pradeo

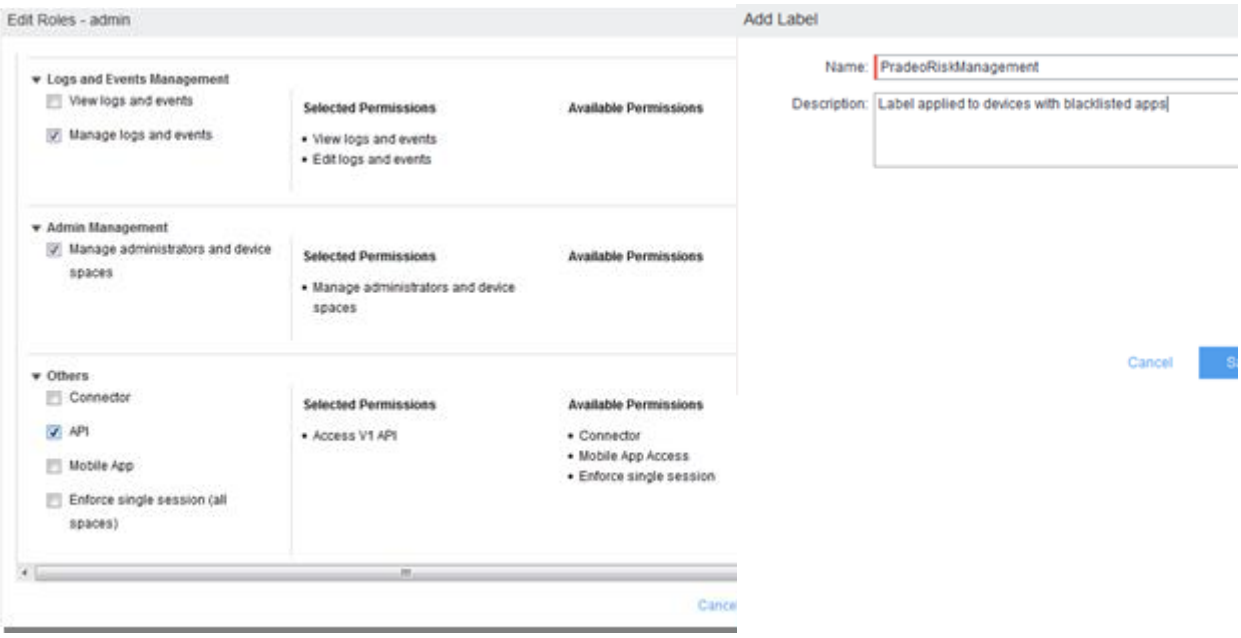
Pradeo Security for MobileIron Solution Guide

TABLE OF CONTENTS

Contents

1. Preconfiguration on MobileIron

On the MobileIron console, a user with API privileges and a “PradeoRiskManagement” label must be created. It will be applied on all devices where at least one blacklisted app is installed. Please refer to the MobileIron documentation for more details about how to manage users’ privileges, and how to create a label.



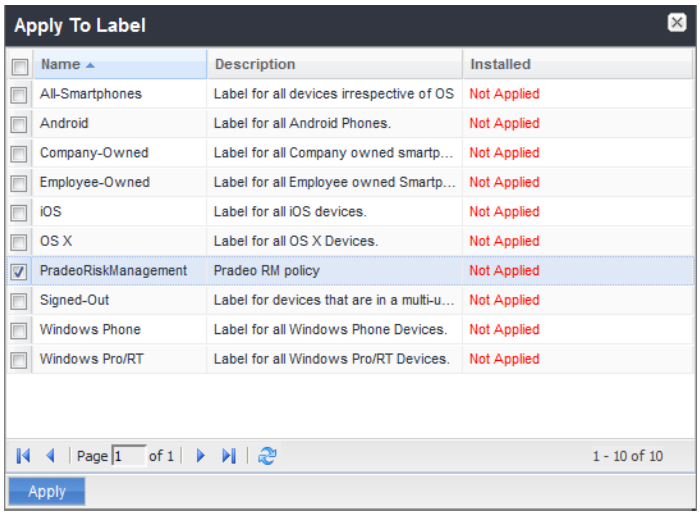
2. Connect the MobileIron server to the Pradeo Security server

On the Pradeo Security console, open the menu and go to Administration – Enterprise Mobility Management then click on the MobileIron logo. A frame asks you for the REST API URL and credentials that you can find on the MobileIron console.

After saving credentials by clicking on « save », all apps installed on devices are automatically retrieved by Pradeo thanks to their name and version. They are automatically analyzed. The security policy can be defined on the “Applications’ validation policy” page by simply setting up the alert level for all behaviors that can be detected by Pradeo. Apps are also added to the “Applications analysis” page on Pradeo Security’s console.

	Name	Version	Category	Installation date	Policy	Approved
	AndroidTestApplication	2	-	June 22 2015 14:30:19	Notify & forbid	✖
	CheckMyApps	1.4	Tools	June 22 2015 14:30:19	Free use	✔
	Chrome	42.0.2311.111	Communication	June 22 2015 14:30:19	Free use	✔

Devices are added in the “Users administration” section. On the page of a user, all the apps are visible, with a colored indicator showing if the app is whitelisted (green) or blacklisted (red).



The “PradeoRiskManagement” Label is deployed on all devices with at least one blacklisted app installed. Any security policy defined on MobileIron console can be linked to this label and applied on all matching devices.

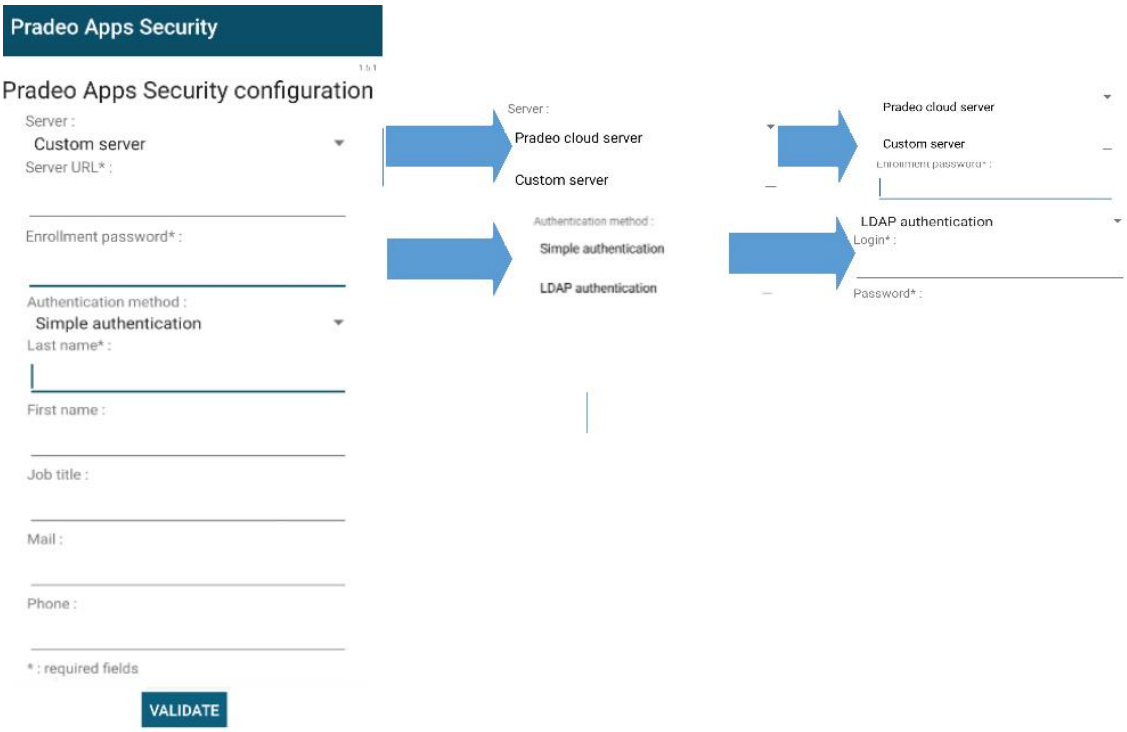
3. Enrollment

1.1 Android

Pradeo Apps Security: application that manages the global functionalities of the solution on the Android OS and, more importantly, the connection to the Pradeo Security administration server from which it downloads the latest security policy.

Pradeo Browser: secured web-browser for Android. It replaces the default browser and blocks the access to websites that are blocked or black-listed by the administrator for the specific group to which the device is assigned to. The usage of the browser may be made optional in the options (Security, URL Filtering, Browser policy), though the installation of the app remains mandatory

Once you have downloaded and installed the first one (the order has no importance) by launching it, you will be automatically prompted to download the second one too.



The user is requested to fill in the following information:

- Server's address: (mandatory) - IP or domain name on which the Pradeo Security server can be reached. (IP address preconfigured if Pradeo Cloud is selected)
- Client Password: (mandatory) – allows linking a device with a client.
- Authentication method:

  LDAP Authentication:

  - Login (mandatory): your LDAP login
  - Password (mandatory): your LDAP password

  Simple Authentication:

  - Last Name: (mandatory) – your last name or the name of the device
  - First name: optional
  - Function: optional
  - E-mail: optional
  - Telephone number: optional.

If you want to link this device with an LDAP user (the LDAP server must be configured on the interface), select the LDAP authentication method and enter your LDAP credentials.

Once you typed all mandatory information, click on « Validate ». The device will try to enroll on server. Once the enrollment request is sent, the message « Data successfully saved, waiting for administrator approval » will confirm the process is on the way, waiting for the administrator's approval.

In case the device has been pre-approved by the administrator, the enrollment does not require any action from the administrator in order to finalize the process.

When the enrollment process is finalized, the message « Service configured » will be displayed in the notifications bar. Then the agent will download and apply the security policy for its group and sent to the server the list of all applications installed on the device.

Note: In order to use the MDM functionalities on the device, it is necessary to activate the option « Device Administrator ». If this option is not activated on the device, the user will be invited to check this option in order to have the best level of protection.

1.2 iOS

The Pradeo Apps Security agent available on the Apple AppStore requires an enrollment on the platform, and the installation of an MDM profile. As a consequence, this agent cannot be installed on a device already managed by MobileIron.

A private agent can be installed, to display security information about your apps.

Do not hesitate to ask us for this agent!