A very common use for managed preferences on Mac OS X is to manage mobile accounts. In fact, it was precisely this need that caused one of your humble authors to implement Local MCX in his organization—he had previously managed a lot of things through the use of various scripts that directly manipulated preference files. But a desire to automate the creation of mobile accounts and the enforcement of FileVault protection for these accounts led him to implement managed preferences. This then trickled down and replaced most of the homegrown management scripts used earlier.

Apple has provided many useful controls for configuring and controlling the creation and management of mobile accounts in their Managed Preferences framework. Many of the things that are relatively straightforward to implement using Managed Preferences are difficult if not impossible to implement any other way.

Chapter 11 contains several small, self-contained recipes for using managed preferences to address common administrative tasks. This chapter can be thought of as a bigger recipe devoted to a single subject, mobile accounts. We’ll explore using managed preferences to simplify the creation of mobile accounts, the enforcement of FileVault security, and the setup of HomeSync preferences. We’ll also discuss some of the major choices to consider when implementing a management policy for mobile accounts.
Mobile Accounts Review

You may remember that a mobile account is a user account whose information originates in a network directory service, but is cached in the local directory service. This provides the benefits of a network account, such as centralized administration, consistent access to internal network resources, and the same username and password regardless of machine. However, since the account information is cached locally on the machine, a user can still log in and use the computer even if it’s not connected to the organization’s network. Changes in the network account information are synchronized with the locally cached account, and vice versa.

Mobile accounts are especially useful on laptops, which, due to their nature, are frequently not on the organization’s network. In the past, laptops were difficult to manage with management systems that relied on a continuously available network connection. This was less of a problem when laptops were relatively uncommon. But today, laptops are a larger percentage of machines in many organizations, making it increasingly important to develop and implement effective management strategies. Because they may regularly leave the premises of your organization, laptops introduce new things to worry about, making consistently managing these devices even more important.

Prerequisites

There are certain prerequisites for mobile accounts. Most importantly, you must have a network directory service already in place. In most cases, you’ll also want to have network home directories available. Setting up a network account/network home infrastructure is beyond the scope of this book. But if your organization already has in place a network directory service such as Open Directory, Active Directory, or an LDAPv3 directory, you should be able to configure mobile accounts, using this chapter as a guide.

NOTE: For best results, if you are using an LDAPv3 directory you may need to extend the LDAP schema to include the apple-generateduid attribute for all user objects (and index this attribute as well!). Refer to Chapter 6 for more information about LDAP schema extension.

If, in addition, user accounts in the network directory service have network home directories, you can also create “portable home directories,” in which a subset of the network home is kept in sync with a local home directory.