Workspace ONE UEM Integration with OpenTrust CMS Mobile 2

VMware Workspace ONE UEM 1902

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Workspace ONE UEM Integration with OpenTrust CMS Mobile 2

1

Workspace ONE UEM is flexible in PKI integration approach by being able to request certificates from internal or external certificate authorities. This documentation explains how to incorporate OpenTrust CMS Mobile 2.0 services to issue certificates for your Workspace ONE UEM MDM solution.

This chapter includes the following topics:

- System Requirements
- High Level Design

System Requirements

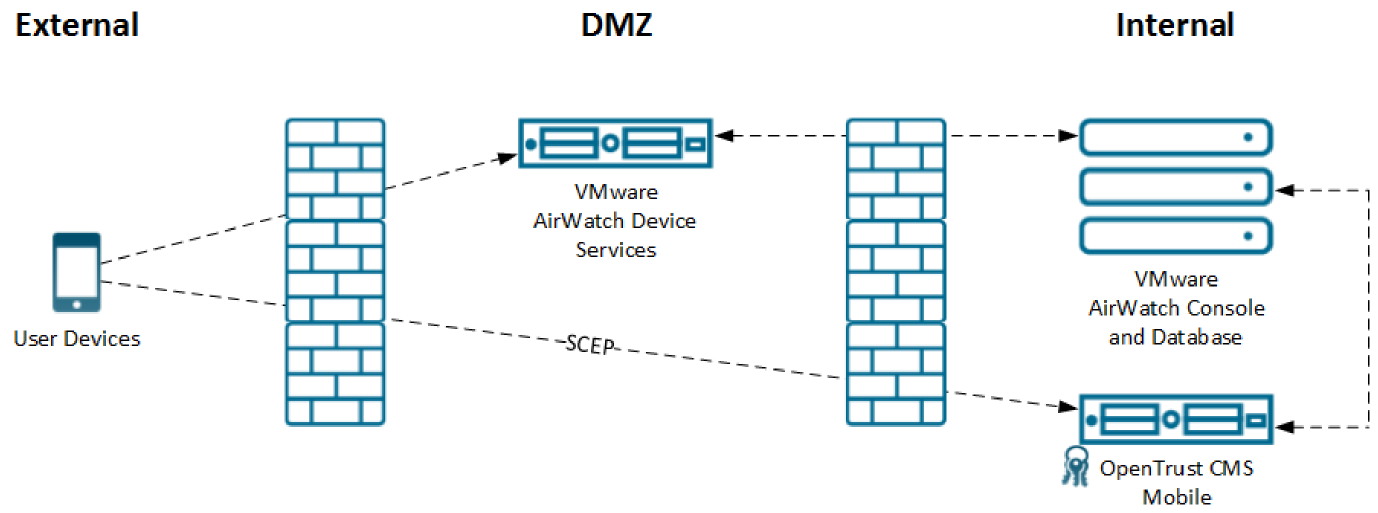
The following tasks must be completed before proceeding with the steps outlined in this documentation.

- An OpenTrust CMS Mobile 2.0 instance needs to be available. Contact your OpenTrust administrator to obtain a digital identity configured with appropriate rights for configuration.
- Workspace ONE UEM version 8.0 or greater.
- AirWatch Cloud Connector is required if the OpenTrust CMS instance is installed behind a firewall.

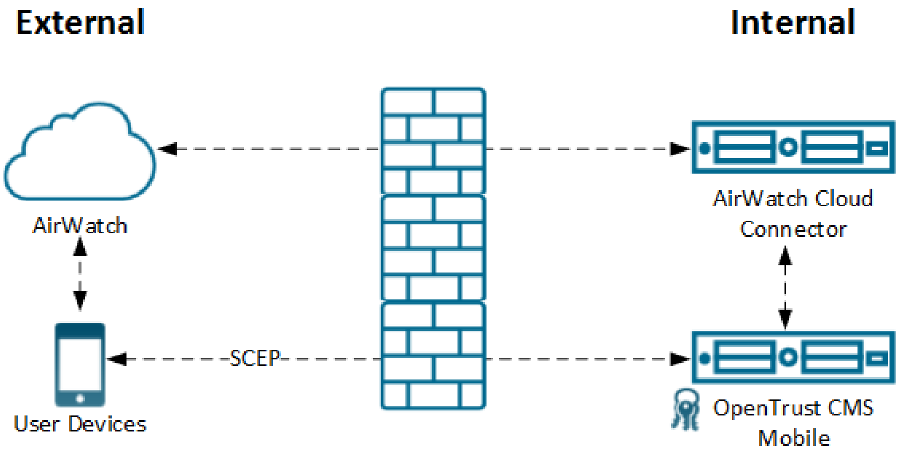
High Level Design

OpenTrust CMS Mobile 2.0 can be used as a third-party certificate authority for Workspace ONE UEM in multiple configurations and environments. These diagrams highlight the four major examples of a communications flow between OpenTrust, Workspace ONE UEM, and mobile devices.

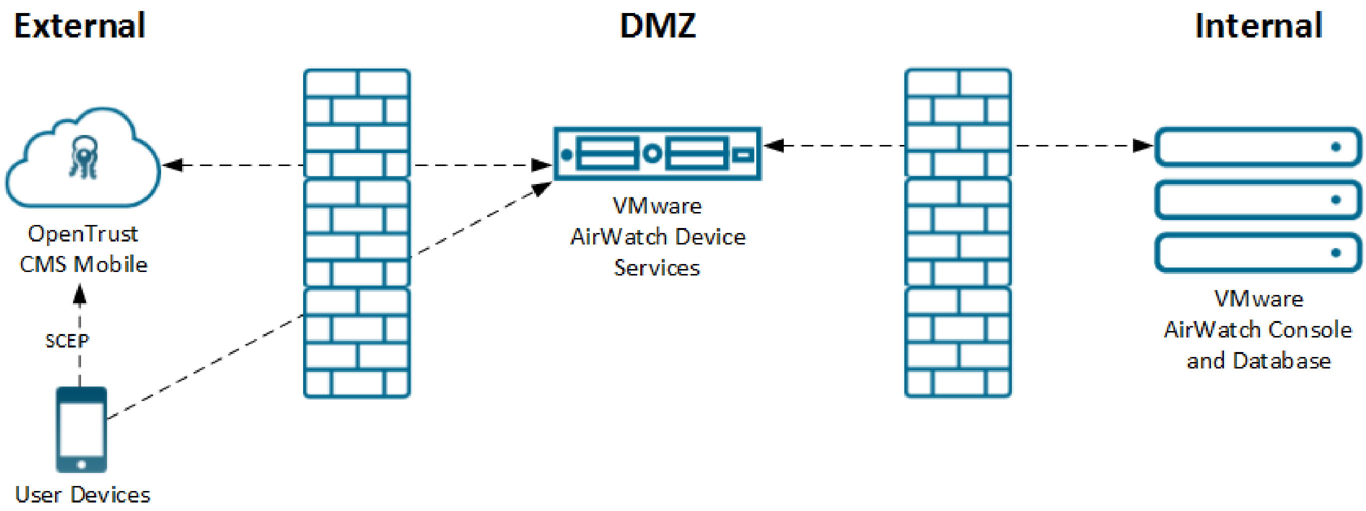
OpenTrust and Workspace ONE UEM Configured Internally


External
DMZ
Internal
VMware AirWatch Device Services
VMware AirWatch Console and Database
User Devices
SCEP
OpenTrust CMS Mobile

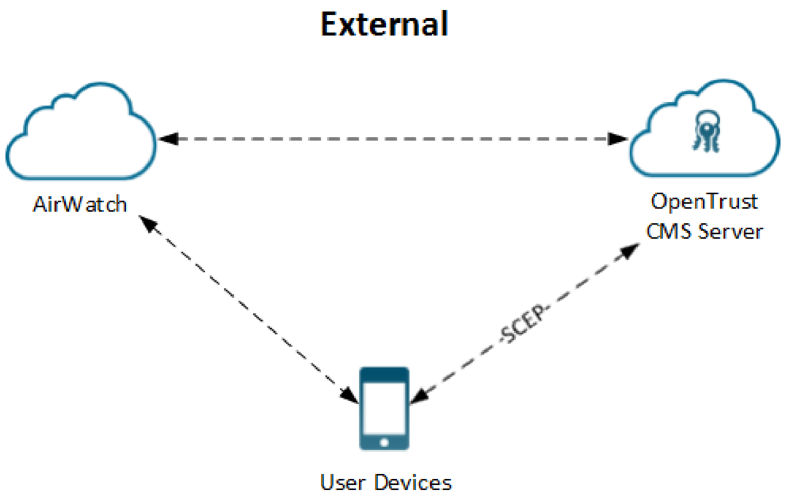
Workspace ONE UEM Cloud with OpenTrust On Premises



OpenTrust Cloud with Workspace ONE UEM On Premises


External
DMZ
Internal
OpenTrust CMS Mobile
SCEP
User Devices
VMware AirWatch Device Services
VMware AirWatch Console and Database

Both OpenTrust and Workspace ONE UEM Configured Externally



Install, Set Up, Configure Certificate

2

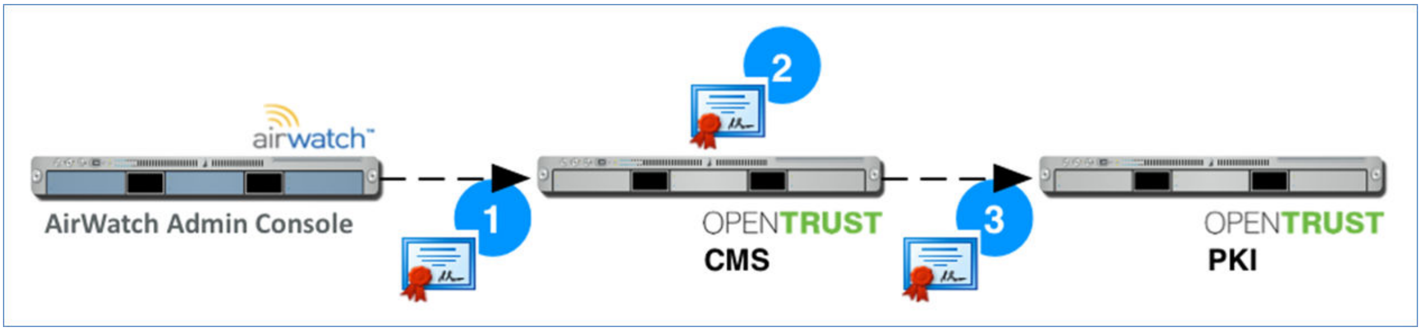
This section provides instructions to configure the certificate authority (CA) of your choice to work with the Workspace ONE ™ UEM console.

Take the following steps and procedures to integrate the certificate.

This chapter includes the following topics:

Step 1: Obtain Certificates for Communication with OpenTrust CMS Mobile

After OpenTrust CMS Mobile has been installed, either in your on-premises environment or available from a provider's cloud, you will receive a connection URL and three identities contained in password-protected PKCS#12 (.PFX or .P12) files. These identities are illustrated and explained below.



1 One identity is meant for communication between Workspace ONE UEM and OpenTrust CMS Mobile, hereafter referred to as "CMS JSON Connector".

2 One identity is meant for OpenTrust CMS Mobile administration, hereafter referred to as "CMS Admin".

3 One identity is meant for communication between OpenTrust CMS Mobile and OpenTrust PKI, hereafter referred to as "PKI SOAP Connector".

These identities must have been configured by the CMS administrator with appropriate rights for each task.

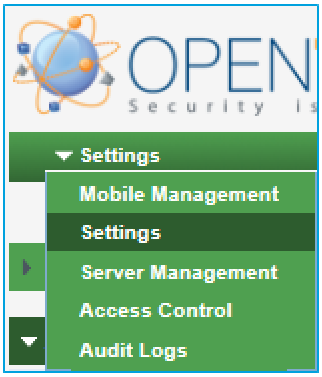
You only need to integrate the CMS Admin identity into your browser, the two other PKCS#12 files need to remain available later for configuration. Check your browser's documentation about integrating a digital identity if needed.

Step 2: Configure a Workspace ONE UEM Datasource in OpenTrust CMS Mobile

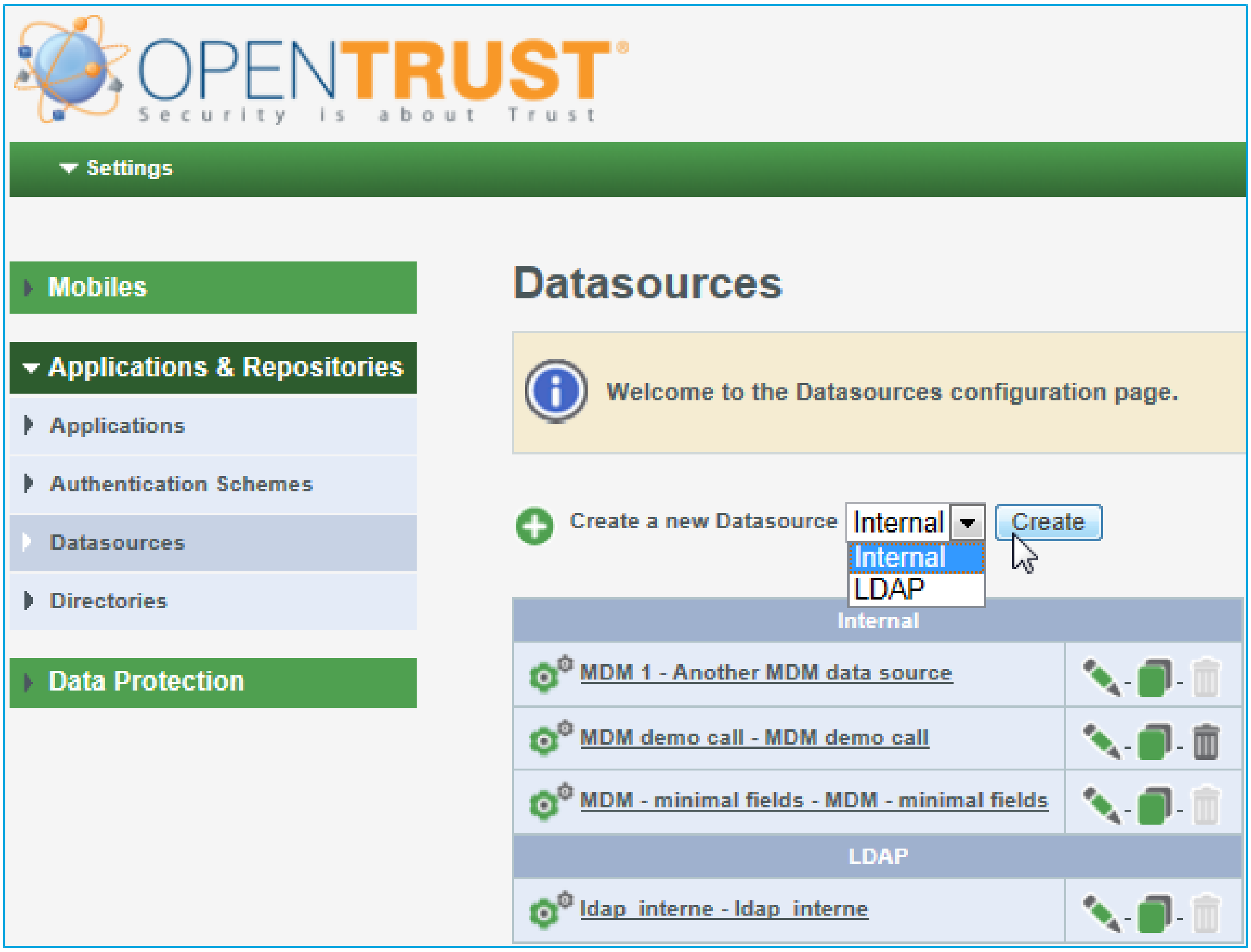
The first step is to configure an internal data source in CMS Mobile to store incoming data from Workspace ONE UEM.

1 Connect to the OpenTrust CMS Mobile using an administrator identity.

2 If the OpenTrust application does not open on the **Settings** page, select the drop-down arrow on the top, left corner of the dashboard and select **Settings** from the drop-down list.



3 Navigate to **Datasources** by selecting **Applications & Repositories > Datasources**. The **Datasources** screen displays.



Welcome to the Datasources configuration page.

Create a new Datasource: Internal

Internal

MDM 1 - Another MDM data source

MDM demo call - MDM demo call

MDM - minimal fields - MDM - minimal fields

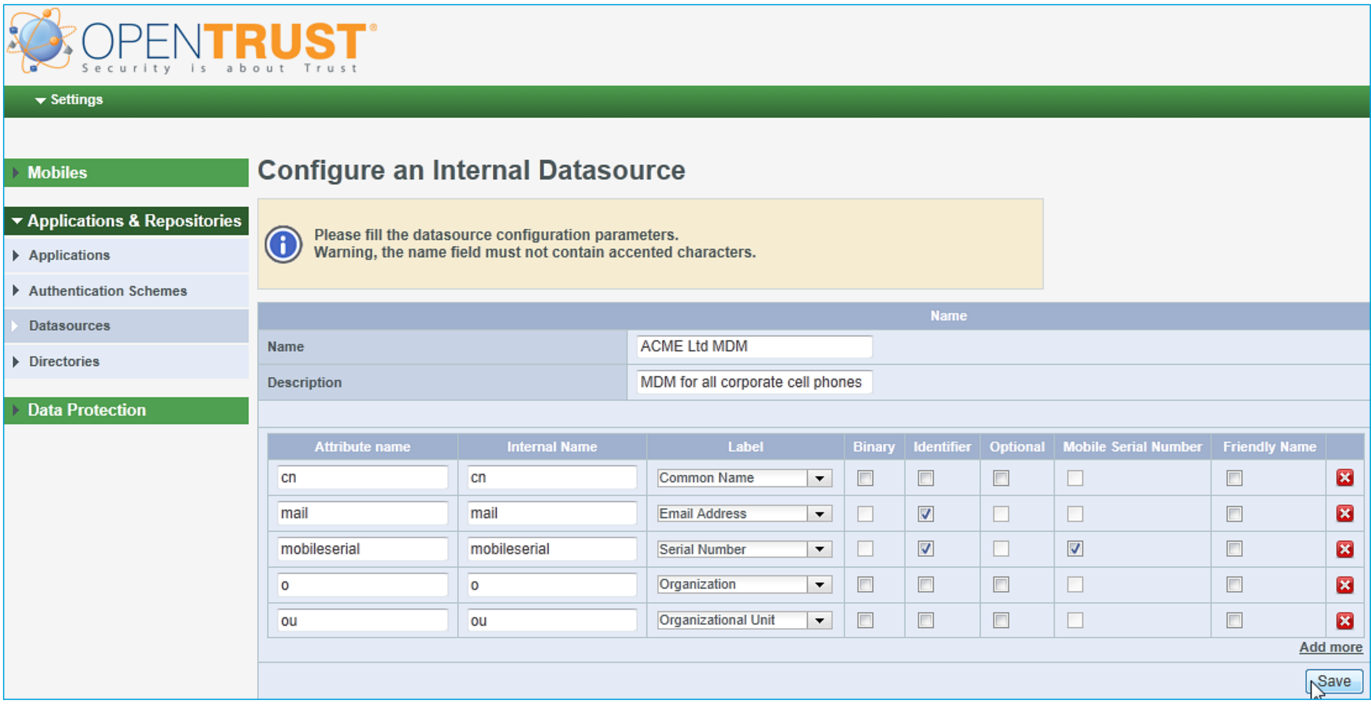
LDAP

ldap_interne - ldap_interne

4 Click on the **Create a new Datasource** drop-down and select Internal.

5 Click on the **Create** button. The **Configure an Internal Datasource** window displays. The field names will be the ones received from Workspace ONE UEM during each enrollment. The ones listed below are typical examples; the ones you want should have been decided in the previous step.

These fields will be displayed in the Workspace ONE UEM console later when performing the integration.



Configure an Internal Datasource

Please fill the datasource configuration parameters.
Warning, the name field must not contain accented characters.

Name	
Name	ACME Ltd MDM
Description	MDM for all corporate cell phones

Attribute name	Internal Name	Label	Binary	Identifier	Optional	Mobile Serial Number	Friendly Name	
cn	cn	Common Name	□	□	□	□	□	☒
mail	mail	Email Address	□	☑	□	□	□	☒
mobileserial	mobileserial	Serial Number	□	☑	□	☑	□	☒
o	o	Organization	□	□	□	□	□	☒
ou	ou	Organizational Unit	□	□	□	□	□	☒

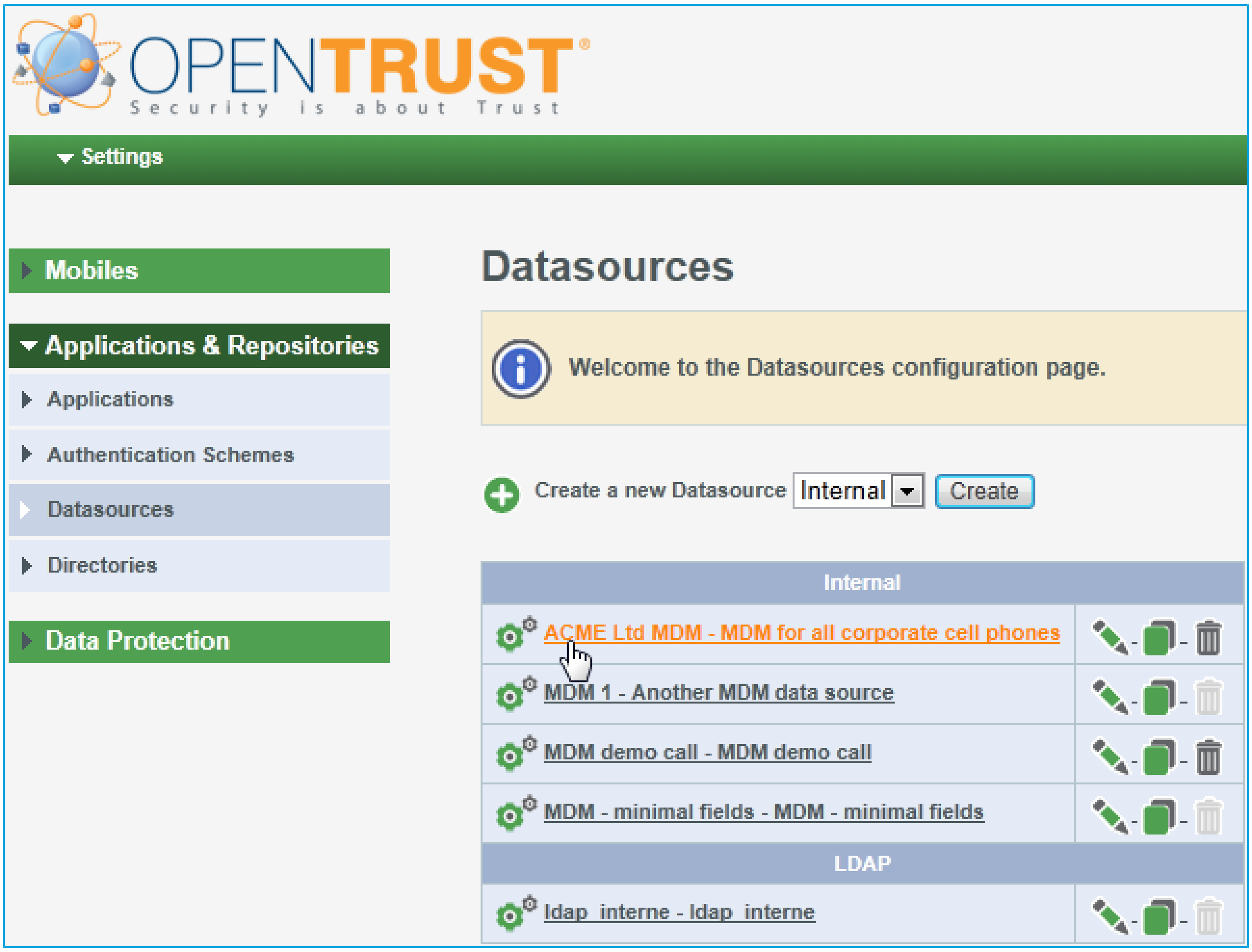
Add more

Save

6 Enter a **Name** and **Description** for the new Datasource.

7 Enter an **Attribute name**, **Internal Name**, and select a **Label** from the drop-down list that matches the **Mandatory Fields** you will be configuring in Step 6: Set Up Certificate Template for OpenTrust CA Type.

8 Click on **Save**. The new Datasource is added to the **Internal** list as shown in the screen below.



Datasources

Welcome to the Datasources configuration page.

Create a new Datasource Internal Create

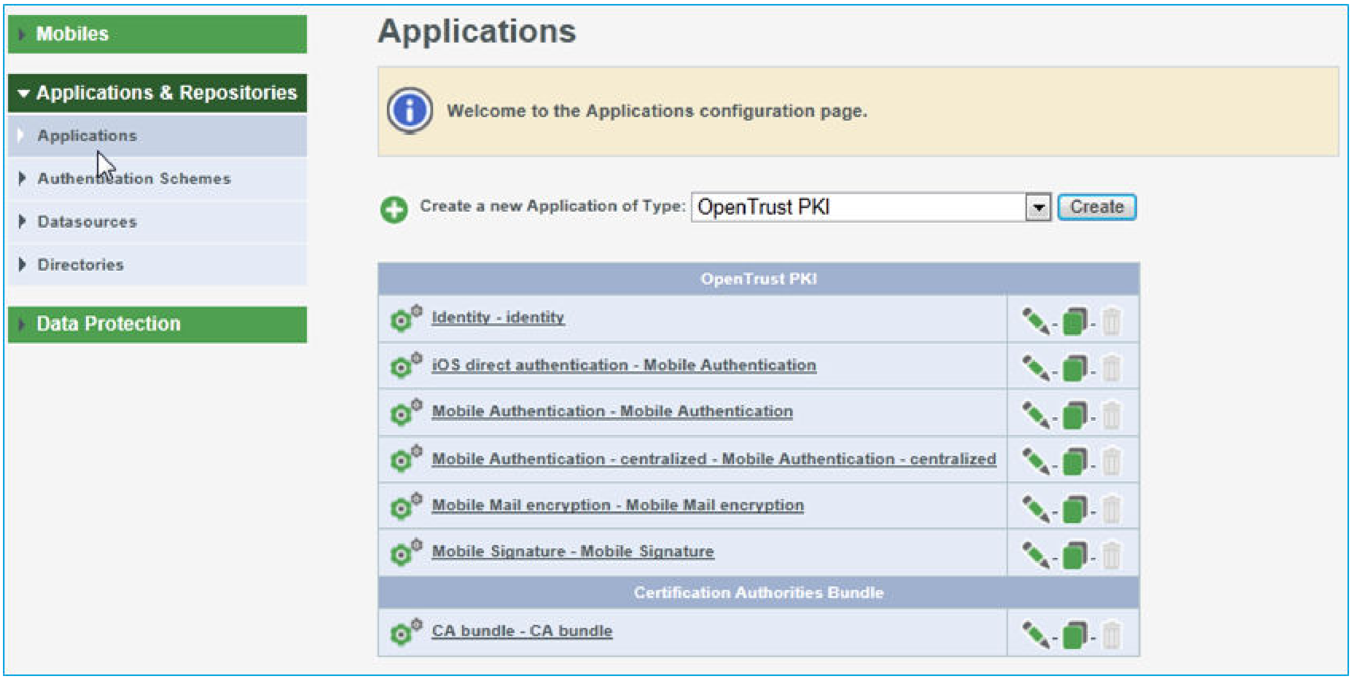
Internal
ACME Ltd MDM - MDM for all corporate cell phones
MDM 1 - Another MDM data source
MDM demo call - MDM demo call
MDM - minimal fields - MDM - minimal fields
LDAP
ldap_interne - ldap_interne

Further information about configuring datasources is available from OpenTrust's documentation.

Step 3: Configure the OpenTrust CMS Mobile Application

After you set up the Datasource, you need to configure the OpenTrust Application to point to the Datasource. In this very specific context, an Application refers to a digital credential, for example, an X. 509 certificate.

1 Click on **Applications & Repositories > Applications** to navigate to the **Applications** screen.



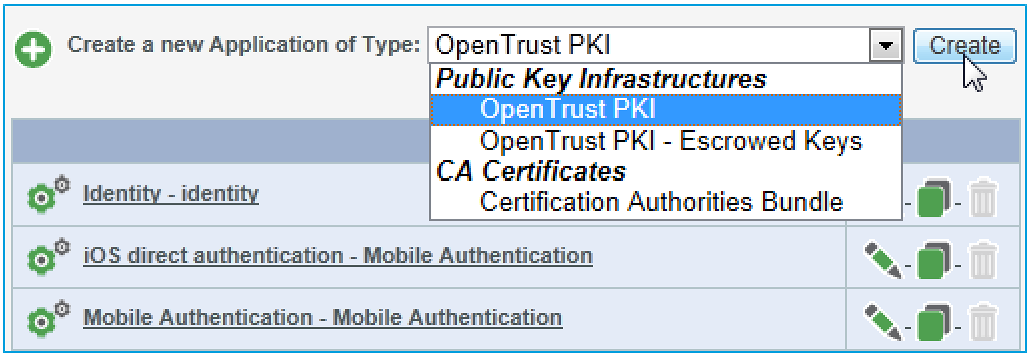
Applications

Welcome to the Applications configuration page.

Create a new Application of Type: OpenTrust PKI

OpenTrust PKI
Identity - identity
iOS direct authentication - Mobile Authentication
Mobile Authentication - Mobile Authentication
Mobile Authentication - centralized - Mobile Authentication - centralized
Mobile Mail encryption - Mobile Mail encryption
Mobile Signature - Mobile Signature
Certification Authorities Bundle
CA bundle - CA bundle

2 Click on the **Create a new Application of Type:** drop-down arrow and **OpenTrust PKI**, **OpenTrust PKI – Escrowed Keys**, and **Certificate Authorities Bundle** displays the available selections. These are three different ways to configure the Application Type. This documentation covers OpenTrust PKI and Certification Authorities Bundle. OpenTrust PKI Escrowed Keys is configured in a similar fashion.



Create a new Application of Type: OpenTrust PKI

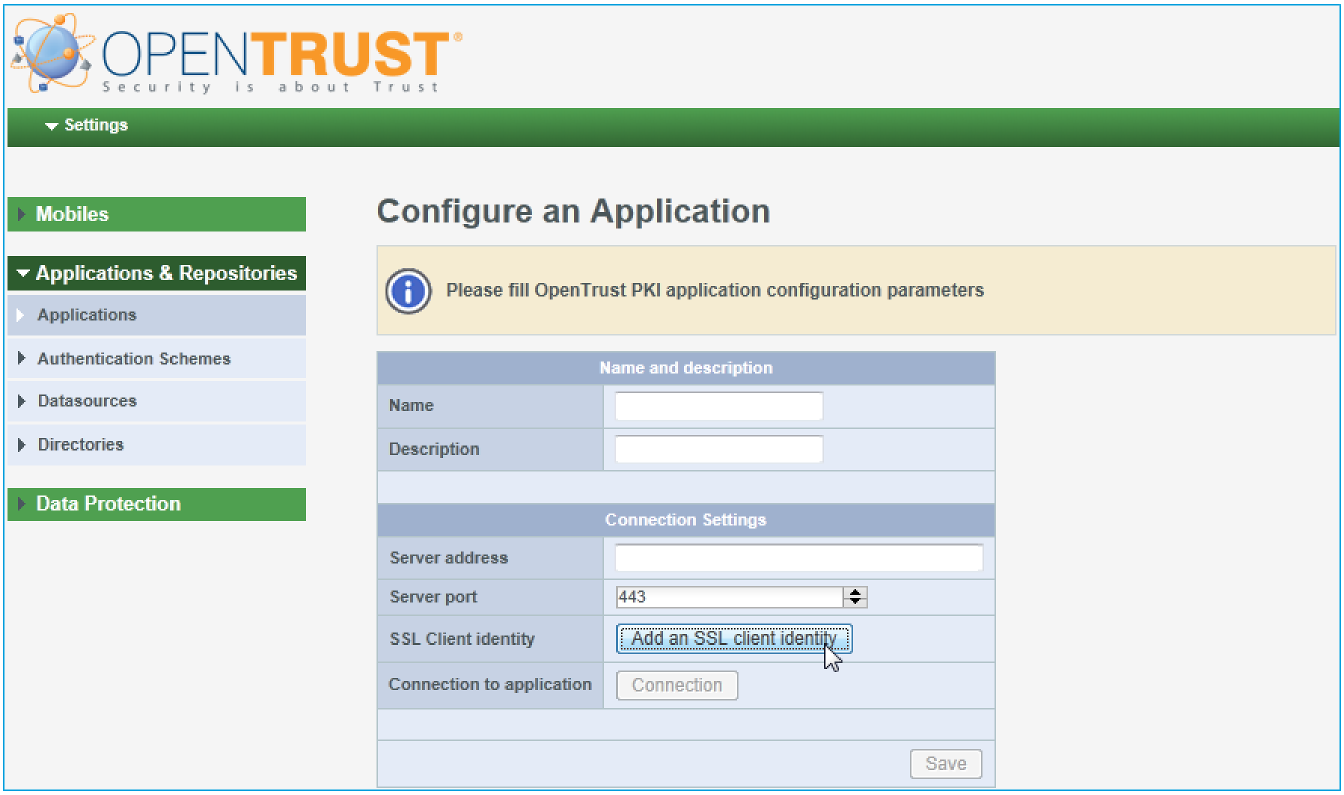
Public Key Infrastructures
OpenTrust PKI
OpenTrust PKI - Escrowed Keys
CA Certificates
Certification Authorities Bundle

Identity - identity
iOS direct authentication - Mobile Authentication
Mobile Authentication - Mobile Authentication

Select the OpenTrust PKI Application Type

1 Select **OpenTrust PKI** from the drop-down.

2 Click **Create**. The **Configure an Application** window appears.



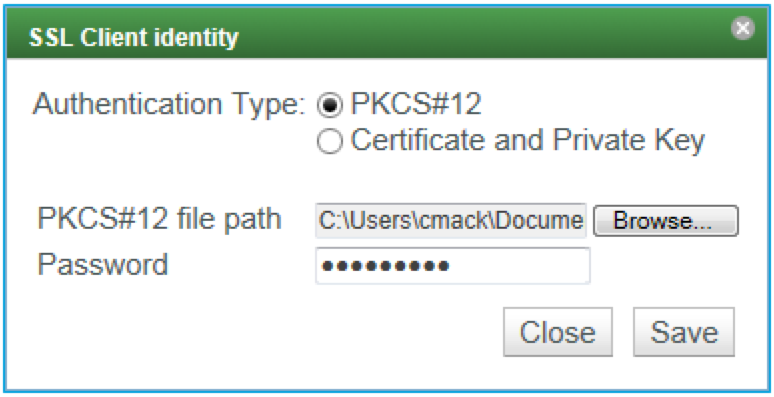
Configure an Application

Please fill OpenTrust PKI application configuration parameters

Name and description	
Name	
Description	
Connection Settings	
Server address	
Server port	443
SSL Client identity	Add an SSL client identity
Connection to application	Connection

3 Enter appropriate information in the fields and then select on the **Add an SSL client identity** button.

4 The **SSL Client identity** dialog box appears. Select the **Authentication Type** radio button. In this example, choose **PKCS#12** since you are uploading a **P12** (= PFX) file.



SSL Client identity

Authentication Type: ● PKCS#12
○ Certificate and Private Key

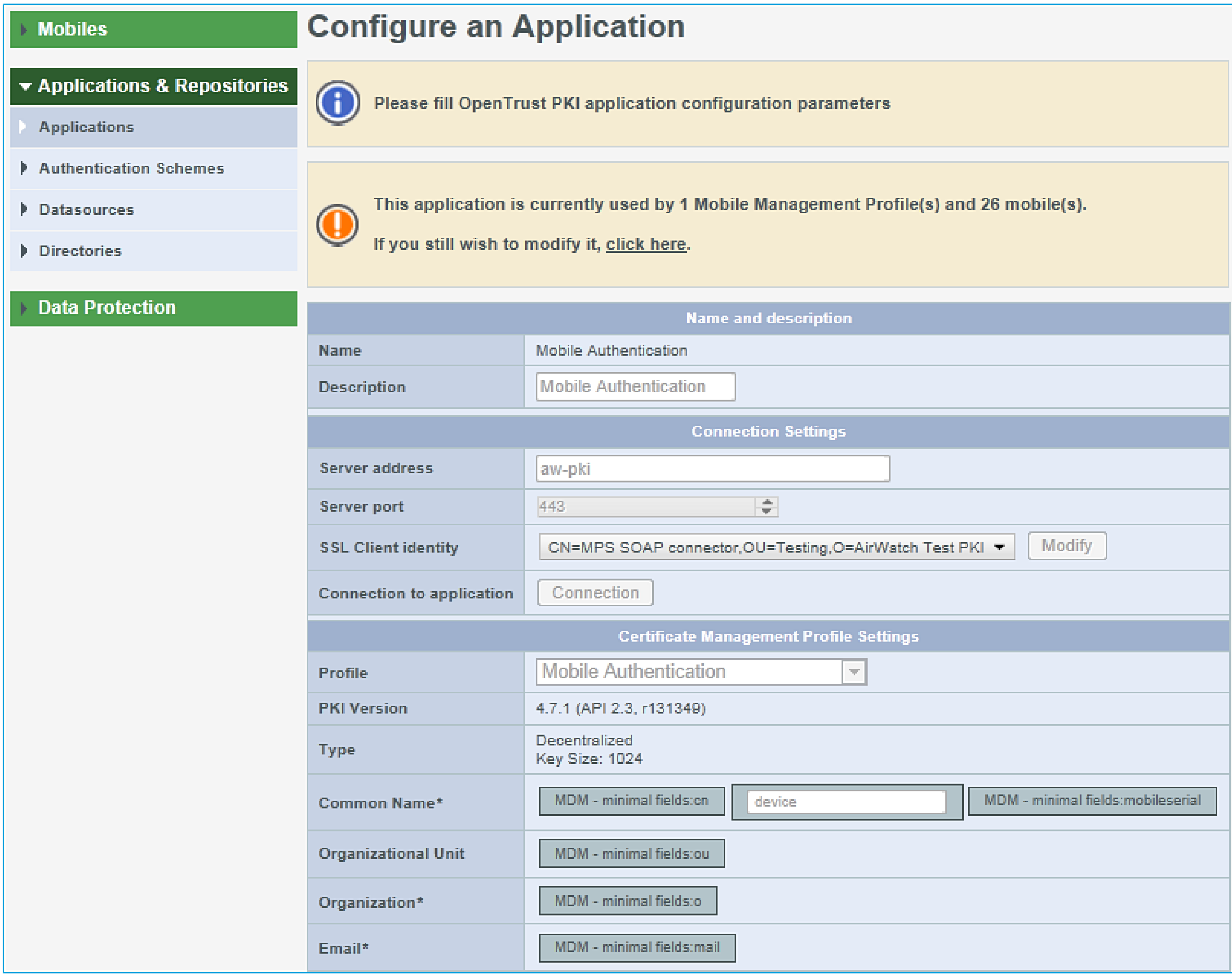
PKCS#12 file path C:\Users\cmack\Docume Browse...
Password ●●●●●●●●●●

5 Click on the **Browse** button and navigate to the **P12** file containing the “PKI SOAP connector” identity.

The certificate you need to upload here corresponds to the “PKI SOAP connector identity”. This identity must have been created by the PKI administrator and configured to have access rights to enroll/revoke certificates on all profiles chosen for mobile usage. This certificate needs not be integrated into a browser; it is only used server-to-server for strong authentication. You should have received a PFX/P12 file together with the associated password.

6 Enter the **Password** you received when you received the P12 file.

7 Click **Save**. The window expands to display the **Certificate Management Profile Settings** section. This section provides you with the ability to link the **Certificate Profile** Fields to the **Datasource** fields.



Configure an Application

Please fill OpenTrust PKI application configuration parameters

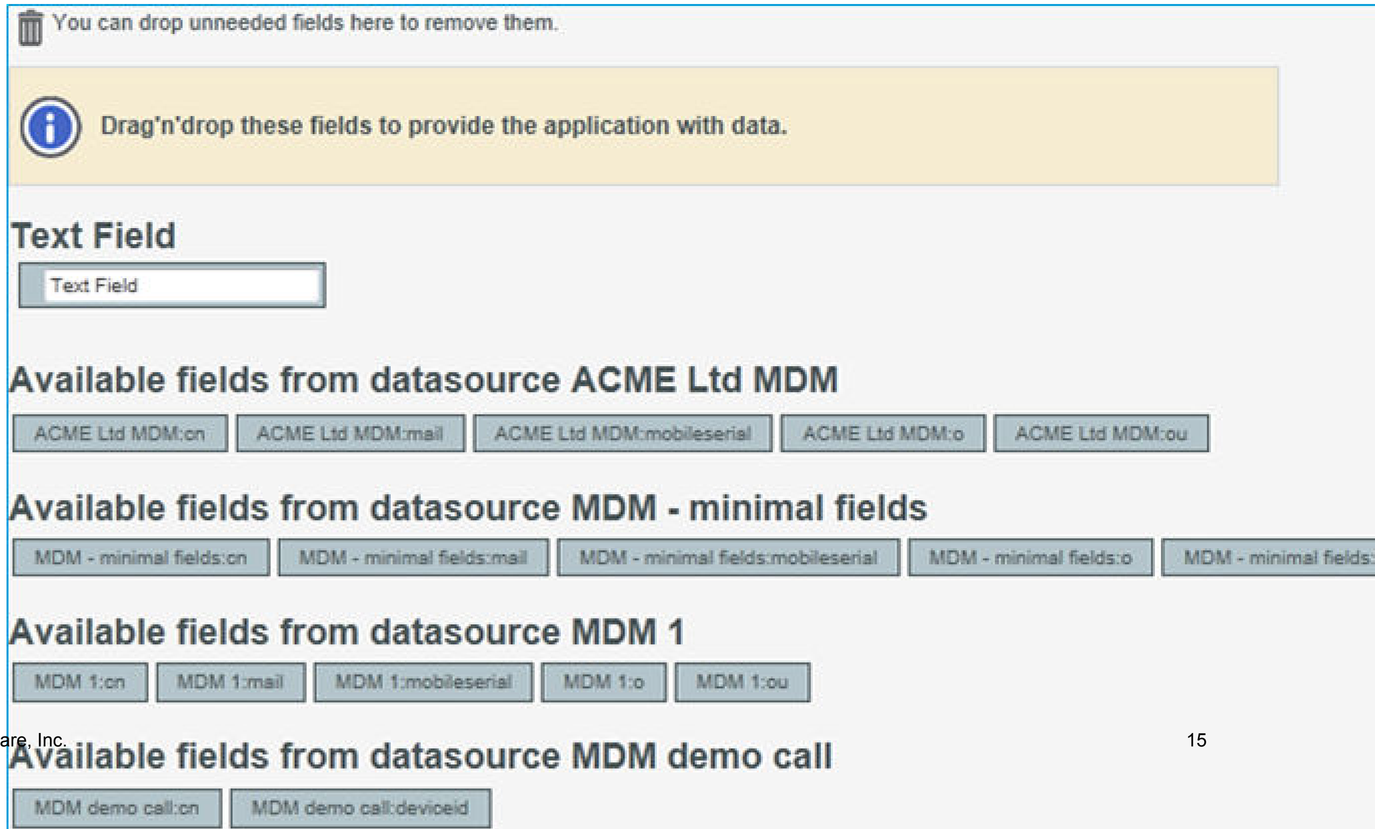
This application is currently used by 1 Mobile Management Profile(s) and 26 mobile(s).

If you still wish to modify it, click here.

Name and description	
Name	Mobile Authentication
Description	Mobile Authentication

Connection Settings	
Server address	aw-pki
Server port	443
SSL Client identity	CN=MPS SOAP connector,OU=Testing,O=AirWatch Test PKI ▾ Modify
Connection to application	Connection

Certificate Management Profile Settings	
Profile	Mobile Authentication ▾
PKI Version	4.7.1 (API 2.3, r131349)
Type	Decentralized Key Size: 1024
Common Name*	MDM - minimal fields:cn · device · MDM - minimal fields:mobileserial
Organizational Unit	MDM - minimal fields:ou
Organization*	MDM - minimal fields:o
Email*	MDM - minimal fields:mail



You can drop unneeded fields here to remove them.

Drag'n'drop these fields to provide the application with data.

Text Field

Available fields from datasource ACME Ltd MDM

Available fields from datasource MDM - minimal fields

Available fields from datasource MDM 1

Available fields from datasource MDM demo call

8 Click on the **Profile** drop-down and select the profile from the list. Based on the selection, the **PKI Version** and **Type** automatically populates and the Mandatory Fields that is associated with Workspace ONE UEM Template display.

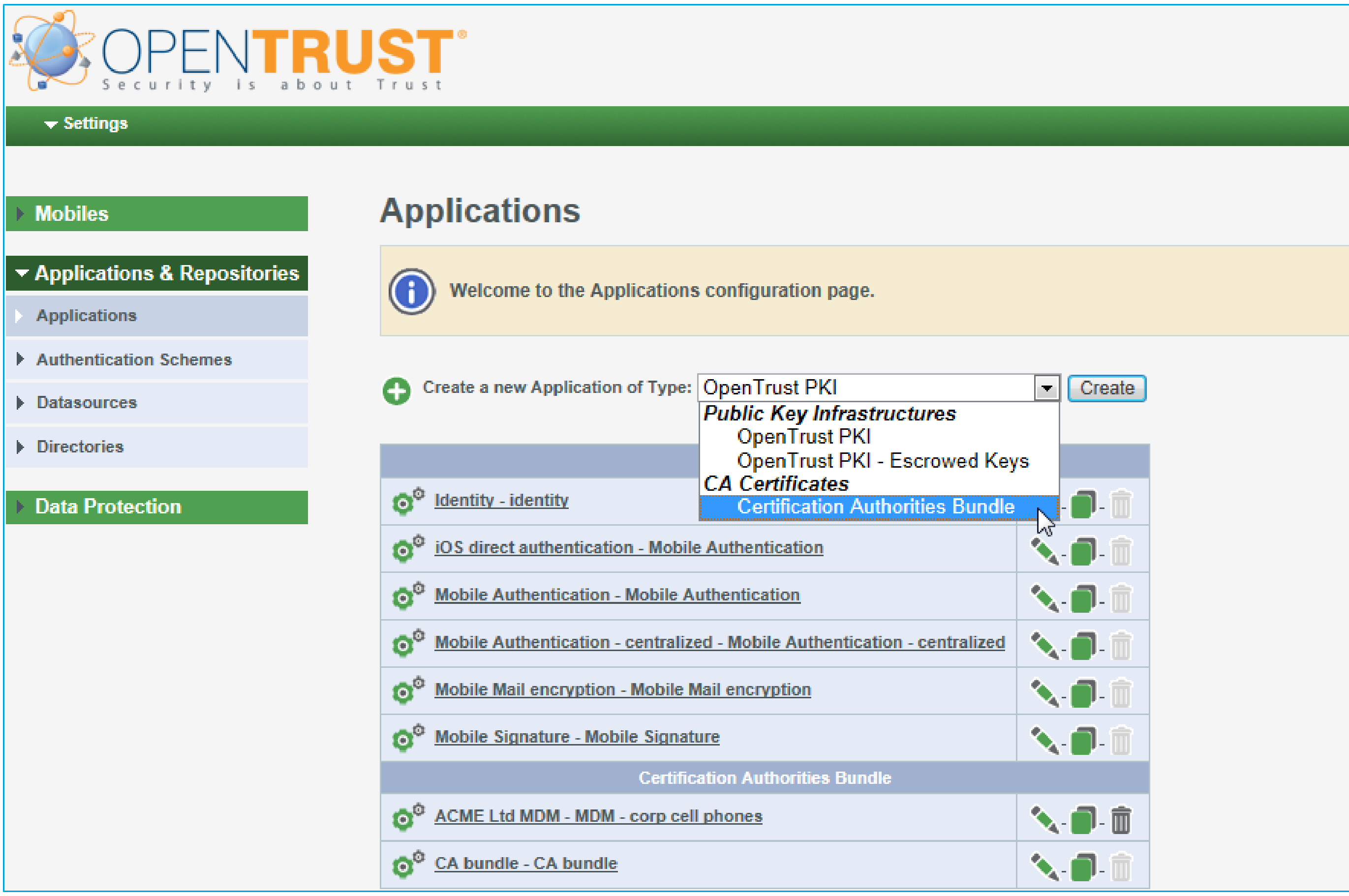
9 Drag and drop the available **Data Source Fields** from the bottom of the screen to the **Mandatory Fields**. In this example, it is the **Common Name**, **Organizational Unit**, **Organization**, and **Email**.

10 Click **Save**. This links the OpenTrust **Mobile Management Profile** to the **Data Source** fields.

Select the Certification Authorities Bundle Application Type

You can add a bundle of Root and Sub-CA certificates by selecting this kind of application. To be part of a distributable bundle, a CA certificate needs to be trusted first by OpenTrust CMS Mobile. This can be achieved by editing trusted Certification Authorities through **Server Management / Trust & Internal Certificates / Trusted External CAs**, then selecting the right button **Trust an external CA**.

1 Select **Certification Authorities Bundle** from the drop-down.



Applications

Welcome to the Applications configuration page.

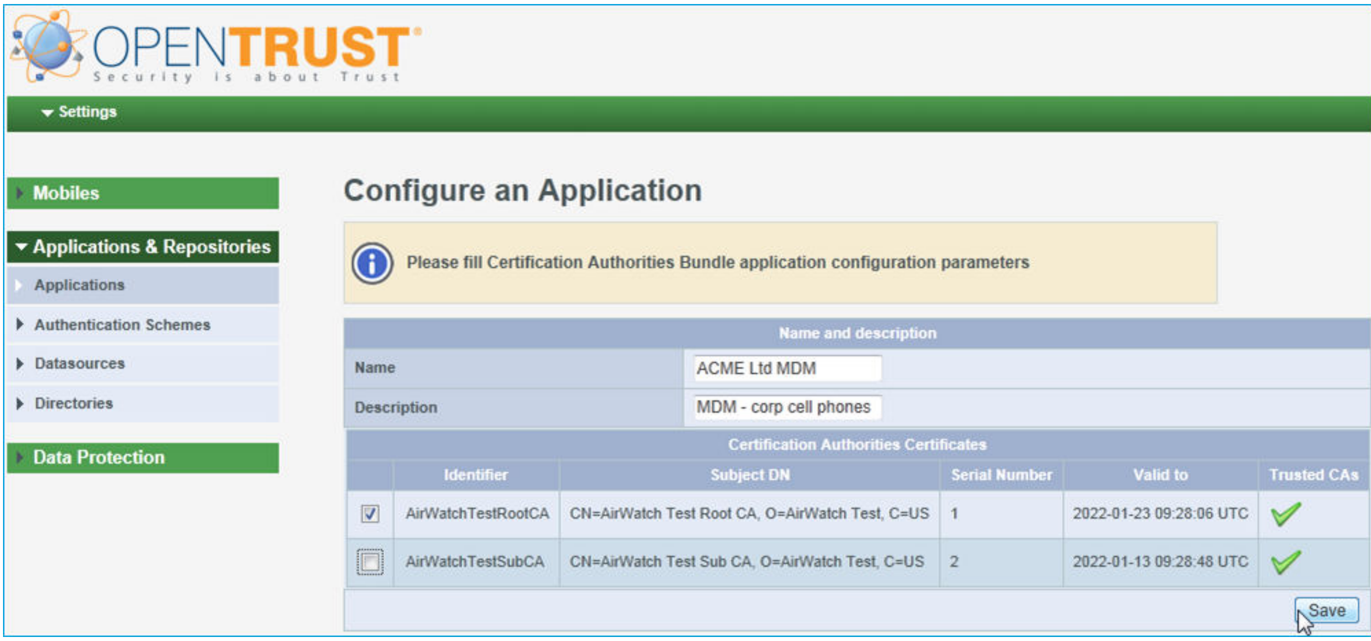
Create a new Application of Type: OpenTrust PKI

Identity - identity
iOS direct authentication - Mobile Authentication
Mobile Authentication - Mobile Authentication
Mobile Authentication - centralized - Mobile Authentication - centralized
Mobile Mail encryption - Mobile Mail encryption
Mobile Signature - Mobile Signature

Certification Authorities Bundle

ACME Ltd MDM - MDM - corp cell phones
CA bundle - CA bundle

2 Click **Create**. The **Configure an Application** window appears.



Configure an Application

Please fill Certification Authorities Bundle application configuration parameters

Name and description	
Name	ACME Ltd MDM
Description	MDM - corp cell phones

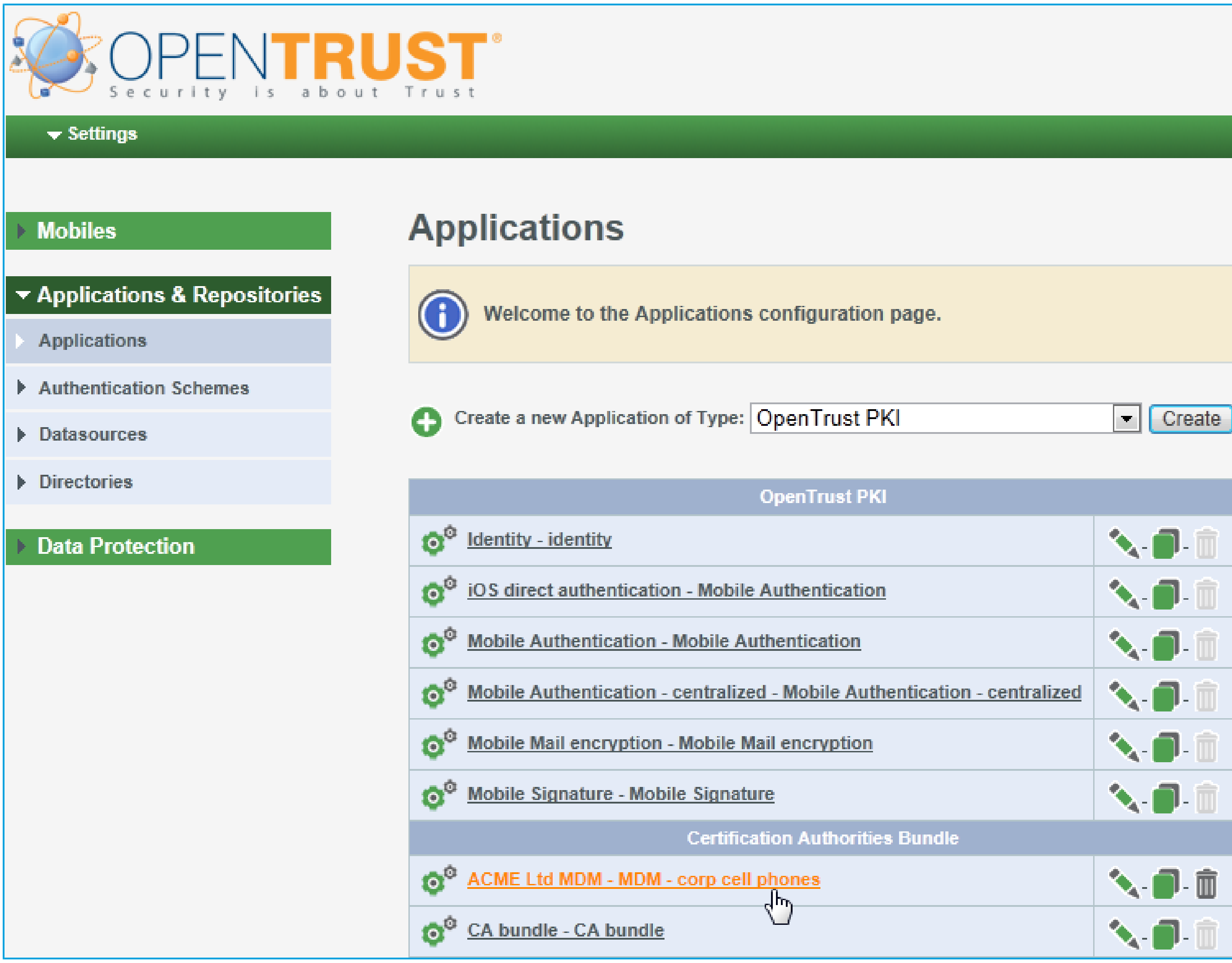
Certification Authorities Certificates

	Identifier	Subject DN	Serial Number	Valid to	Trusted CAs
☑	AirWatchTestRootCA	CN=AirWatch Test Root CA, O=AirWatch Test, C=US	1	2022-01-23 09:28:06 UTC	✓
□	AirWatchTestSubCA	CN=AirWatch Test Sub CA, O=AirWatch Test, C=US	2	2022-01-13 09:28:48 UTC	✓

3 Enter appropriate information in the fields and then check the appropriate checkbox for the certificate you want to associate to the Application.

4 Click **Save**. This links the **Certificate** to the **Application**.

5 The **Applications** window appears. The new **Certification Authorities Bundle** appears in the list.



Applications

Welcome to the Applications configuration page.

Create a new Application of Type: OpenTrust PKI

OpenTrust PKI

- Identity - identity
- iOS direct authentication - Mobile Authentication
- Mobile Authentication - Mobile Authentication
- Mobile Authentication - centralized - Mobile Authentication - centralized
- Mobile Mail encryption - Mobile Mail encryption
- Mobile Signature - Mobile Signature

Certification Authorities Bundle

- ACME Ltd MDM - MDM - corp cell phones
- CA bundle - CA bundle

Step 4: Configure the OpenTrust CMS Mobile MDM Profile

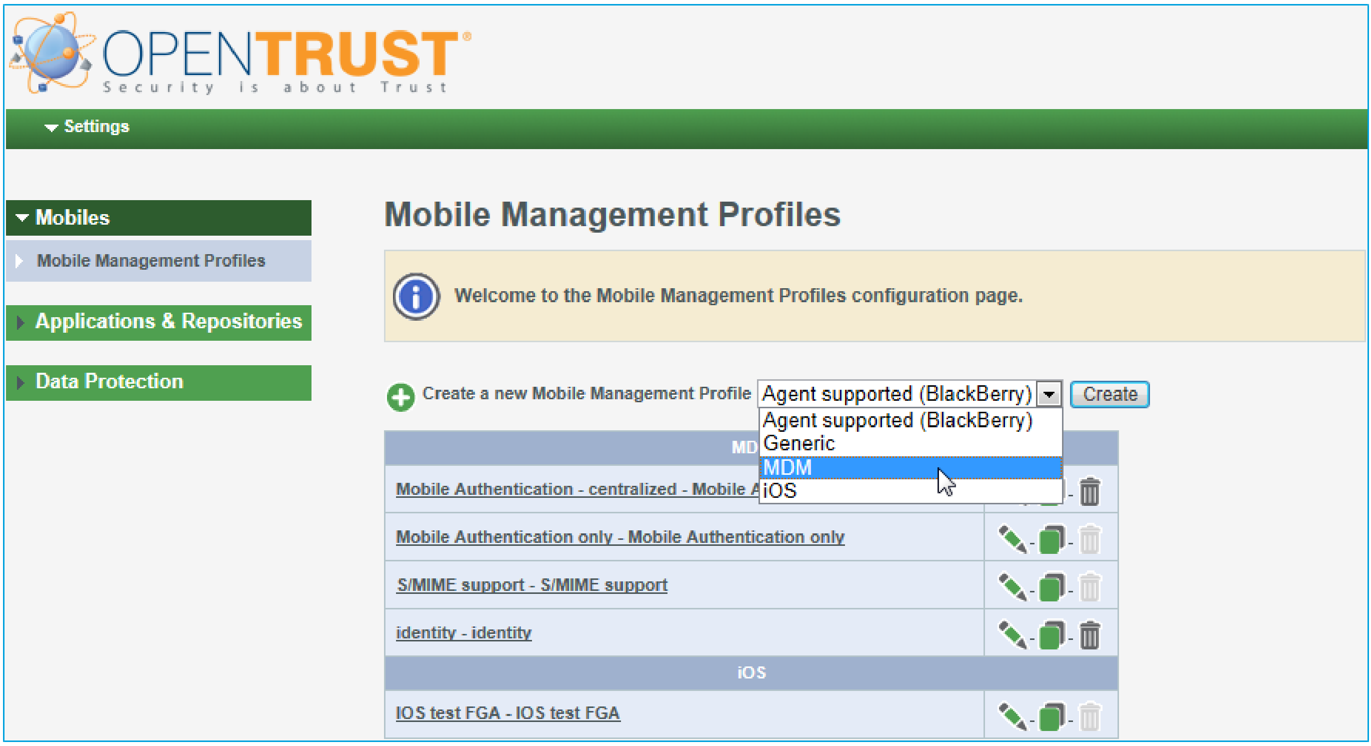
After you set up the OpenTrust **Application**, you need to configure the OpenTrust **Mobile Management Profile** to point to one or more OpenTrust **Applications**. This completes the process by connecting all the points needed by OpenTrust to enroll devices submitted by Workspace ONE UEM. A Mobile Management Profile essentially represents a list of one or more certificates linked together which will be retrieved by Workspace ONE UEM and deployed on a given mobile device.

For example, one profile contains a single certificate for VPN users; one profile containing two certificates for S/MIME users; or one do-it-all profile containing authentication, signing, and encryption certificates. A Mobile Management Profile links all of these certificates together. When users enroll against a profile they get all the defined certificates in one go. Note that Workspace ONE UEM supports only one credential per mobile management profile.

1 Click the **Create a new Mobile Management Profile** drop-down arrow.

2 Select **MDM** from the list.

Note You can select **Agent supported (BlackBerry)**, **Generic**, **MDM**, and **iOS** from the drop-down list. Since the configuration of all selection are similar, except for the addition configuration of **Wi-Fi**, **Exchange**, and **VPN** if you select **iOS**, and this guide is only intended to provide guidance through some examples, we chose the most common selection – **MDM**. For more detailed information, refer to your OpenTrust manual, or call their technical support.


OPENTRUST
Security is about Trust
Settings
Mobiles
Mobile Management Profiles
Applications & Repositories
Data Protection
Create
Agent supported (BlackBerry)
Agent supported (BlackBerry)
Generic
MDM
iOS

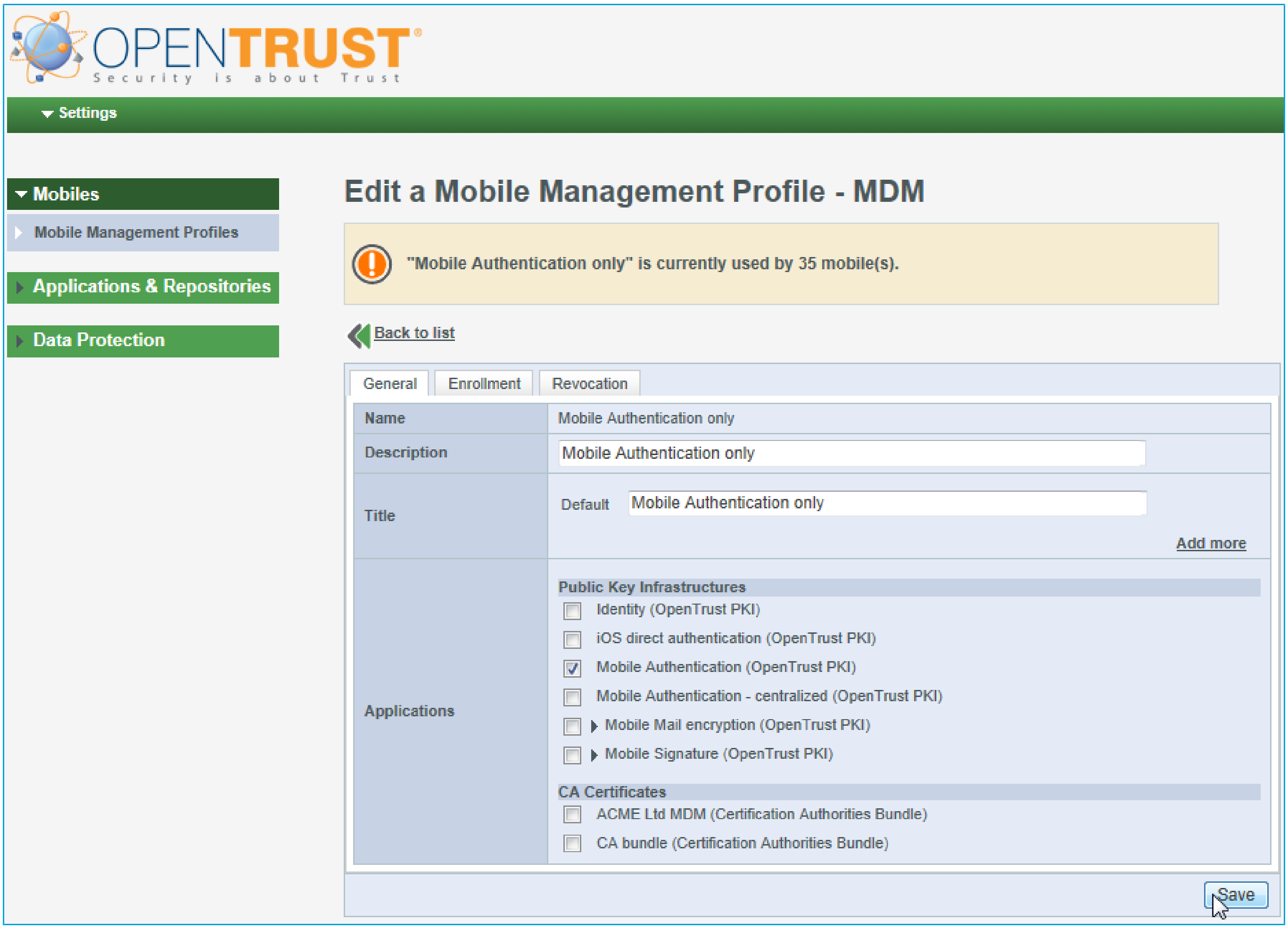
Mobile Management Profiles

Welcome to the Mobile Management Profiles configuration page.

Create a new Mobile Management Profile

MD	
Mobile Authentication - centralized - Mobile A	
Mobile Authentication only - Mobile Authentication only	
S/MIME support - S/MIME support	
identity - identity	
iOS	
IOS test FGA - IOS test FGA	

3 Click **Create**. The **Edit a Mobile Management Profile - MDM** window appears.



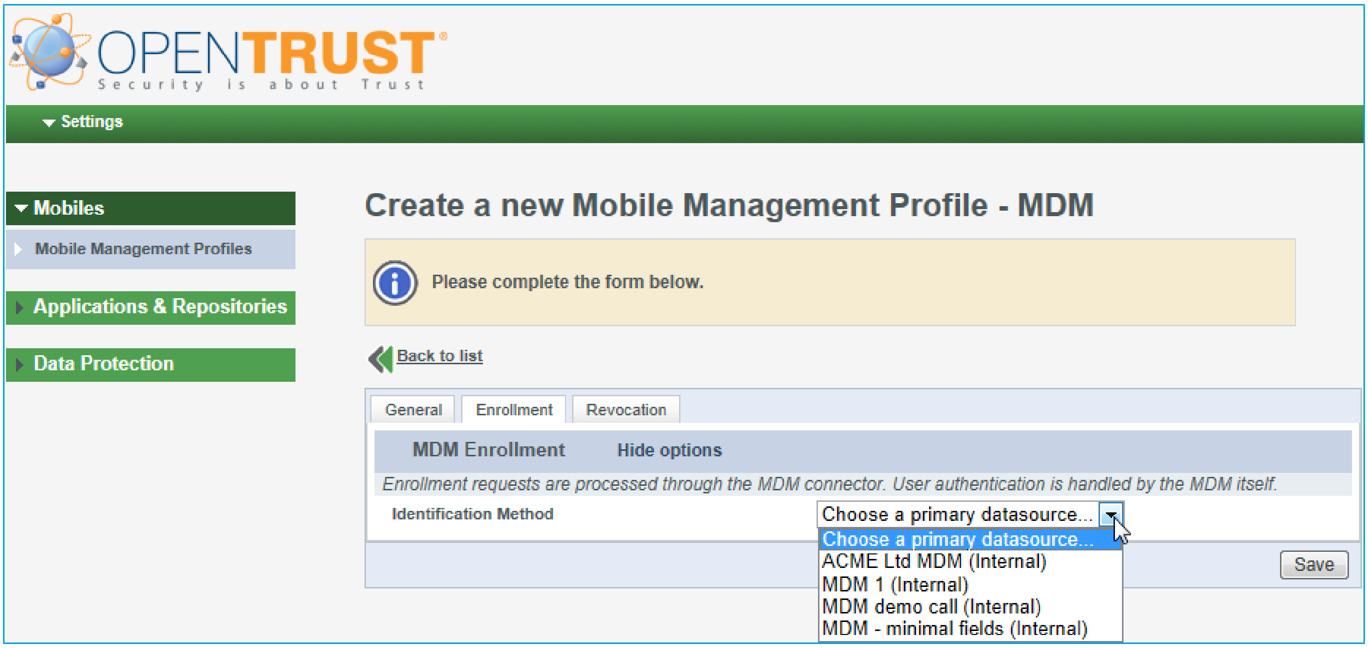
Edit a Mobile Management Profile - MDM

"Mobile Authentication only" is currently used by 35 mobile(s).

Name	Mobile Authentication only
Description	Mobile Authentication only
Title	Default Mobile Authentication only
Applications	Public Key Infrastructures □ Identity (OpenTrust PKI) □ iOS direct authentication (OpenTrust PKI) ☑ Mobile Authentication (OpenTrust PKI) □ Mobile Authentication - centralized (OpenTrust PKI) □ Mobile Mail encryption (OpenTrust PKI) □ Mobile Signature (OpenTrust PKI) CA Certificates □ ACME Ltd MDM (Certification Authorities Bundle) □ CA bundle (Certification Authorities Bundle)

4 Enter appropriate information in the **Name**, **Description**, and **Title** fields and then check the appropriate **Application** checkbox for the **Public Key Infrastructure** or **CA Certificate** you want to associate to the **Profile**.

5 Click the **Enrollment** tab.



Create a new Mobile Management Profile - MDM

Please complete the form below.

MDM Enrollment Hide options

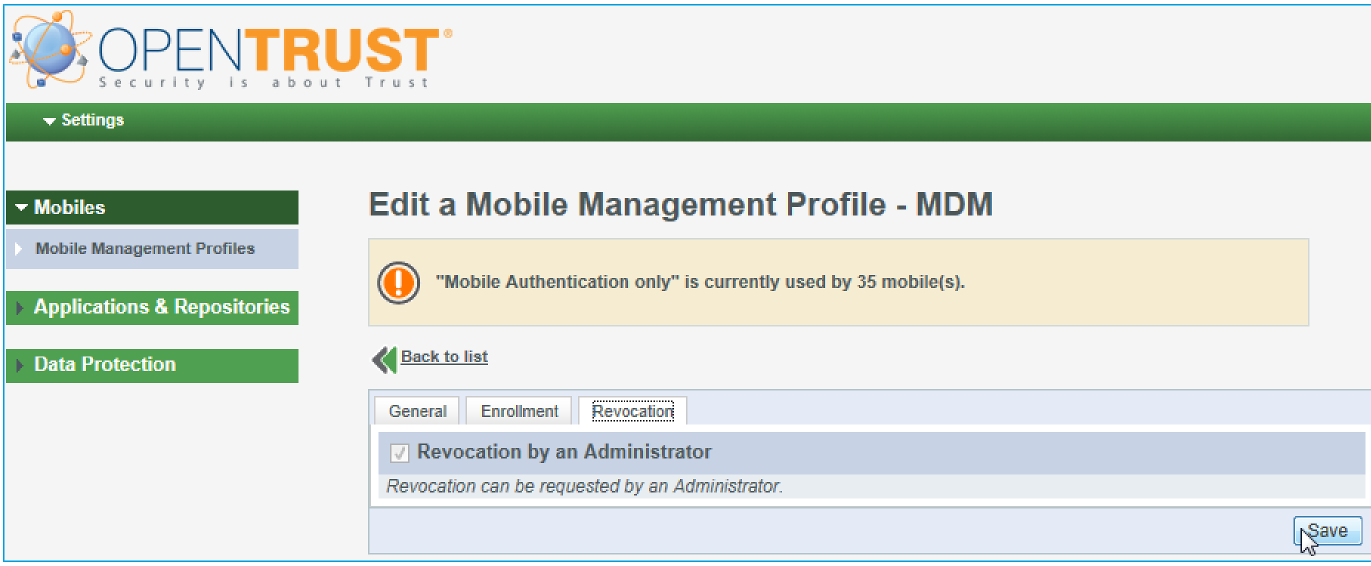
Enrollment requests are processed through the MDM connector. User authentication is handled by the MDM itself.

Identification Method: Choose a primary datasource...

- Choose a primary datasource...
- ACME Ltd MDM (Internal)
- MDM 1 (Internal)
- MDM demo call (Internal)
- MDM - minimal fields (Internal)

6 Click the **Identification Method** drop-down arrow and select one method from the list. This allows you to choose any of the **Internal Datasources** that were previously created. Select the main datasource that was declared in Applications.

7 Click the **Revocation** tab.



Edit a Mobile Management Profile - MDM

"Mobile Authentication only" is currently used by 35 mobile(s).

☑ Revocation by an Administrator

Revocation can be requested by an Administrator.

8 Click to select the **Revocation by an Administrator** checkbox if you want to allow administrators to revoke this profile.

9 Click **Save**. This saves the profile and completes the connection between the **Datasource**, **Application**, and **Mobile Management Profile**.

Step 5: Configure OpenTrust in Workspace ONE UEM

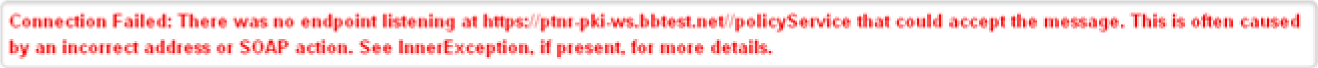
Now that you have generated an OpenTrust CMS Mobile 2.0 RA certificate, Workspace ONE UEM can be configured to communicate with OpenTrust.

1. Navigate to **Devices > Certificates > Certificate Authorities** and in the **System Settings** page that displays, ensure the **Certificate Authorities** tab is selected.
2. Select the **Add** button.

   The **Certificate Authority – Add / Edit** page displays.
3. Select the **Authority Type** drop-down and select **OpenTrust CMS Mobile**.
4. Enter in the **Name** field a unique name that identifies the OpenTrust certificate authority.
5. Enter in the **Server URL** field; enter the URL of your OpenTrust CMS instance.

   The URL is different for each customer and your Workspace ONE UEM administrator should ask the MPS administrator where to connect to. Its general form is https://FQDN/connector/mdm.cgiwhere FQDN is the Fully Qualified Domain Name of the OpenTrust CMS Mobile server.
6. Select the **Protocol** either the **PKI** or **SCEP** radio button.
7. Lastly, select on the **Upload** button and select the "CMS JSON connector" certificate (PFX or P12 file) that you received in order to communicate with OpenTrust CMS Mobile.
8. If applicable, the root certificate of the CMS JSON connector (pfx file) needs to be uploaded in the Trusted Root store of the Workspace ONE UEM Cloud Connector server.
9. Enter in the **Certificate Password** field the password you received with the P12 file.
10. Select the **Save** button and the **PFX/P12** file uploads into Workspace ONE UEM and displays pertinent information about the certificate.
11. When complete, select the Test Connection button and verify that the test is successful.

    If the connection failed, an error displays. This error could be the result of a certificate not being installed on the Workspace ONE UEM server, the URL not being correct, etc. In this case, the **Server URL** was not correct.

    Connection Failed: There was no endpoint listening at https://ptnr-pki-ws.bbtest.net//policyService that could accept the message. This is often caused by an incorrect address or SOAP action. See InnerException, if present, for more details.
12. Select **Save**.

Step 6: Set Up Certificate Template for OpenTrust CA Type

Now that you have completed Step 5: Configure OpenTrust in Workspace ONE UEM, Workspace ONE UEM is able to communicate with OpenTrust. The next step is to define which certificate will be deployed to devices by setting up a certificate template in Workspace ONE UEM.

Use the following steps whether you are setting up a template for PKI or SCEP.

1 While still in the **Certificate Authorities** system settings page (**Groups & Settings > All Settings > System > Enterprise Integration > Certificate Authorities**), select the **Request Templates** tab.

2 Select the **Add** button to add a new Certificate Template.

3 The **Certificate Template Add/Edit** window displays. First, select on the **Certificate Authority** drop-down and select the OpenTrust certificate authority you created in completed in Step 5: Configure OpenTrust in Workspace ONE UEM.

4 Enter in the **Name** and **Description** fields the name you want to give the OpenTrust certificate template.

5 If Workspace ONE UEM is going to automatically request the certificate to be renewed by OpenTrust when it expires, check the **Automatic Certificate Renewal** checkbox and then enter in the **Auto Renewal Period (days)** field the number of days prior to expiration before Workspace ONE UEM automatically requests OpenTrust to reissue the certificate.

6 Click on the **Profile Name** drop-down and select the OpenTrust profile you created in Step 4: Configure the OpenTrust CMS Mobile MDM Profile.

   Mandatory Fields display. These fields can change depending on which OpenTrust profile you choose since the information within the profile may be different. The fields you see on the left side correspond to the datasource fields you declared on the OpenTrust side. The values on the right are the Workspace ONE UEM variables.

   The lookup values you enter in the Workspace ONE UEM Certificate Template **Mandatory Fields** above are used as attributes for certificate generation. Make sure the lookup values you use match those used in the OpenTrust Portal. For example, if your **mail** in OpenTrust Portal is **email address** then use the **{EmailAddress}** lookup value for **mail** in the Workspace ONE UEM certificate template. If the lookup values do not match, OpenTrust will create a new user.

7 Enter **Lookup Values** in each of the fields that complement those fields in the OpenTrust profile.

8 Click **Save**.

Deploy OpenTrust S/MIME Certificates

S/MIME certificates are used primarily to encrypt/decrypt and sign emails, and unlike client authentication certificates, the same S/MIME certificate needs to be installed on all devices associated with a specific user.

To achieve this OpenTrust separates a user's devices into primary and secondary devices. Each user can have only one primary device and multiple secondary devices. New S/MIME certificates can only be requested by the primary device and then installed on secondary devices. Primary and secondary devices will therefore need separate OpenTrust Profiles and corresponding Workspace ONE UEM Templates, profiles, and assignment groups.

Procedure

1 Separate primary and secondary devices by assignment group.

   a Create different assignment groups for primary and secondary devices respectively.

      These can be Smart Groups, Organization Groups, or User Groups.

   For example, create a smart group “Primary S/MIME” and populate it with one primary device per user. Create another smart group “Secondary S/MIME” which will contain all other devices.

2 Add templates for primary and secondary devices.

   a Create individual Certificate Authority Templates for primary and secondary devices.

   b Navigate to **Devices > Certificates > Certificate Authorities > Request Templates** and select **Add**.

   c Select OpenTrust CA as the **Certificate Authority** and under **Profile Name** choose the corresponding OpenTrust profile for primary devices.

   d Configure any other settings required and select **Save**.

   e Add another template where the **Profile Name** chosen is for secondary devices.

3 Add device profiles.

   a Create device profiles for primary devices, by platform, including **Email** and **Credentials** payloads.

   b In the **Credentials** payload, select Defined Certificate Authority and choose the template defined for primary devices.

   c Save and publish.

   d Once confirmed, repeat for secondary devices.