



How to use the Mac OS X Configuration Profile dialog in the Configuration Manager console

- Parallels Device Management

Information

The Mac OS X Configuration Profile dialog can be used to create and edit SCCM configuration items that allow you to deliver Mac OS X Configuration Profiles to managed Macs.

The dialog mimics the interface of the Mac OS X Server's Profile Manager. The left pane of the dialog contains the list of payloads that define groups of settings. The right pane contains the settings for a selected payload. Once you configure Mac OS X system preferences and close the dialog, the preferences are saved in the profile and can then be used to configure Mac computers using the Desired Configuration Management functionality. You can read more about Desired Configuration Management in the [Parallels Mac Management for Microsoft SCCM 2012 administrator's guide](#).

Please note that Parallels Mac Management v5.0 supports a limited set of available payloads. The lists below describe the supported and unsupported payloads.

The following list contains payloads that are supported and can be configured using the Mac OS X Configuration Profile dialog:

- Passcode. Specifies passcode policies.
- Exchange. Exchange account configuration.
- Dock. Dock item settings. Dock appearance settings.
- Contacts. Contacts LDAP configuration (CardDAV).
- Calendar. Calendar server account configuration (CalDAV).
- Network. Network connections settings (Ethernet or Wi-Fi).

Note: The Network payload is not fully implemented in Parallels Mac Management version 4.5. Specifically, when choosing one of the enterprise-level security types (the Security Type option), the corresponding certificate lists will be disabled, so you cannot select a certificate.

- Certificate. X.509 certificates.
- Security & Privacy. Usage and diagnostic information opt-out.

The following list contains payloads that are currently not supported and cannot be configured using the dialog (these payloads will be implemented in the future Parallels Mac Management releases):

- Mail
- LDAP
- VPN
- SCEP
- Web Clips
- Restrictions

If you want to configure an unsupported payload, you can use an alternative approach. You can create a configuration profile using the Mac OS X Server's Profile Manager, save it to a file, and then create an SCCM configuration item from this file. For more information about Profile Manager, please visit this

page:

<http://www.apple.com/support/lionserver/profilemanager/>

To create a Mac OS X configuration profile from file:

1. Use Profile Manager to configure the Mac OS X settings and save them as a ?.mobileconfig? file. Copy the created file to a computer where it can be accessed from the Configuration Manager console.
 2. Depending on the SCCM version you are using, do the following:
 - ◆ In the Configuration Manager 2012 console, navigate to Assets and Compliance / Overview / Compliance Settings. Right-click Configuration Items. In the pop-up menu, point to Create Parallels Configuration Item and then click Mac OS X Configuration Profile from File. The Mac OS X Configuration Profile dialog opens.
 - ◆ In the Configuration Manager 2007 console, navigate to Site Database / Computer Management / Desired Configuration Management / Configuration Items. Right-click Configuration Items. In the pop-up menu, point to Create Parallels Configuration Item and then click Mac OS X Configuration Profile from File. The Mac OS X Configuration Profile dialog opens.
 3. Click the Browse button and select the ?.mobileconfig? file that you've created earlier using Profile Manager. This will embed the settings from the file in the configuration item.
 4. Type a name and an optional description and select the desired configuration profile type. Click OK to save the configuration item.
-

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.