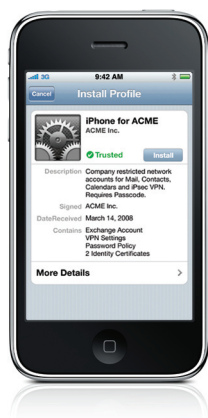




iPhone in Business

Device Configuration Overview



Supported passcode policies:

- Require passcode
- Allow simple value
- Require alphanumeric value
- Passcode length
- Number of complex characters
- Passcode age
- "Time before" auto-lock
- Number of unique passcodes before reuse
- Grace period for device lock
- Number of failed attempts before wipe

Available restrictions

- Access to explicit media in iTunes Store
- Use of Safari
- Use of YouTube
- Access to iTunes Store
- Use of App Store and iTunes to install applications
- Use of the camera (can also be controlled with an Exchange policy)

Deploying iPhone across your organization is easy with the use of configuration profiles. Configuration profiles are XML files that contain configuration information and settings that permit iPhone to work with your enterprise systems.

iPhone Configuration Utility 2.0 lets you easily create, encrypt and install configuration profiles. It can also track and install provisioning profiles and authorized applications, and capture device information including console logs. The iPhone Configuration Utility is available for Windows and Mac OS X.

Configuration Profile Components



Passcode policies

Protect your enterprise data by configuring device passcode policies and requiring their use.



Restrictions

In addition to passcode policies, configuration profiles can be used to restrict certain device features.



Wi-Fi settings

Whether you are configuring iPhone to connect to a private network or for RADIUS authentication to enterprise wireless access points, configuration profiles can be deployed to streamline access to Wi-Fi networks.



VPN settings

Configure VPN server settings including accounts, proxies, and authentication settings for your corporate private networks.



Email settings

Configure IMAP or POP mail settings, including incoming and outgoing mail servers.



Exchange settings

Include server, domain, and account information in a configuration profile so that your users can connect via Microsoft Exchange ActiveSync.



LDAP

Configure access to LDAP directories for contact look-up in Mail, Address Book, and SMS.



CalDAV

Provide these settings to synchronize calendar data with your company's CalDAV server wirelessly.



Web Clips

Place icons on your user's home screen to provide quick access to internal or external websites.



Credentials

Ensure the identity of your users and control access to key enterprise services such as Microsoft Exchange ActiveSync, VPN, and WPA2 Enterprise Wi-Fi networks on iPhone.



Advanced

Edit these settings to modify the Access Point Name (APN) on iPhone. APN proxy settings can be specified using a configuration profile as well.

Protecting Configuration Profiles

Security options

When preparing to deploy your configuration settings, you'll need to export your configuration profile from the iPhone Configuration Utility. The file that is created has a .mobileconfig extension. This file can be created with three different levels of security. With any of these methods, you should make sure that when the profile is distributed, it is accessible only to authorized users.

Unsigned—A plain text .mobileconfig file is created. It can be installed on any device. Some content in the file is obfuscated to prevent casual snooping if the file is examined. This profile will appear as unsigned and will prompt the user with a security message.

Signed—The .mobileconfig file is signed and will not be installed by a device if it is altered. Once installed, the profile can only be updated by a profile that has the same identifier and is signed by the same instance of the iPhone Configuration Utility. Like unsigned profiles, some of the information in the signed profile is obfuscated to prevent casual snooping if the file is examined.

Signed and encrypted—The profile is signed so it cannot be altered, and all of its contents are encrypted so the profile cannot be examined. Encrypted profiles can be distributed via desktop synchronization using the iPhone Configuration Utility or by Over-the-Air Enrollment and Configuration. An encrypted configuration profile can only be installed on the device for which it was created.

Controlling the removal of profiles

When creating a configuration profile, you have the option of controlling whether or not it can be removed by the user. You can lock the profile so that once it has been installed, its removal requires an administrative password or a full reset of the device.

Deploying Configuration Profiles

Configuration profiles can be distributed using four different deployment methods.



Desktop installation via USB

iPhone configuration profiles can be installed through a USB connection with the iPhone Configuration Utility. When you install directly onto a device using USB, the configuration profile is automatically signed and encrypted.

1. Connect the device to your computer using a USB cable.
2. Select the iPhone from the Devices list, and then click the Configuration Profiles tab.
3. Select a configuration profile from the list, and then click Install.
4. On the device, tap Install to install the profile.



Email

You can distribute configuration profiles using email. Users install the profile by receiving the message on their device, then tapping the attachment to install it.

1. Export the profile from the iPhone Configuration Utility.
2. Attach the configuration profile (uncompressed) to an email and send to user(s).
3. Users install the profile by tapping the file directly from the message body in Mail on iPhone.



Website

You can distribute configuration profiles using a website. Users install the profile by downloading it using Safari on their device.

1. Export the profile from the iPhone Configuration Utility.
2. Host the configuration profile (uncompressed) on a secure site accessible to user(s).
3. Users navigate to the website using Safari on iPhone and tap the file to initiate installation on iPhone.



Over-the-Air Enrollment and Distribution

You can distribute encrypted configuration profiles over the air using a secure enrollment and configuration process enabled by the Simple Certificate Enrollment Protocol (SCEP).

For more information about Over-the-Air Enrollment and SCEP, visit www.apple.com/iphone/enterprise/integration.html