Configuration Profiles Reference Guide

Configuration Profiles: Reference Guide

Courtesy of http://help.apple.com/configurator/mac/1.4.1/

General payload settings

This is where you provide the name and identifier of the profile, and specify whether users can remove the profile after it's installed.

Name: This name appears in the profiles list and is displayed on the device after the configuration profile is installed. The name doesn't have to be unique, but you should use a descriptive name that identifies the profile.

Organization: The name of your organization, which helps users identify the source of this profile.

Description: The purpose of the profile. A description is useful if you manage profiles wirelessly using a mobile device management solution that queries devices for the installed profiles. This description is shown in the device's Settings app.

Consent Message: This message is presented to the user during profile installation.

Security: Choose an option from the pop-up menu to prevent a user from deleting a profile installed on a device. Use the With Authorization option to specify an authorization password that lets the profile be removed from the device. If you choose Never, the profile can be updated with a new version, but it can't be removed from the device by the user.

Automatically Remove Profile: Choose when to remove this profile from the device. You can choose to not automatically remove this profile, to remove this profile on a specific date, or to remove the profile after a specific length of time from when it is installed.

Passcode payload settings

Use this payload to set device policies if you aren't using Exchange passcode policies. You can specify whether a passcode is required to use the device, specify the characteristics of the passcode, and specify how often it must be changed. When the configuration profile is loaded, the user is asked to enter a passcode that meets the policies you specify. Otherwise, the profile won't be installed.

If you use device policies and Exchange passcode policies, the two sets of policies are merged and the strictest settings are enforced. For information about supported Exchange ActiveSync policies, see Exchange ActiveSync and iOS 5 Devices.

Allow simple value: Permits users to use sequential or repeated characters in their passcodes. For example, "DEFG" and "3333."

Require alphanumeric value: Requires that the passcode contain at least one letter or number.

Minimum passcode length: The minimum number of characters a passcode must contain.

Minimum number of complex characters: The number of non-alphanumeric characters (such as $, &, and !) that a passcode must contain.

Maximum passcode age: The number of days until users must change their passcode. It can be set to "none," or from 1 to 730 days.

Maximum Auto-Lock time: If the device isn't used for the period of time you specify, it automatically locks. It can be set to "none," or to lock after 1 to 5 minutes. Enter the passcode to unlock the device.

Passcode history: The number of previous passcodes that are remembered and compared for uniqueness. It can be set to "none," or from 1 to 50 passcodes. If you set a number, a new passcode won't be accepted if it matches a remembered passcode.

Grace period for device lock: Specifies for how long the device can be unlocked again after being locked, without prompting again for the passcode.

Maximum number of failed attempts: The number of failed passcode attempts that can be made before the device is erased. If you don't change this setting, after six failed passcode attempts, the device imposes a time delay before a passcode can be entered again. The time delay increases with each failed attempt. After the final failed attempt, all data and settings are securely erased from the device. The passcode time delay begins after the sixth attempt, so if you set this value to 6 or lower, no time delay is imposed and the device is erased when the limit is exceeded.

Configuration Profiles: Reference Guide

Restrictions payload settings

Use this payload to specify which device features can be used. When the same restriction is set or cleared in more than one configuration profile, the more restrictive setting is applied.

Functionality restrictions

Allow use of camera: When this option is off, cameras are disabled and the Camera icon is removed from the Home screen. Users can't take photos or videos, or use FaceTime.

Allow FaceTime: When this option is off, users can't make or receive FaceTime video calls.

Allow screenshots: When this option is off, users can't save a screenshot of the display.

Allow Photo Stream: When this option is on, users can turn on My Photo Stream. When this option is off, photos in My Photo Stream are erased from the device, and photos from the Camera Roll aren't sent to My Photo Stream. If there are no other copies of these photos, they may be lost.

Allow Shared Photo Streams: When this option is on, users can turn on iCloud Photo Sharing to create photo streams to share with other people, or to subscribe to other people's shared photo streams. When this option is off, photos and videos in shared streams can no longer be viewed on the device. If there are no other copies of these photos and videos, they may be lost.

Allow AirDrop (Supervised Only): When this option is off, users cannot use AirDrop with any apps.

Allow iMessage (Supervised Only): When this option is off, you can't send or receive messages using iMessage. If your device supports text messaging, you can still send and receive text messages. If your device doesn't support text messaging, the Messages icon is removed from the Home screen.

Allow voice dialing: When this option is off, users can't dial a phone number using voice commands.

Allow Siri: When this option is off, users can't use Siri voice commands.

Allow Siri while device is locked: When this option is off, Siri is disabled when the device is locked.

Enable Siri profanity filter (Supervised Only): When this option is off, profanity isn't filtered.

Show user-generated content in Siri (Supervised Only): When this option is off, users cannot add their own content to Siri.

Allow iBooks Store (Supervised Only): When this option is off, iBooks Store is disabled, and users can't access it from the iBooks app.

Allow installing apps: When this option is off, App Store is disabled and its icon is removed from the Home screen. Users can't install or update apps using App Store or iTunes. You also can't use Apple Configurator to install apps on unsupervised devices, but you can use Apple Configurator to install apps on supervised devices.

Allow removing apps (Supervised Only): When this option is on, users can remove apps. Users can't remove apps that are included with iOS, such as App Store and iTunes.

Allow in-app purchase: When this option is off, users can't make in-app purchases.

Require iTunes password for all purchases: When this option is on, users are required to enter their Apple ID password before making any purchases. Usually, there's a brief grace period after a purchase is made before users have to authenticate for subsequent purchases.

Allow iCloud documents & data: When this option is on, users can store documents in iCloud.

Allow iCloud backup: When this option is on, users can back up their device to iCloud.

Allow automatic sync while roaming: When this option is off, devices that are roaming will sync only when an account is accessed by the user.

Allow iCloud keychain: When this option is off, the iCloud Keychain is not used.

Force encrypted backups: When this option is off, users can choose whether or not device backups performed in iTunes are stored in encrypted format on their computer. If any profile is encrypted and this option is turned on, encryption of backups is required and enforced by iTunes. Profiles installed on the device by Apple Configurator are never encrypted. Don't turn on this option when you're configuring supervised devices, because encrypted devices can't be configured in Apple Configurator. For more information about iTunes backups, see help.apple.com/iosdeployment-itunes/.

Configuration Profiles: Reference Guide

Force limited ad tracking: When this option is on, apps are not permitted to use the Advertising Identifier (a non-permanent device identifier) to serve you targeted ads.

Allow users to accept untrusted TLS certificates: When this option is off, users aren't asked if they want to trust certificates that can't be verified. This setting applies to Safari and to Mail, Contacts, and Calendar accounts.

Allow automatic updates to certificate trust settings: When this option is on, iOS devices automatically accept trust setting changes for a known, trusted certificate.

Allow installing configuration profiles (Supervised Only): When this option is off, users can't install additional configuration profiles onto their device.

Allow modifying account settings (Supervised Only): When this option is off, users can't create new accounts or change their user name, password, or other settings associated with their account.

Allow modifying Find my Friends settings (Supervised Only): When this option is off, users cannot change any settings in the Find My Friends app.

Allow pairing with non-Configurator hosts (Supervised Only): When this option is on, the device can sync with any Mac.

Allow documents from managed apps in unmanaged apps: When this option is off, documents created in managed apps cannot be opened in unmanaged apps.

Allow documents from unmanaged apps in managed apps: When this option is off, documents created in unmanaged apps cannot be opened in managed apps.

Allow sending of diagnostic and usage data to Apple: When this option is on, users can choose to send usage information.

Allow Touch ID to unlock device: When this option is off, users must use a passcode to unlock the device.

Allow Passbook notifications while locked: When this option is on, Passbook notifications are shown while the device is locked.

Show Control Center in lock screen: When this option is off, users cannot swipe up to view the Control Center.

Show Notification Center in lock screen: When this option is off, users cannot receive notifications if the screen is locked.

Show Today view in lock screen: When this option is off, users cannot swipe down to see Notification Center using the Today View in the Lock screen.

Application restrictions

Allow use of YouTube: When this option is off, the YouTube app is disabled and its icon is removed from the Home screen. This option only applies to pre-iOS 6 devices.

Allow use of iTunes Store: When this option is off, the iTunes Store is disabled and its icon is removed from the Home screen. Users can't preview, purchase, or download content.

Allow use of Game Center (Supervised Only): When this option is off, Game Center is disabled and its icon is removed from the Home screen.

Allow adding Game Center friends: When this option is off, users can't add friends in Game Center.

Allow multiplayer gaming: When this option is off, users can't play multiplayer games in Game Center.

Allow use of Safari: When this option is off, the Safari web browser app is disabled and its icon is removed from the Home screen. This also prevents users from opening web clips.

Enable autofill: When this option is off, Safari doesn't remember information users enter in web forms.

Force fraud warning: When this option is off, Safari warns users about visiting websites identified as being fraudulent or compromised.

E**nable JavaScript:** When this option is off, Safari ignores all JavaScript on websites.

Configuration Profiles: Reference Guide

Block pop-ups: When this option is off, pop-up blocking in Safari is disabled.

Accept cookies: This option sets the cookie policy in Safari. Choose to accept all cookies, accept no cookies, or reject cookies from sites not directly accessed.

Media content restrictions

Ratings region: This option lets you choose which country's ratings system to use.

Allowed content ratings: This option lets you choose the maximum rating allowed for each content type.

Allow playback of explicit music, podcasts & iTunes U media: When this option is off, explicit music or video content purchased from the iTunes Store or listed in iTunes U is hidden. Explicit content is flagged by content providers, such as record labels, when sold through the iTunes Store or distributed through iTunes U.

Allow explicit sexual content in the iBooks Store: When this option is off, explicit sexual content purchased from the iBooks Store is hidden. Explicit content is flagged by content providers when sold through the iBooks Store.

Global HTTP Proxy payload settings

Use this payload to specify a proxy for all HTTP traffic to and from the device. If you choose Manual proxy type, you need the proxy server address including its port, and optionally a user name and password for logging in to the proxy server. If you choose Auto proxy type, you can enter a proxy auto-configuration (PAC) URL.

Proxy type: Use Manual for proxies that require authentication.

Proxy server and port: Required if the proxy type is Manual.

Proxy PAC URL: Required if the proxy type is Automatic.

Authentication: The user name for the proxy server. This setting is only available for the Manual proxy type.

Password: The authentication password for the proxy server. This setting is only available for the Manual proxy type.

Allow direct connection if PAC is unreachable: When this option is turned on, the iOS device bypasses the proxy server if it's unreachable.

Allow bypassing proxy to access captive networks: When this option is turned on, the iOS device can ignore proxy settings to access a known wireless network.

Web Content Filter payload settings

Use this payload to choose which websites the device can view. You can automatically filter out adult content, and then allow or deny access to specific sites. You can also set up a device so that it can view only specific websites and create bookmarks for those websites.

When you enter URLs, start the URL with http:// or https://. If necessary, add separate entries for http:// and https:// versions of the same URL.

Allowed websites: Choose to limit browsing to non-adult content and provide a list of allowed URLs, or limit browsing to specific websites only.

Permitted URLs (for Limit Adult Content): Add URLs to this list to allow access certain websites, even if they are considered adult by the automatic filter. If you leave this list empty, access is allowed to all non-adult websites except for those listed in Blacklisted URLs.

Blacklisted URLs (for Limit Adult Content): Add URLs to this list to deny access to certain websites. Users can't visit these sites even if they are considered non-adult by the automatic filter.

Specific websites (for Specific Web Sites Only): Add the websites that you want to give access to. Enter the URL of the website in the URL column. Enter the name for the bookmark in the Name column. To create a bookmark in a folder, enter the location of the folder in the Bookmark column. For example, create a bookmark in the Favorites folder by entering /Favorites/.

Configuration Profiles: Reference Guide

Wi-Fi payload settings

iOS supports the following wireless networking security standards, as defined by the Wi-Fi Alliance:

- WEP
- Dynamic WEP
- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise

iOS also supports the following 802.1X authentication methods for WPA Enterprise and WPA2 Enterprise networks:

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- EAP-AKA
- PEAP v0, PEAP v1
- LEAP

Use the Wi-Fi settings payload to set how the device connects to your wireless network. For a user to make a connection, these settings must be specified and must match the requirements of your network. To add multiple network configurations, click the Add button (+) in the editing pane.

Service Set Identifier: Enter the SSID of the wireless network to connect to.

Hidden Network: Specify whether the network is broadcasting its identity.

Auto Join: Allow the device to automatically join the specified network. When this option is off, the user is asked to allow the connection.

Proxy Setup: Specify manual or automatic web proxy settings for this connection.

- For PAC-based auto-proxy, choose Automatic from the pop-up menu, then enter the URL of the PAC file—for example, http://www.example.com/filename.pac.
- For Web Proxy Autodiscovery (WPAD) configurations, choose Automatic from the pop-up menu. If you leave the Proxy Server URL field empty, the device will request the wpad.dat file using DHCP (via a 252 entry) or DNS (via an A Record with the name WPAD).

Security Type: Select an authentication method for the network. The following choices are available for both personal and enterprise networks.

- None: The network doesn't use authentication.
- WEP: The network uses only WEP authentication.
- WPA/WPA 2: The network uses only WPA authentication.
- Any: The device uses either WEP or WPA authentication when connecting to the network, but won't connect to non-authenticated networks.

Password: Enter the password to join the wireless network, if applicable. If you don't specify the password, the user is asked to enter it.

Enterprise settings

In this section, specify settings for connecting to enterprise networks. These settings appear when you choose an Enterprise setting from the Security Type pop-up menu.

In the Protocols pane, specify which EAP methods to use for authentication, and configure the EAP-FAST Protected Access Credential settings. After choosing an EAP method, specify sign-in settings, such as user name and authentication protocols. If you've installed an identity in the Credentials section, you can choose it from the Identity Certificate pop-up menu.

In the Trust pane, specify which certificates should be trusted to validate the authentication server for the Wi-Fi connection. The Trusted Certificates list shows certificates that have been added using the Credentials pane, and lets you select which certificates are trusted. Add the names of the authentication servers to be trusted to the Trusted Server Certificates Names list. You can specify a particular server, such as server.mycompany.com, or a partial name such as *.mycompany.com.

Passpoint: Configure the device so it can connect to network access points using Hotspot 2.0, or other Passpoint technologies.

Configuration Profiles: Reference Guide

VPN payload settings

Use this payload to enter the VPN settings for connecting to your network. You can add multiple VPN configurations by clicking the Add button (+). Settings you specify in the configuration profile can't be modified by the user.

For information about supported VPN protocols and authentication methods, see VPN Server Configuration for iOS Devices. The options available vary based on the protocol and authentication method you select.

To configure F5 SSL, Juniper SSL, Cisco AnyConnect, or Aruba VIA, choose the appropriate item from the Connection Type pop-up menu. Make sure that the Realm and Role (Juniper) or Group (Cisco) values match those specified on the VPN server. Users must install both the configuration profile and the appropriate authentication app. F5 BIG-IP Edge Client, Junos Pulse, Cisco AnyConnect, and Aruba Network VIA apps are available from the App Store.

For other SSL VPN solutions, contact your vendor and ask if they have an app in the App Store. If they do, choose Custom SSL from the Connection Type pop-up menu, then enter the configuration information provided by the vendor. Make sure the Identifier field matches the identifier specified by your vendor's VPN app and is in reverse DNS format (for example, com.example.myvpn). Your users must install both the vendor's app and the configuration profile to connect to your network.

VPN on demand

For certificate-based and SSL configurations, you can turn on VPN On Demand so that a VPN connection is automatically established when accessing certain domains. The VPN On Demand options are:

Always: Establishes a VPN connection for any address that matches the specified domain.

Never: Doesn't establish a VPN connection for addresses that match the specified domain, but if VPN is already active, it can be used.

Establish if needed: Establish a VPN connection for addresses that match the specified domain, after a failed DNS lookup occurs.

The action applies to all matching addresses. Addresses are compared using simple string matching, starting from the end and working backward. The address ".example.org" matches "support.example.org" and "sales.example.org," but doesn't match "www.private-example.org." However, if you specify the match domain as "example.com"—notice there isn't a period at the beginning—it matches "www.private-example.com" and all the others.

LDAP connections don't establish a VPN connection; if the VPN connection hasn't already been established by another app such as Safari, the LDAP lookup fails.

The device closes a VPN session established by VPN On Demand after two minutes of inactivity. If the connection was established manually using the Settings app, the VPN server's timeout applies.

VPN proxy

iOS supports manual VPN proxy and automatic proxy configuration using PAC or WPAD. To specify a VPN proxy, choose an option from the Proxy Setup pop-up menu.

PAC-based auto-proxy configuration: Choose Automatic from the pop-up menu, then enter the URL of a PAC file.

Web Proxy Autodiscovery (WPAD) configuration: Choose Automatic from the pop-up menu. Leave the Proxy Server URL field empty, and iOS will request the WPAD file using DHCP and DNS.

AirPlay Mirroring payload settings

Use this payload to preconfigure passwords for AirPlay Mirroring destinations and list allowed destinations for the device.

Passwords: Configure the device with passwords for password-protected AirPlay destinations users can connect to. Because you enter passwords here, you can minimize the number of people who need to know the passwords. When you add a destination, you can add destinations found by Bonjour, or other destinations that you know the name and password for. The Discoverable list shows all the destinations the computer with Apple Configurator can find using Bonjour. If the destination you want to save a password for is listed, select it, then enter the device's password. If the destination

you want to save a password for is not listed, select Undiscoverable, then enter the device's name and password.

Whitelist: Add the MAC address of devices to this list to allow AirPlay mirroring to only these devices. If this list is empty, the device can connect with any destination.

AirPrint payload settings

Use this payload to choose which AirPrint printers pre-populate the list of available printers for a device.

To add printers, click the Add button (+). When you add a printer, you can add printers found by Bonjour, or other printers that you know the IP address and resource path for. The Discoverable list lists all printers the computer with Apple Configurator can find using Bonjour. If the printer you want to use is listed, select it. If the printer you want to use is not listed, select Undiscoverable, then enter the device's IP address.

Mail payload settings

Use this payload to configure POP or IMAP mail accounts for users. iOS supports industry-standard IMAP4 and POP3 mail solutions on a range of server platforms, including OS X, Windows, UNIX, and Linux.

You can add multiple mail accounts by clicking the Add button (+).

Account settings

Users can modify some of the mail settings you provide in a profile, such as the account name, password, and alternative SMTP servers. If you omit this information from the profile, users are asked to enter it when they access the account.

Privacy settings

Allow user to move messages from this account: When this option is off, email messages cannot be moved between mail accounts.

Allow Recent Address syncing: When this option is off, recently used addresses are not synced across devices.

Use Only in Mail: When this option is off, users can use any mail app to send email.

Enable S/MIME: When this option is off, S/MIME is disabled.

Exchange ActiveSync payload settings

Use this payload to enter the user's settings for your Microsoft Exchange server. You can create a profile for a particular user by specifying the user name, host name, and email address, or you can provide just the host name—users are prompted to fill in the other values when they install the profile.

You can configure multiple Exchange accounts by clicking the Add button (+). If you select the Use SSL option, use the Credentials pane to add any root or intermediate certificates that are necessary to validate the server's SSL certificate. To provide a certificate that identifies the user to the Exchange ActiveSync server, choose one from the Authentication Credential pop-up menu. The Authentication Credential pop-up menu lists your Credentials payloads.

For information about requirements and supported features, see the Exchange ActiveSync and iOS Devices website.

Privacy settings

Allow user to move messages from this account: When this option is off, email messages cannot be moved between mail accounts.

Allow Recent Address syncing: When this option is off, recently used addresses are not synced across devices.

Use Only in Mail: When this option is off, any apps able to send email can be used.

Enable S/MIME: When this option is off, S/MIME is disabled.

Configuration Profiles: Reference Guide

LDAP payload settings

iOS devices retrieve contact information from your company's LDAPv3 server's corporate directories. You can access LDAP directories when searching in Contacts, and the info there is used to automatically complete email addresses as you enter them.

Use this payload to enter settings for connecting to an LDAPv3 directory. You can specify multiple search bases for each directory. You can configure multiple directory connections by clicking the Add button (+).

If you select the Use SSL option, use the Credentials pane to add any root or intermediate certificates that are necessary to validate the server's SSL certificate.

Calendar payload settings

iPad, iPhone, and iPod touch sync calendar data with your company's CalDAV server. Changes to the calendar are periodically updated between the device and the server.

Use this payload to provide account settings for connecting to a CalDAV-compliant calendar server. These accounts will be added to the device. As with Exchange accounts, users need to manually enter information you omit from the profile, such as their account password, when the profile is installed.

If you select the Use SSL option, add Certificate payloads to add any root or intermediate certificates that are necessary to validate the server's SSL certificate.

To configure multiple CalDAV accounts, click the Add button (+).

Contacts payload settings

iOS devices retrieve contact information from your company's CardDAV contact list. You can access CardDAV directories when searching in Contacts, and they're automatically used to complete email addresses as you enter them.

Use this payload to provide account settings for connecting to a CardDAV-compliant contact server. If you omit the account information, users need to enter it manually when the profile is installed.

If you select the Use SSL option, add Certificate payloads to add any root or intermediate certificates that are necessary to validate the server's SSL certificate.

To configure multiple CardDAV accounts, click the Add button (+).

Subscribed Calendars payload settings

Use this payload to add read-only calendar subscriptions to the device's Calendar app. To configure multiple subscriptions, click the Add button (+).

A list of public calendars you can subscribe to is available on the iCal Calendar Downloads website.

If you select the Use SSL option, use the Credentials pane to add any root or intermediate certificates that are necessary to validate the server's SSL certificate.

Web Clips payload settings

Use this payload to add web clips to the Home screen of the user's device. Web clips provide fast access to favorite webpages or links. For example, add a web clip with a phone number (in the format tel://18006927753), to provide a quick way to dial your support desk. To add multiple web clips, click the Add button (+).

If you choose to prevent the user from removing the web clip, it cannot be deleted from the device without removing the configuration profile that installed it.

To add a custom icon, select a graphics file in GIF, JPEG, or PNG format. For best results, provide a square image that's no larger than 400 x 400 pixels and less than 1 MB when uncompressed. The graphics file is automatically scaled and cropped to fit, if necessary, and converted to PNG format. Web clip icons are 144 x 144 pixels for iPad devices with a Retina display, and 114 x 114 pixels for iPhone devices. To prevent the device from adding a shine to the image, choose Precomposed Icon.

A full-screen web clip opens the URL as a web app without a browser (there's no URL or search bar, or bookmarks).

Configuration Profiles: Reference Guide

Font payload settings

Use this payload to add fonts to the user's device so that apps can use the fonts.

To add multiple fonts, click the Add button .

Certificates payload settings

iOS devices can use X.509 certificates with RSA keys. The file extensions .cer, .crt, and .der are recognized.

Use this payload to add certificates and identities to the device. Certificates in PKCS1 and PKCS12 format are supported. Use P12 (PKCS #12 standard) files that contain exactly one identity. The file extensions .p12 and .pfx are recognized. When an identity is installed, the user is prompted for the passphrase that protects it, unless you include the passphrase in the payload.

When you install certificates, also install the intermediate certificates that are necessary to establish a chain to a trusted certificate that's on the device. To view a list of the preinstalled roots, see the Apple Support article iOS: List of available trusted root certificates.

If you include the certificate passphrase in the payload, you should encrypt the configuration profile when you export it. If you omit the passphrase, the user is asked to enter it when the profile is installed.

If the certificate or identity that you want to install is in your keychain, use Keychain Access to export it in .p12 format. Keychain Access is located in /Applications/Utilities/. For more information, see Keychain Access Help, available from the app's Help menu.

Instead of installing certificates using a configuration profile, you can let users use Safari to download the certificates to their device from a webpage. Or, you can email certificates to users. You can also use the SCEP settings, described below, to specify how the device obtains certificates when the profile is installed.

SCEP payload settings

Use this payload to specify settings that allow the device to obtain certificates from a Certificate Authority (CA) using Simple Certificate Enrollment Protocol (SCEP).

URL: The address of the SCEP server.

Name: This can be any string that's understood by the CA. It can be used to distinguish between instances, for example.

Subject: The representation of an X.500 name represented as an array of OID and value. For example, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, which translates to: [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]

Subject Alternative Name: Specify the type and value of an alternative name for the SCEP server. Valid values are an email address (RFC-822), the DNS name of the server, or the server's fully-qualified URL.

NT Principal Name: An NT principal name for use in the certificate request.

Retries: The number of times to poll the SCEP server for a signed certificate before giving up.

Retry Delay: The number of seconds to wait between poll attempts.

Challenge: A pre-shared secret the SCEP server can use to identify the request or user.

Key Size and Usage: Select a key size, and—using the checkboxes below this field—the acceptable uses of the key.

Fingerprint: If your CA uses HTTP, use this field to provide the fingerprint of the CA's certificate, which the device uses to confirm the authenticity of the CA's response during the enrollment process. You can enter a SHA1 or MD5 fingerprint, or select a certificate to import its signature.

APN payload settings

Use this payload to change the device's Access Point Name (APN) and cell network proxy settings. These settings define how the device connects to the carrier's network. Change these settings only if instructed to do so by a carrier network expert. If these settings are incorrect, the device can't access data using the cellular network. To undo a change to these settings, remove the profile from the device.

iOS supports APN user names and passwords of up to 64 characters.