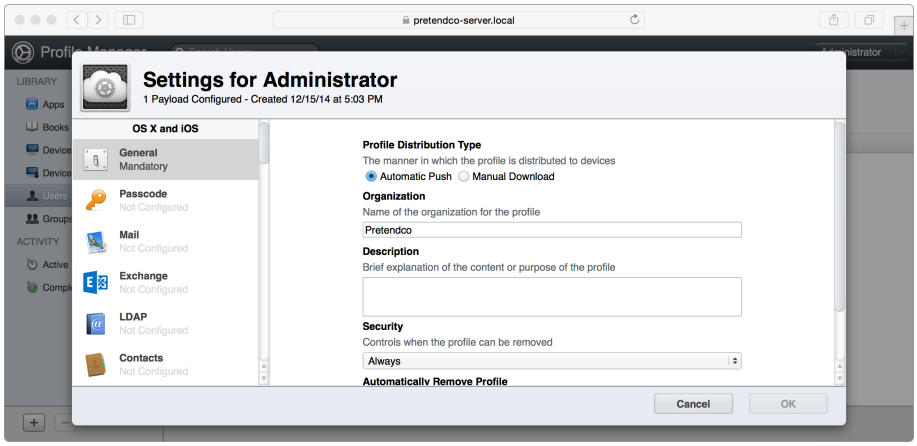
    You can manage settings beyond those defined by Profile Manager. With the Custom Settings, you can add a payload with key-value pairs that override settings in the corresponding preference domain. For example, you might want to manage settings for an app that isn't included with OS X. Another example may be that there isn't a payload setting that corresponds to the Finder preference setting to control the display of hard drives on the desktop.

1. Open a web browser and navigate to the following, where *yourserver* is the name or IP address of your server running the Profile Manager service:

   https://*yourserver*/profilemanager
2. Authenticate as needed with administrator credentials.
3. Click the Settings tab.
4. Select the user, group, device, or device group profile that you want to edit.
5. Click Edit.



6. Select Custom Settings from the list of payload types.
7. Click Configure.



8. Enter the name of the preference domain that you want to manage.

   This example uses com.pretendco.widget, which is the identifier for an in-house app at PretendCo.
9. Click Add Item.
10. Under Key, replace the New Item text with the key representing the preference you want to manage.

    In this example, the preference to automatically dial phone numbers selected in the app is AutoDialNumbers.
11. From the Type pop-up menu, choose the value type for the setting.

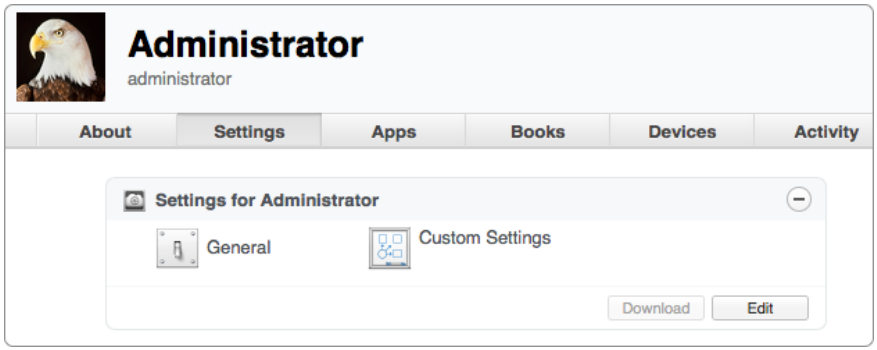
    The AutoDialNumbers setting is Boolean.

12. Set the value.

    For the Boolean type, the value is represented by a checkbox. (Checking the box means true; not selecting it means false.)

13. Click OK.

    The Custom Settings payload is added to the profile.



14. Click Save to save the updated profile.

15. 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 can then delete any preference entries you don't want to manage.

Distributing configuration profiles

After you define 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 the Profile Manager administration web app and send them to your users via email or post them to a website you create. When users receive or download the profiles, they install them on their device.
- **User self-service** Users can download and install the settings from the built-in user portal of Profile Manager. The user portal ensures that users receive the configuration profiles that you assign to them or their group.
- **Remote device management** You can enable the Profile Manager MDM server, which allows you to remotely install, remove, and update configuration profiles on enrolled devices.

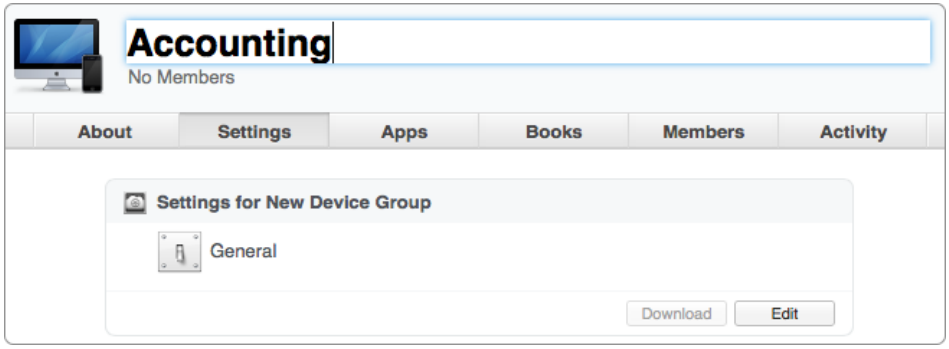
Creating device groups

Use device groups to assign profile settings to specific groups of Mac computers.

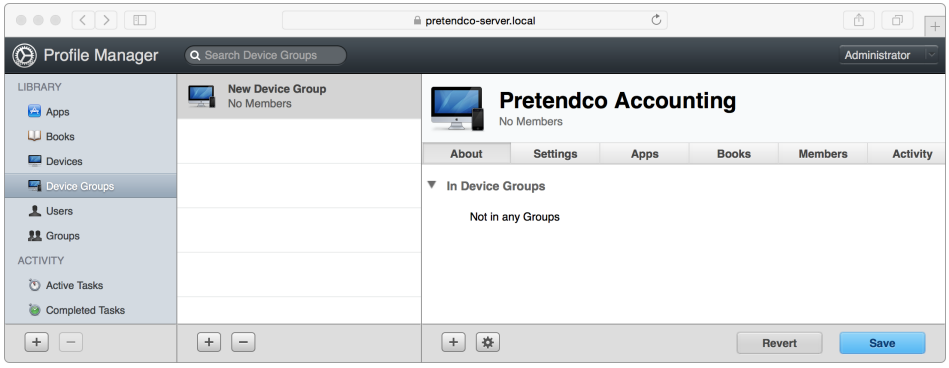
To create a device group:

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

   https://*yourserver*/profilemanager
2. Authenticate as needed with administrator credentials.
3. From the Library list on the left, 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 the Settings tab.



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

Adding devices to a device group

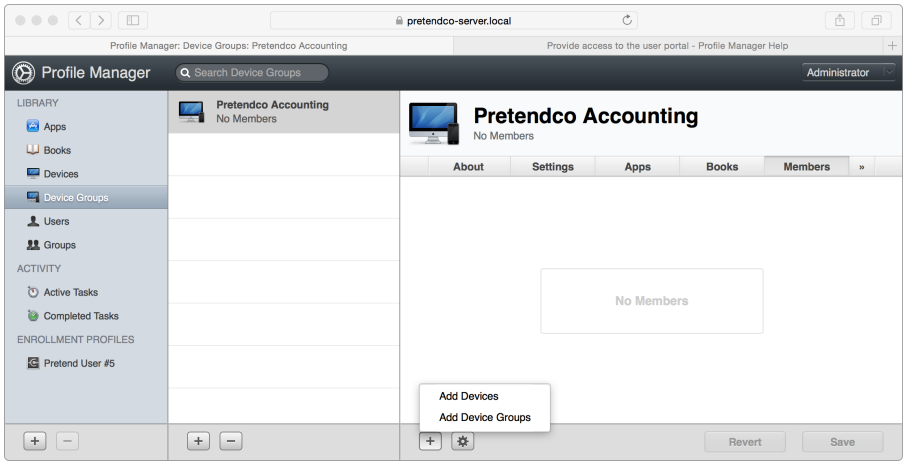
After a device has been enrolled with your Profile Manager server, you can assign the device to a group so you can manage several devices with a common profile.

To add devices to a device group:

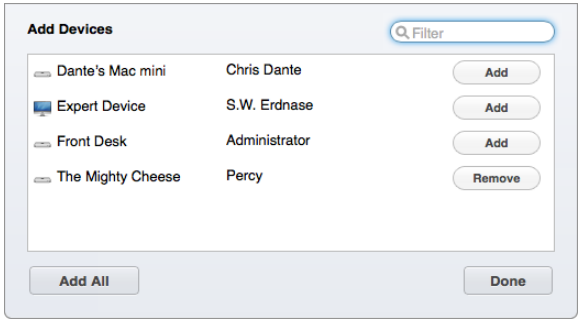
1. Open a web browser and navigate to the following, where *yourserver* is the name or IP address of your server running the Profile Manager service:

   https://*yourserver*/profilemanager

2. Authenticate as needed with administrator credentials.
3. From the Library list on the left, select Device Groups.
4. Select a device group.
5. Click Add (+) inside the 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 from the group, click Remove.

7. Click Done when you're finished adding (or removing) devices.

   The device group updates to reflect the changes you made.

8. Click Save.

Creating device placeholders

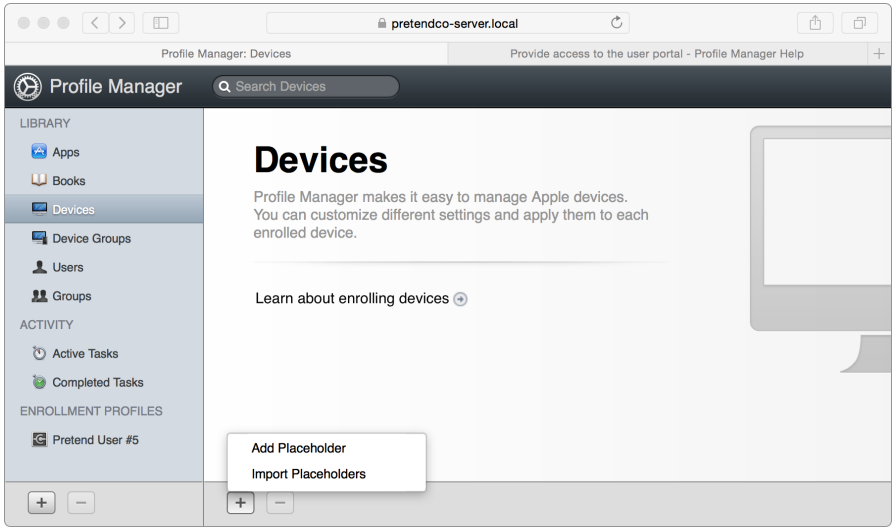
Use device placeholders to prepopulate device records and groups with profile settings. A placeholder record is created based on the device's serial number, Unique Device Identifier (UDID), International Mobile Equipment Identity (IMEI), or Mobile Equipment Identifier (MEID). When you enroll the matching 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.

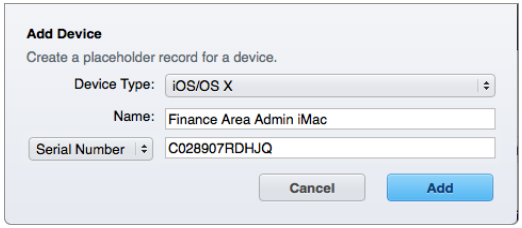
To create a device placeholder:

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

   https://*yourserver*/profilemanager
2. Authenticate as needed with administrator credentials.
3. From the Library list on the left, select Devices.
4. Click Add (+) on the right and choose Add Placeholder.

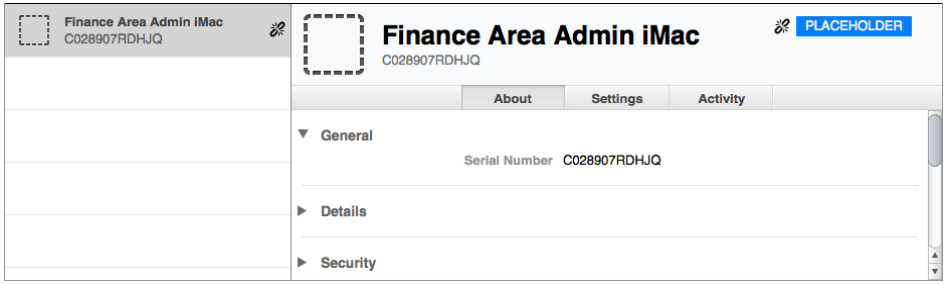


5. In the Add Device dialog, choose iOS/OS X from the Device Type pop-up menu.
6. Enter a name for the device.
7. Choose Serial Number from the Identifier Type pop-up menu and enter the serial number for the device that you'll enroll later.



8. Click Add.

   A placeholder is added to the Devices list.



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.

Once the file is uploaded, placeholders for each of the devices appear in the device list. The file has certain requirements and options:

- The column titles can't contain spaces.
- The device name and at least one additional identifier is required for each device.
- The file can be a mix of any number or type of character identifiers for each device name and can contain kanji characters.

The CSV file should have the following column headers:

Column header	Example
DeviceName	OurPhone
SerialNumber	23432AABCZ5
IMEI	U8938932ae89ui8989eaooi78

Column header	Example
MEID	1312aiu3io2o243234oo23
UDID	ab458782ui3972342

Placeholders for Mac computers can have the SerialNumber or UDID. If UDID is selected, provide the computer hardware UUID.

The DeviceName isn't used to match to a placeholder to an enrolled Mac. When a match occurs, the Device Name is updated to match the computer's Computer Name.

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 and import it.

Enrolling OS X devices

After you set up the Profile Manager server, 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.

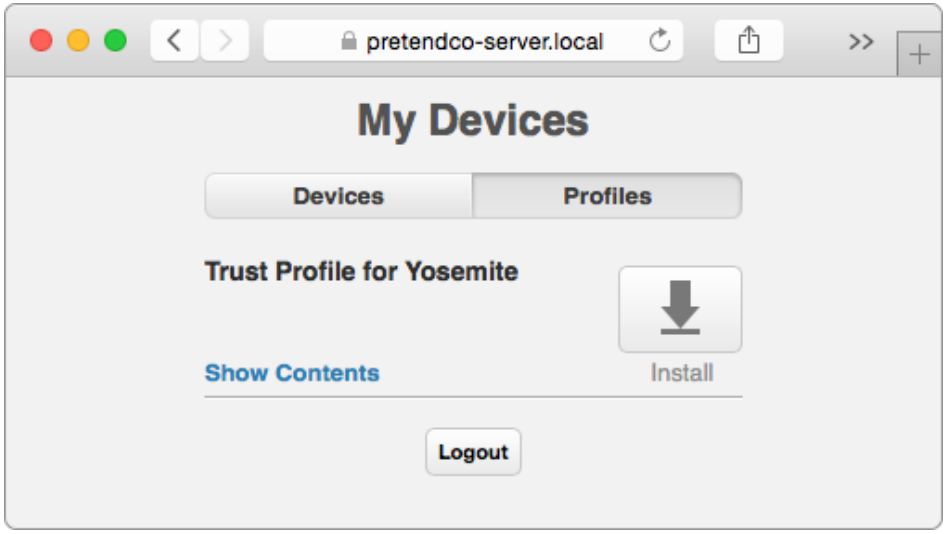
To enroll a Mac:

1. Open a web browser and navigate to the following, where *yourserver* is the name or IP address of your server running the Profile Manager service:

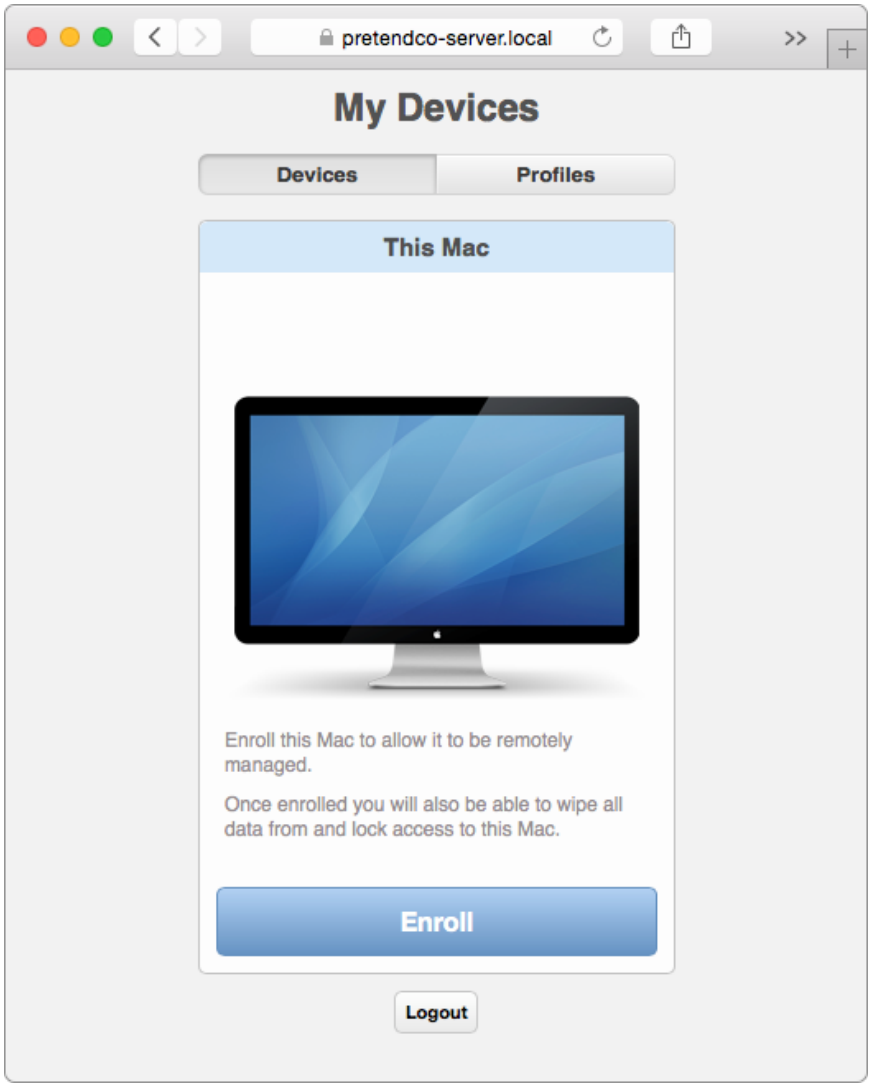
   https://*yourserver*/mydevices
2. Authenticate with a user account on the server.

   The My Devices page appears.

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 enroll a device using Profile Manager, the user responsible for it can perform basic security tasks. The most basic task is a remote lock, which is 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 the following, where *yourserver* is the name or IP address of your server running the Profile Manager service:

   https://*yourserver*/mydevices
2. Log in as the user who enrolled the device.
3. Click the Devices tab.

   The Devices pane shows enrolled OS X and iOS devices.
4. Click Lock for the device you want to lock.
5. Enter the passcode 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

Among the basic security tasks that users can perform, a remote wipe is the most intrusive action because it erases all data on a device.

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

http://support.apple.com/kb/HT4790.

To remotely wipe a device with the user portal:

1. Open a web browser and navigate to the following, where *yourserver* is the name or IP address of the server running the Profile Manager service:

   https://*yourserver*/mydevices
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. Click Wipe.
5. Click OK to confirm that you want to wipe the computer.

   The Mac is wiped, erasing all data.
6. Use Profile Manager to verify that the device was wiped.

   The device entry is now a placeholder. If you reenroll the device, it will automatically match up to the device Profile Manager entry.

Remotely locking a device with Profile Manager

After you enroll a device using Profile Manager, the user responsible for the device can perform basic security tasks. As an administrator, you can also perform security tasks on remote devices.

To remotely lock a device with Profile Manager:

1. Open a web browser and navigate to the following, where *yourserver* is the name or IP address of your server running the Profile Manager service:

   https://*yourserver*/profilemanager

   Authenticate as needed with administrator credentials.
2. From the Library list on the left, choose Devices or Device Groups.
3. Select the device or device group you want to lock.
4. Click the Action menu (gear icon) in the device or device group pane.
5. Choose Lock.
6. Enter a lock PIN code to unlock the device.
7. 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.
8. To make sure the device has been locked, go to the Completed Tasks section of Profile Manager.

Remotely wiping a device with Profile Manager

You can use Profile Manager to perform security tasks on remote devices.

To remotely wipe a device with Profile Manager:

1. Open a web browser and go to the following, where *yourserver* is the name or IP address of your server running the Profile Manager service:

   https://*yourserver*/profilemanager
2. Authenticate with your 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 device passcode. Click Wipe.

   The device will be locked and wiped. All data will be lost.
8. To make sure that 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 Profile Manager user portal, 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 the following, where *yourserver* is the name or IP address of your server running the Profile Manager service:

   https://*yourserver*/mydevices
2. Log in as the user who enrolled the device.

   The Devices pane shows the OS X and iOS devices that you 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

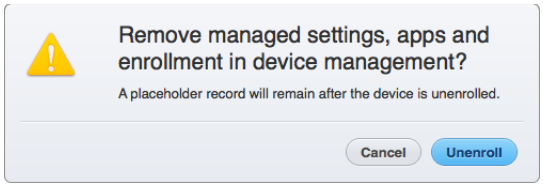
Users who enrolled devices can use the user portal in Profile Manager to lock and wipe devices, as well as disable remote management. With Profile Manager, administrators also have the ability to act on remote devices.

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 the following, where *yourserver* is the name or IP address of the server running the Profile Manager service:

   https://*yourserver*/profilemanager
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.

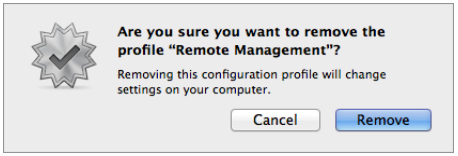
You can use the Profiles pane to review which profiles are installed, to add additional profiles, and to remove or verify existing profiles. You can also install configuration profiles by double-clicking them in the Finder.

Any user with administrator access can remove a device profile.

To remove a device 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 administrator user name and password. Then click OK.

Forcing management profiles

Use management profiles to enforce policy. You have options for controlling how profiles are removed when you 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 can remove it.

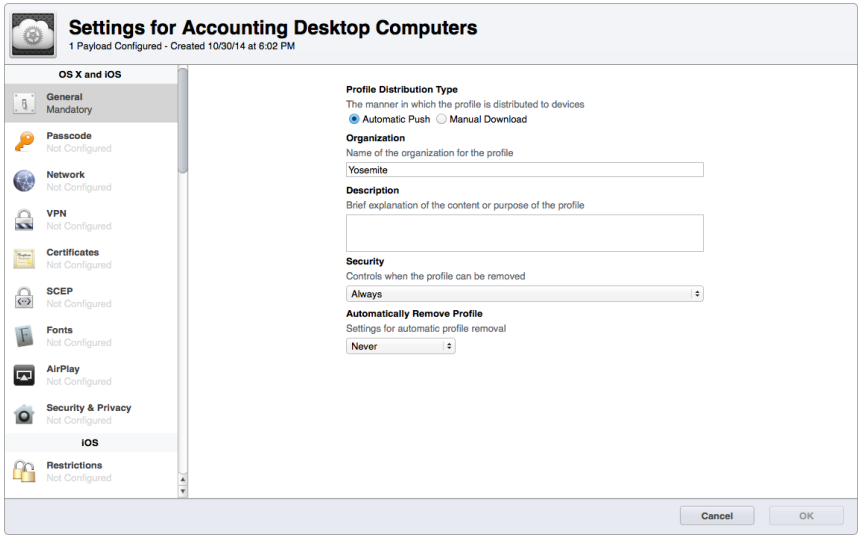
The Never removal setting indicates that a profile can't be removed. The device must be wiped to remove the profile.

To change profile removal rules:

1. Open a web browser and navigate to the following, where *yourserver* is the name or IP address of the server running the Profile Manager service:

   https://*yourserver*/profilemanager
2. Authenticate as needed with administrator credentials.
3. From the Library list on the left, choose Devices, Device Groups, Users, or Groups.
4. Select the device, device group, user, or group you want to edit.
5. Select Settings.
6. Click Edit for the profile.

   The settings pane appears for the profile you chose.
7. In the General settings for the profile, change the Security settings as needed.



8. Configure the other settings that should be deployed with the profile.
9. Click OK to close the settings pane.
10. Click Save to update the profile settings.

Client management suites

You probably use a client management suite to centralize your workflows. The workflow that you develop for software delivery and management, patching, and remediation is probably 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 many ways. For available software solutions, see the following lists.

Imaging and client management

- JAMF's Casper Suite
- Absolute Manage
- KACE
- LANDesk
- FileWave

Client management only

- AirWatch
- MobileIronlivepage.apple.com
- Centrify
- Thursby's ADmitMac
- Quest Management Xtensions (QMX)

Additional resources

- "Manage devices with Profile Manager" section, OS X Server: Advanced Administration
- *Apple Technical White Paper: Managing OS X with Configuration Profiles*
- Managing Devices with Configuration Profiles, *OS X Server Essentials 10.10: Using and Supporting OS X Server on Yosemite*, Peachpit Press

Managing Software Updates

5

OS X Server 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.

In this chapter, you'll learn how to develop an effective software-update policy and how to use the OS X Server Software Update service.

Developing an effective software update policy

After you deploy Mac computers, you should develop a policy for managing software updates. Doing this helps you prevent bad software-update deployments. It also reduces the chances that you'll have to redeploy systems that you know are good. Your policy should cover these processes:

- Testing software updates before they're deployed
- Deploying software updates
- Logging changes in your organizational management data base after you deploy software updates

Here's an example of an effective three-phase policy 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. If you build a software update service, you help keep large operating system updates and software packages from increasing network traffic in environments with larger deployments. You also give your IT department a built-in way to manage releases.

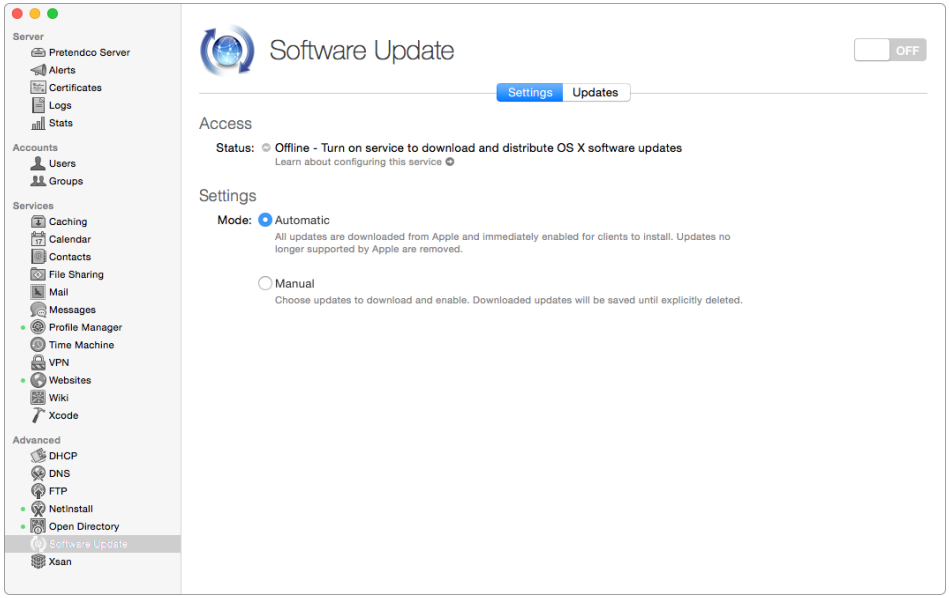
The Apple Software Update service runs on the Apache web server in OS X Server. The Software Update service synchronizes updates from Apple Software Update servers and stores update digests in XML files. Client computers poll the XML files to determine which updates to install and then they remotely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

Only software updates marked "Enabled in the Software Update service" are available for client Mac computers to download. You can disable an update to block its distribution until it has been approved.

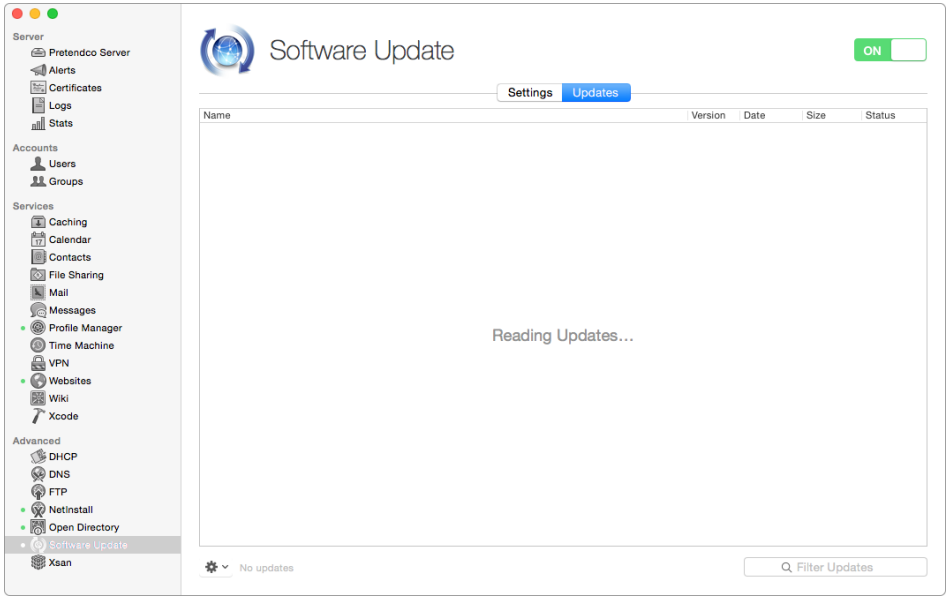
To configure the Software Update service for OS X Server:

1. Open the Server app from /Applications/.
2. Select Software Update in the sidebar. Click Settings.
3. Choose whether updates should be automatic or manual.

   Automatic updates mirror those from Apple with no intervention. With manual updates, you can choose whether to release each patch provided by Apple.



4. Click the on/off switch to turn on Software Update and begin caching patches from Apple.
5. Click the Updates tab.



If you don't immediately see updates, don't be concerned. In some cases, it can take many hours for them to appear.

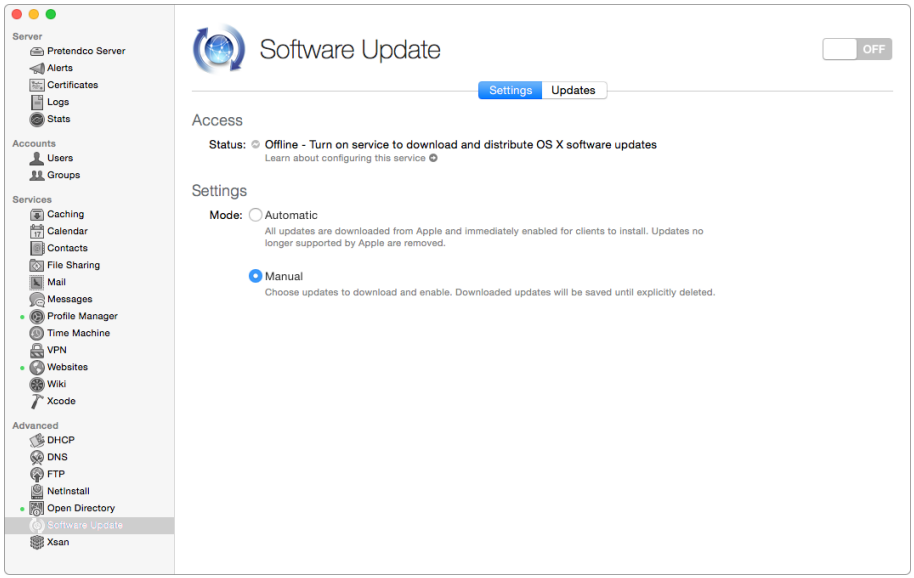
To enable or disable a software update:

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

1. In the Software Update pane, click the Settings tab.

   To manage available updates, set the Software Update service to Manual mode.

2. Select Manual.



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.

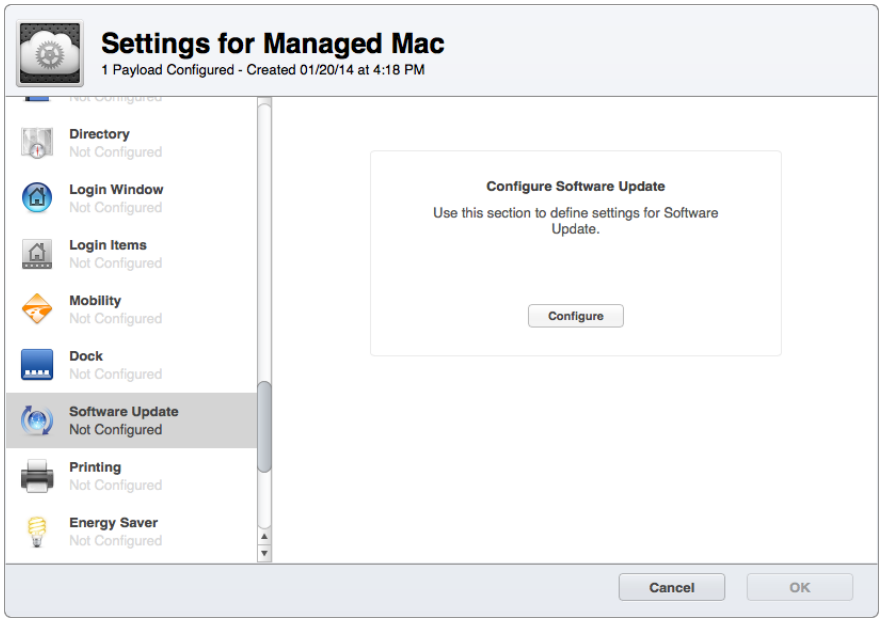
Configuring Software Update Server clients

After you set up Software Update services, point client computers to them. Whether you use Profile Manager or edit the com.apple.SoftwareUpdate.plist file, test your Software Update service settings to ensure that they're working the way you want them to. Do this before you push settings to your organization.

After you set up the Profile Manager service, you can modify a profile to configure clients to use a specific software update server.

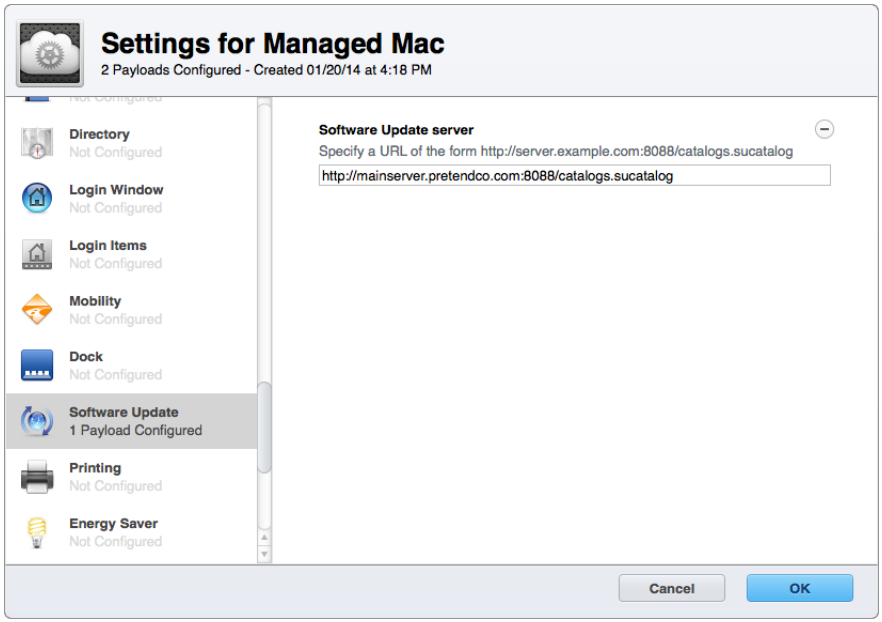
To configure clients to use Software Update Server using Profile Manager:

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 following for Software Update Server, where *server.example.com* is the IP address or DNS name of the host running the Software Update service:

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



6. Click OK.
7. Click Save.
8. Click Save again to confirm that you want to save the updated profile.

To manually configure clients to use Software Update Server:

1. If your client systems aren't managed, or if you want to test Software Update functionality without using a policy, enter the following at the command line:

   defaults write /Library/Preferences/com.apple.SoftwareUpdate CatalogURL "http://server.pretendco.com:8088/catalogs.sucatalog"

   This step augments the default software update settings and replaces *server.pretendco.com* with the IP address or DNS name of the host running the Software Update service.
2. To point a client Mac back to Software Update Server, use the following command:

   defaults delete /Library/Preferences/com.apple.SoftwareUpdate CatalogURL
3. **Optional:** Delete the /Library/Preferences/com.apple.SoftwareUpdate.plist file.

   This resets the Software Update settings to factory defaults and allows the Mac to generate a new preferences file based on default settings.

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. Software agents running on client systems then download Apple updates from the staging servers rather than from Apple. Software agents can be forced to obtain software updates from a local staging server. Both Absolute Manage and JAMF have this functionality and can run on OS X Server, Linux Server, or Microsoft Windows Server.

Additional resources

- "Manage updates and installation: Host software updates," OS X Server: Advanced Administration
- Implementing Software Update Service, *OS X Server Essentials 10.10: Using and Supporting OS X Server on Yosemite*, Peachpit Press

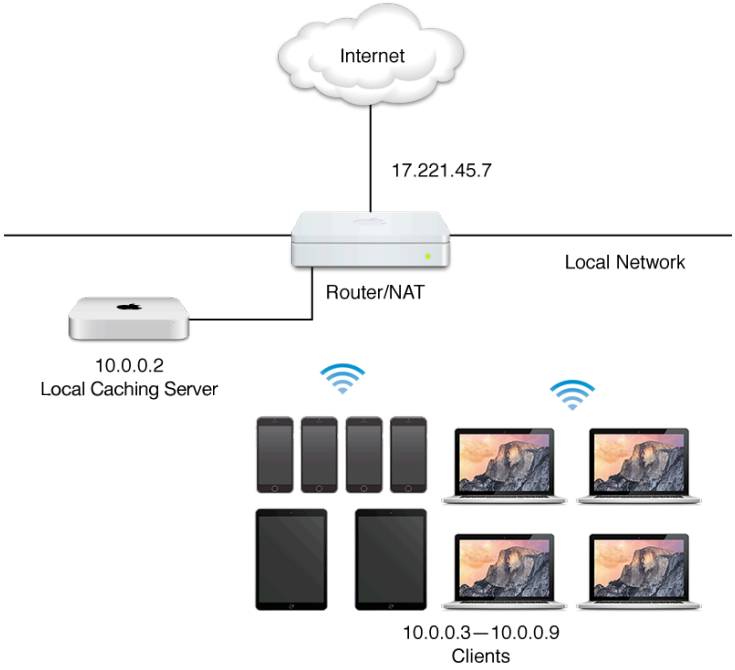
Caching Software Downloads

6

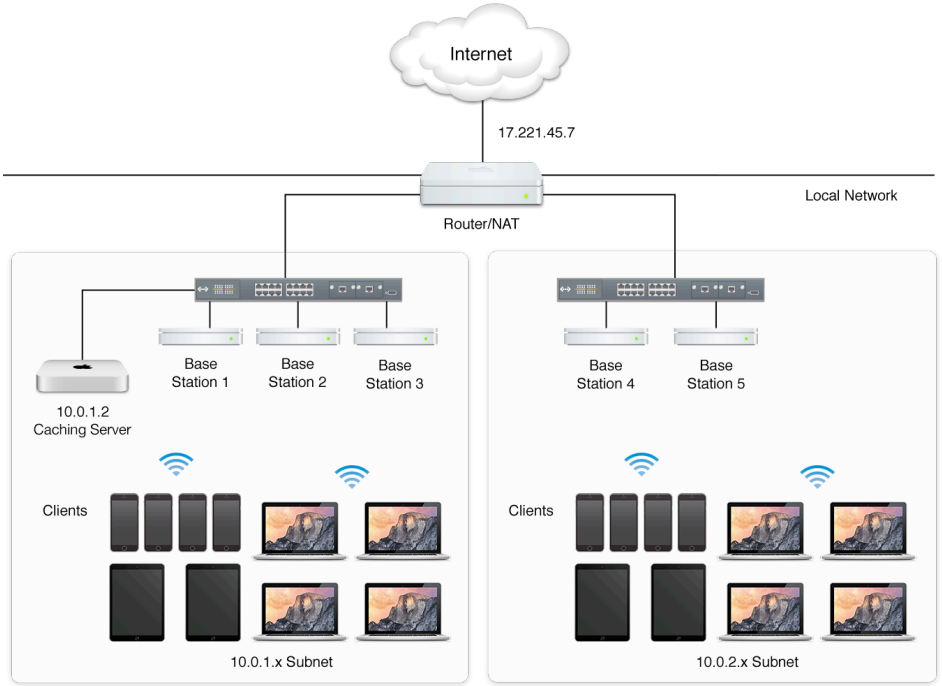
Caching Server speeds up Apple-provided software downloads. When OS X and iOS devices share the same public IP address as Caching Server, and they download Apple-provided software, they're automatically redirected to Caching Server. When users take their devices home and download Apple-provided software, their devices revert to getting software directly from Apple.

Like the Software Update service, the Caching service caches Apple-provided software updates. But the Caching service also caches other content, such as apps and books, downloaded using iTunes, the App Store, iBooks Store, or the Mac App Store.

Caching Server works with single subnets or multiple subnets that share the same IP address. Here's an example of a single subnet and a Mac mini with OS X Server and the caching service:



Here's an example of a network with two subnets that share a single caching server:



Using the caching service

To set up Caching Server:

1. Ensure that your environment meets Caching Server requirements.

   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 when using the network address translation method (NAT).

2. Use Ethernet to get the best performance from Caching Server.

   Caching Server can serve hundreds of clients at once and may saturate a Gigabit Ethernet port. So, if you have a small- to medium-scale deployment and you find a performance bottleneck, it's probably in your local area network bandwidth.

3. Make sure that you have enough caching server hardware.

   If many clients access the caching server at the same time, and you suspect that your caching server hardware may be causing a performance bottleneck, check the Processor Usage graph in the Stats pane of Server app. If the processor usage is constantly at or near the maximum, add caching servers (such as Mac mini or Mac Pro computers with OS X Server) to distribute your client caching requests.

4. Set the appropriate cache limit.

   As Caching Server gets requests for caching downloads, it uses more disk space to store the cached content. When the disk space used reaches the maximum that you specified in the Caching pane, or when the available space on the volume reaches 25GB, Caching Server deletes the least recently used cached content to make space for the next request.

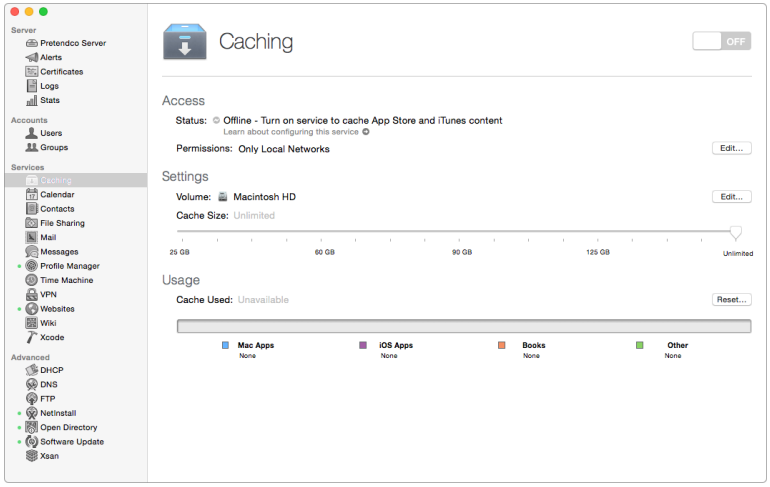
   If your server is in an environment in which clients download different kinds of content,set the cache size limit so Caching Server can handle the volume of downloads. By setting the cache size limit high enough, you prevent Caching Server from frequently deleting cached data. When Caching Server frequently deletes cached data, it may be downloading the same content repeatedly, which consumes Internet bandwidth.

5. Choose a cache location.

   The default location for cached content is the boot volume. You can also choose an alternate location. In both cases, specify how much of the volume will be used by the caching service.

To start the caching service:

1. Open the Server app from /Applications/.
2. Select Caching in the sidebar.

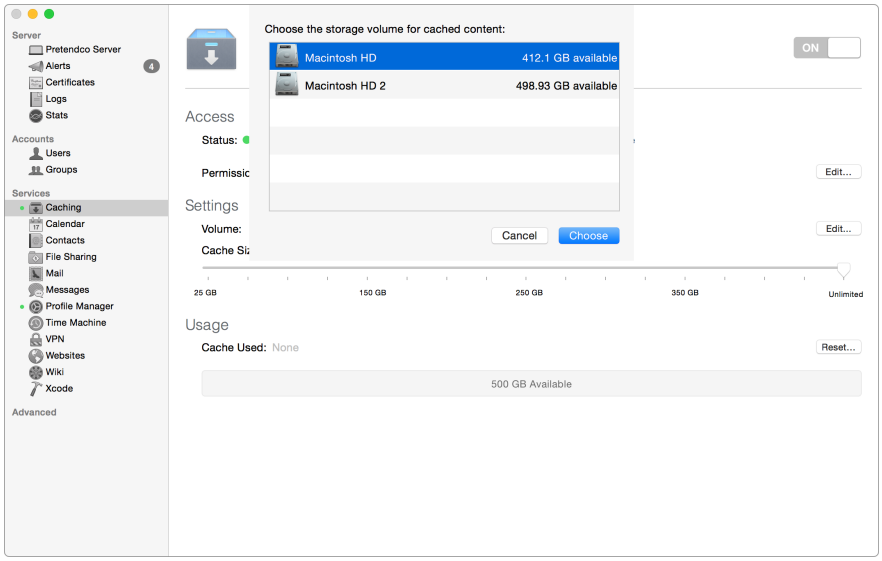


3. Click the on/off slider to turn on the caching service.

   The caching service starts to cache Apple software downloads.

To select a volume for caching:

1. In the Caching pane, click Edit (to the right of Settings).
2. Select a storage volume.



3. Click Choose.

To delete all cached content:

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

To set cache size:

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

Additional resources

- "Manage updates and installation: Provide update Caching service," *OS X Server: Advanced Administration*
- Caching Content from Apple, *OS X Server Essentials 10.10: Using and Supporting OS X Server on Yosemite*, Peachpit Press
- OS X Server: Content types supported by the Caching service

Software Update and Caching Service Differences

7

The Software Update and caching services both cache downloads of Apple-provided software, but they aren't the same. The following list describes some main differences.

- With the Software Update service, updates are downloaded in advance of client computers that request 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 subsequently experience faster downloading as they get the app from Caching Server.
- With Software Update, you can select the updates that are available to client Mac computers. Use Software Update when you want to restrict access to new software until it's tested for compatibility.
- You don't have to configure the caching service. On a regular basis, Caching Server registers itself and its public IP address with Apple software servers. When client devices attempt to access Apple servers, the devices are automatically directed to the caching server associated with your public IP address.
- The caching service doesn't provide control over software availability. Client computers configured to use Software Update Server don't access Caching Server for software updates. They use Caching Server for other downloads, such as app purchases.
- You must manually configure Software Update clients to use a specific software update server. You don't have to configure caching service clients. OS X and iOS devices automatically access the available caching server on the network they're currently connected to. This makes Caching Server mobile-client friendly. For example, when a user is using an OS X or iOS device at work, the device uses Caching Server at work. When the same user uses the same device at home, the device automatically uses a different caching server.
- Software Update downloads and caches available updates when it starts up. Caching Server downloads and caches software based on client requests.

- Software Update provides client management. For example, you can restrict which updates clients see and download. Caching Server doesn't provide client management. If you configure your clients to use Software Update, the client can't use Caching Server.
- You can put the Software Update and caching services on the same computer running OS X Server, but they won't share cached content, and this combination may use more disk space.
- Your users' OS X and iOS devices come ready to use Caching Server.

Additional Resources

Mac Management Basics exam

Add the Apple Certified Associate Mac Management 10.10 certification to your credentials. Instructions for taking the online exam are at:

http://training.apple.com/itpro/macmgmt1010/exam

OS X training and 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

Apple Certified Trainers teach courses through a worldwide network of Apple Authorized Training Centers (AATCs).

OS X Support Essentials 10.10 provides an intensive and in-depth exploration of troubleshooting on OS X, touring the functionality of OS X systems.

OS X Server Essentials 10.10 gives technical coordinators and entry-level system administrators the knowledge to implement an OS X Server–based system.

OS X certifications

Apple OS X certifications are 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.

Books

The Apple Training Series books cover OS X and OS X Server and are a key part of the Apple official curriculum. With these books, you can independently study OS X and OS X Server before you take the certification exam. The books guide you, step by step, through real-world projects. The books are also excellent references for performing specific tasks and understanding Apple technologies.

There are two books in the Apple Training Series. They're both written for IT support and system administration personnel. Both are available from Peachpit Press.

- *OS X Support Essentials 10.10*
- *OS X Server Essentials 10.10*

Support

The AppleCare Protection Plan provides global repair coverage, both parts and labor, from Apple-authorized technicians around the world.

Apple also provides online support where you can access technical articles, download manuals, and join discussion forums.

If you are new to OS X, see Mac Basics on the Apple Support site.