

VMware AirWatch Integration with OpenTrust CMS Mobile 2.0 Guide

For VMware AirWatch

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

Chapter 1: Workspace ONE UEM Integration with OpenTrust CMS Mobile 2	3
System Requirements	3
High Level Design	4
Chapter 2: Install, Set Up, Configure Certificate	7
Step 1: Obtain Certificates for Communication with OpenTrust CMS Mobile	7
Step 2: Configure a Workspace ONE UEM Datasource in OpenTrust CMS Mobile	8
Step 3: Configure the OpenTrust CMS Mobile Application	11
Step 4: Configure the OpenTrust CMS Mobile MDM Profile	17
Step 5: Configure OpenTrust in Workspace ONE UEM	21
Step 6: Set Up Certificate Template for OpenTrust CA Type	21
Deploying OpenTrust S/MIME Certificates	22

Chapter 1:

Workspace ONE UEM Integration with OpenTrust CMS Mobile 2

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.

System Requirements

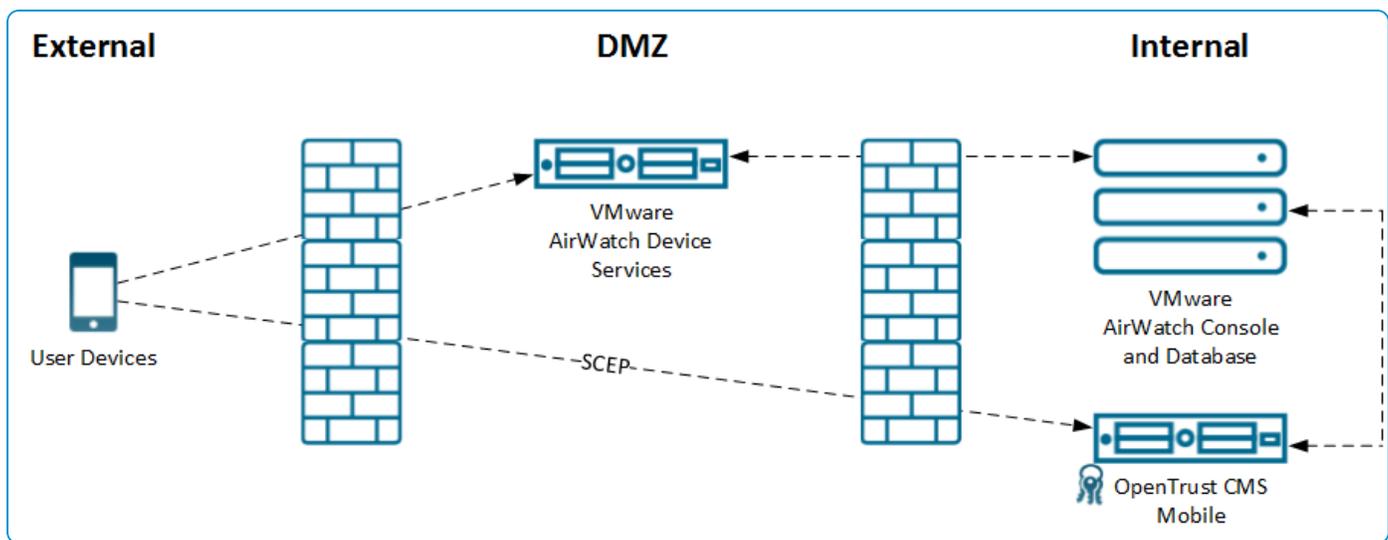
The following tasks must be completed before proceeding with the steps outlined in this documentation.

- 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.

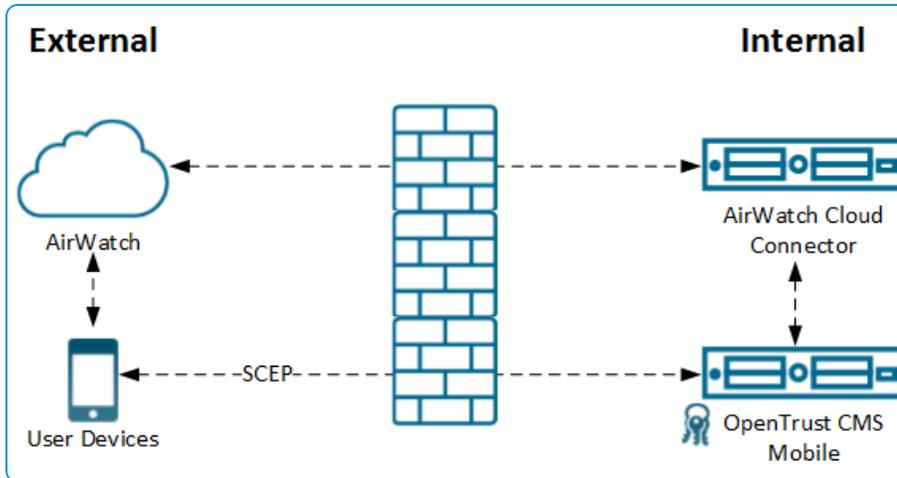
High Level Design

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.

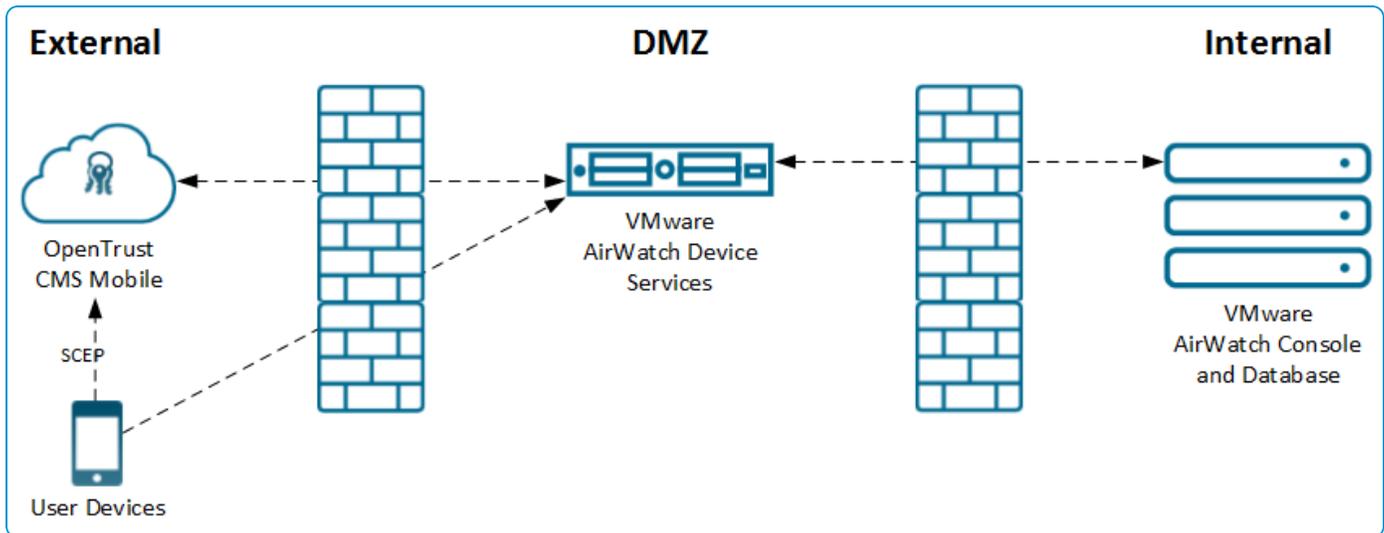
OpenTrust and Workspace ONE UEM Configured Internally



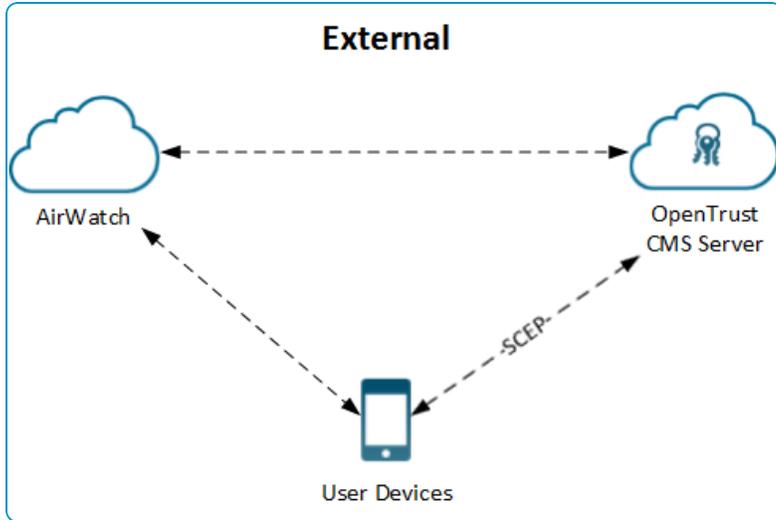
Workspace ONE UEM Cloud with OpenTrust On Premises



OpenTrust Cloud with Workspace ONE UEM On Premises



Both OpenTrust and Workspace ONE UEM Configured Externally



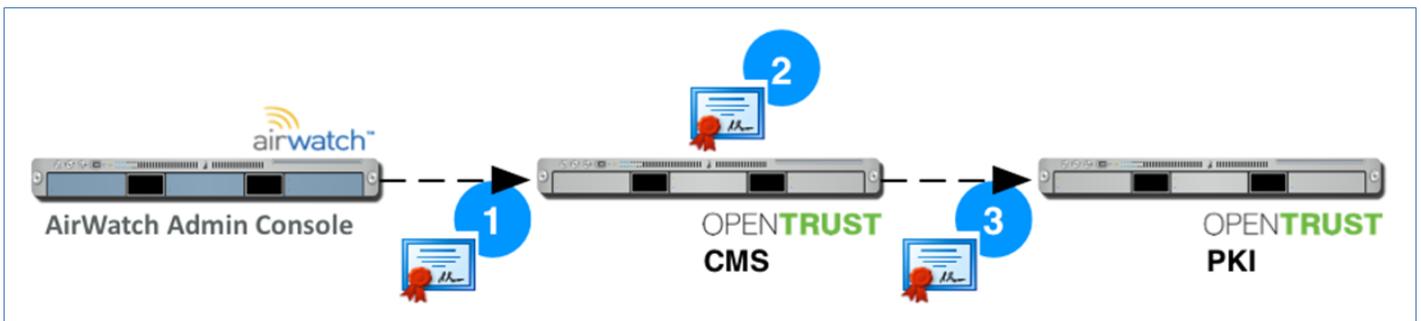
Chapter 2:

Install, Set Up, Configure Certificate

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.

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”.

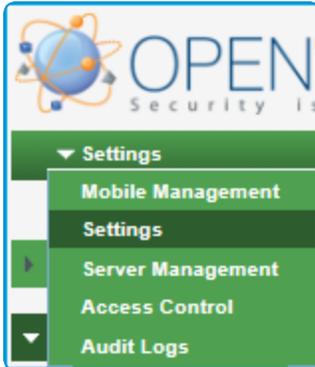
These identities must have been configured by the CMS administrator with appropriate rights for each task.

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.

The screenshot shows the OpenTrust CMS Mobile 2.0 interface. The sidebar on the left contains the following navigation items: Settings, Mobiles, Applications & Repositories (with sub-items: Applications, Authentication Schemes, Datasources, Directories), and Data Protection. The main content area is titled "Datasources" and features a yellow welcome banner: "Welcome to the Datasources configuration page." Below the banner is a "Create a new Datasource" button with a dropdown menu currently showing "Internal" and "LDAP" options, and a "Create" button. A table below lists existing datasources:

Internal	
MDM 1 - Another MDM data source	[Edit] [Duplicate] [Delete]
MDM demo call - MDM demo call	[Edit] [Duplicate] [Delete]
MDM - minimal fields - MDM - minimal fields	[Edit] [Duplicate] [Delete]
LDAP	
ldap interne - ldap interne	[Edit] [Duplicate] [Delete]

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.

OPEN TRUST
Security Is about Trust

Settings

Mobiles

Applications & Repositories

Applications

Authentication Schemes

Datasources

Directories

Data Protection

Configure an Internal Datasource

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

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mail	mail	Email Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
mobileserial	mobileserial	Serial Number	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
o	o	Organization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ou	ou	Organizational Unit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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: Setup 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.

OPENTRUST
Security is about Trust

▼ Settings

► Mobiles

▼ Applications & Repositories

- Applications
- Authentication Schemes
- Datasources
- Directories

► Data Protection

Datasources

Welcome to the Datasources configuration page.

+ Create a new Datasource

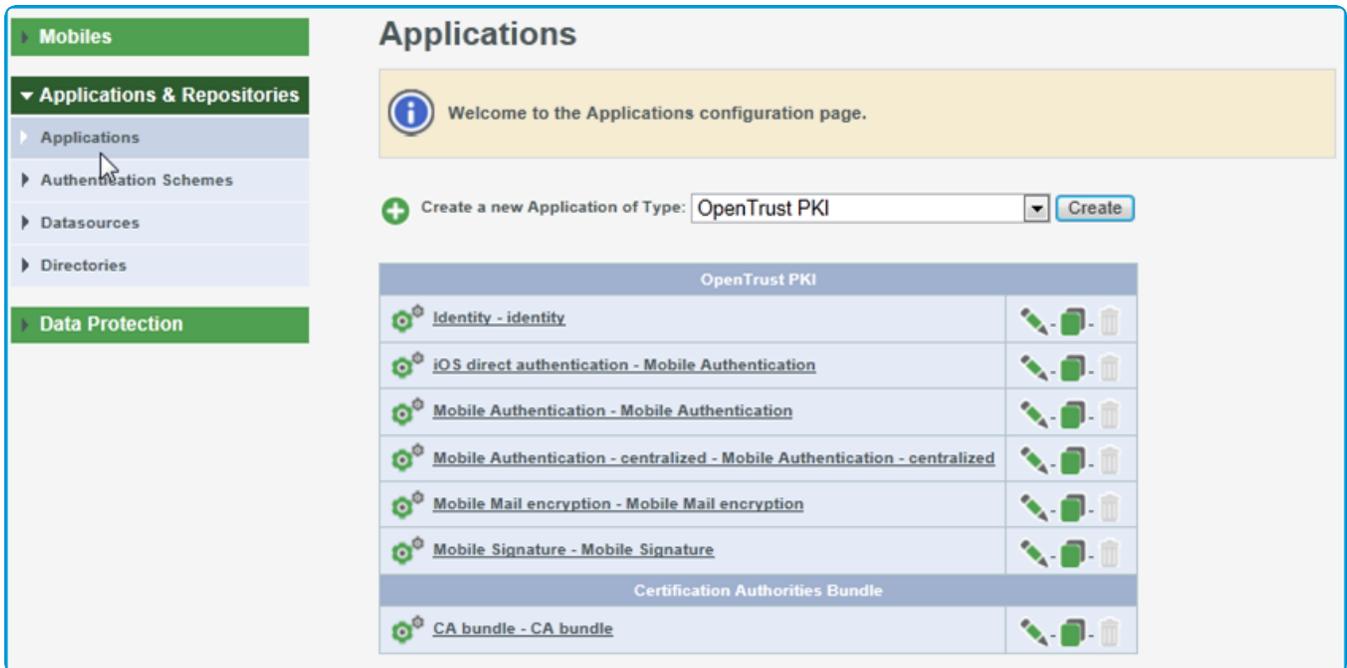
Internal		
	ACME Ltd MDM - MDM for all corporate cell phones	
	MDM 1 - Another MDM data source	
	MDM demo call - MDM demo call	
	MDM - minimal fields - MDM - minimal fields	
LDAP		
	ldap interne - ldap interne	

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.



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 Certificate Authorities Bundle. OpenTrust PKI Escrowed Keys is configured in a similar fashion.



Select the OpenTrust PKI Application Type

1. Select **OpenTrust PKI** from the drop-down.
2. Click **Create**. The **Configure an Application** window appears.

OPEN TRUST
Security Is about Trust

Settings

Mobiles

Applications & Repositories

- Applications
- Authentication Schemes
- Datasources
- Directories

Data Protection

Configure an Application

Please fill OpenTrust PKI application configuration parameters

Name and description	
Name	<input type="text"/>
Description	<input type="text"/>

Connection Settings	
Server address	<input type="text"/>
Server port	443
SSL Client identity	<input type="button" value="Add an SSL client identity"/>
Connection to application	<input type="button" value="Connection"/>

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

Password:

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

- ▶ Mobiles
- ▼ Applications & Repositories
- ▶ Applications
- ▶ Authentication Schemes
- ▶ Datasources
- ▶ Directories
- ▶ Data Protection

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	<input type="text" value="Mobile Authentication"/>
Connection Settings	
Server address	<input type="text" value="aw-pki"/>
Server port	<input type="text" value="443"/>
SSL Client identity	<input type="text" value="CN=MPS SOAP connector,OU=Testing,O=AirWatch Test PKI"/> <input type="button" value="Modify"/>
Connection to application	<input type="text" value="Connection"/>
Certificate Management Profile Settings	
Profile	<input type="text" value="Mobile Authentication"/>
PKI Version	4.7.1 (API 2.3, r131349)
Type	Decentralized Key Size: 1024
Common Name*	<input type="text" value="MDM - minimal fields:cn"/> <input type="text" value="device"/> <input type="text" value="MDM - minimal fields:mobileserial"/>
Organizational Unit	<input type="text" value="MDM - minimal fields:ou"/>
Organization*	<input type="text" value="MDM - minimal fields:o"/>
Email*	<input type="text" value="MDM - minimal fields:mail"/>

You can drop unneeded fields here to remove them.

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

Text Field

Text Field

Available fields from datasource ACME Ltd MDM

ACME Ltd MDM:cn ACME Ltd MDM:mail ACME Ltd MDM:mobileserial ACME Ltd MDM:o ACME Ltd MDM:ou

Available fields from datasource MDM - minimal fields

MDM - minimal fields:cn MDM - minimal fields:mail MDM - minimal fields:mobileserial MDM - minimal fields:o MDM - minimal fields:ou

Available fields from datasource MDM 1

MDM 1:cn MDM 1:mail MDM 1:mobileserial MDM 1:o MDM 1:ou

Available fields from datasource MDM demo call

MDM demo call:cn MDM demo call:deviceid

Available fields from datasource ldap_interne

ldap_interne:cn ldap_interne:employeetype ldap_interne:mail ldap_interne:uid

Required fields are marked with *.

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.

The screenshot shows the OpenTrust CMS Mobile 2.0 interface. The left sidebar contains navigation menus for Settings, Mobiles, Applications & Repositories, and Data Protection. The main content area is titled 'Applications' and includes a welcome message. Below the welcome message is a 'Create a new Application of Type:' dropdown menu. The dropdown is open, showing a list of application types: OpenTrust PKI, Public Key Infrastructures, OpenTrust PKI, OpenTrust PKI - Escrowed Keys, CA Certificates, and Certification Authorities Bundle. The 'Certification Authorities Bundle' option is highlighted by the mouse cursor. A 'Create' button is visible to the right of the dropdown.

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

The screenshot shows the 'Configure an Application' window in the OpenTrust CMS Mobile 2.0 interface. The window displays configuration parameters for a Certification Authorities Bundle application. The Name is 'ACME Ltd MDM' and the Description is 'MDM - corp cell phones'. Below this is a table of Certificates with columns for Identifier, Subject DN, Serial Number, Valid to, and Trusted CAs. Two certificates are listed: AirWatchTestRootCA and AirWatchTestSubCA. A 'Save' button is visible at the bottom right.

Certification Authorities Certificates					
	Identifier	Subject DN	Serial Number	Valid to	Trusted CAs
<input checked="" type="checkbox"/>	AirWatchTestRootCA	CN=AirWatch Test Root CA, O=AirWatch Test, C=US	1	2022-01-23 09:28:06 UTC	✓
<input type="checkbox"/>	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.

The screenshot displays the OpenTrust CMS interface. On the left is a sidebar with a green header 'Settings' and several menu items: 'Mobiles', 'Applications & Repositories' (expanded), 'Data Protection', 'Applications', 'Authentication Schemes', 'Datasources', and 'Directories'. The main area is titled 'Applications' and features a yellow welcome banner. Below it is a 'Create a new Application' form with a dropdown menu set to 'OpenTrust PKI' and a 'Create' button. A table below lists existing applications, grouped into 'OpenTrust PKI' and 'Certification Authorities Bundle'. The 'Certification Authorities Bundle' section includes an entry for 'ACME Ltd MDM - MDM - corp cell phones' which is highlighted by a mouse cursor.

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.

The screenshot displays the OpenTrust web interface for configuring Mobile Management Profiles. The sidebar on the left contains navigation links for Settings, Mobiles, Applications & Repositories, and Data Protection. The main content area is titled "Mobile Management Profiles" and features a welcome message: "Welcome to the Mobile Management Profiles configuration page." Below this, there is a "Create a new Mobile Management Profile" section with a dropdown menu. The dropdown menu is open, showing the following options: "Agent supported (BlackBerry)", "Generic", "MDM" (which is highlighted), and "iOS". A "Create" button is located to the right of the dropdown. Below the dropdown is a table of existing profiles:

Profile Name	Platform	Actions
Mobile Authentication - centralized - Mobile A	MDM	[Edit] [Delete]
Mobile Authentication only - Mobile Authentication only	MDM	[Edit] [Delete]
S/MIME support - S/MIME support	MDM	[Edit] [Delete]
identity - identity	MDM	[Edit] [Delete]
iOS		
IOS test FGA - IOS test FGA	iOS	[Edit] [Delete]

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

Settings

Mobiles

Mobile Management Profiles

Applications & Repositories

Data Protection

Edit a Mobile Management Profile - MDM

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

[Back to list](#)

General Enrollment Revocation

Name: Mobile Authentication only

Description: Mobile Authentication only

Title: Default Mobile Authentication only [Add more](#)

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)

Save

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.

The screenshot shows the OpenTrust CMS Mobile 2.0 interface. The main heading is "Create a new Mobile Management Profile - MDM". Below the heading is a yellow box with an information icon and the text "Please complete the form below." There is a "Back to list" link. The form has three tabs: "General", "Enrollment", and "Revocation". The "Enrollment" tab is active, showing "MDM Enrollment" and "Hide options". Below this, it says "Enrollment requests are processed through the MDM connector. User authentication is handled by the MDM itself." The "Identification Method" field has a dropdown menu open, showing the following options: "Choose a primary datasource...", "Choose a primary datasource...", "ACME Ltd MDM (Internal)", "MDM 1 (Internal)", "MDM demo call (Internal)", and "MDM - minimal fields (Internal)". A "Save" button is located at the bottom right of the form.

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.

The screenshot shows the OpenTrust CMS Mobile 2.0 interface. The main heading is "Edit a Mobile Management Profile - MDM". Below the heading is a yellow box with a warning icon and the text "Mobile Authentication only" is currently used by 35 mobile(s). There is a "Back to list" link. The form has three tabs: "General", "Enrollment", and "Revocation". The "Revocation" tab is active, showing "Revocation by an Administrator" with a checked checkbox. Below this, it says "Revocation can be requested by an Administrator." A "Save" button is located at the bottom right of the form.

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.cgi` where 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.

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: Retrieving Certificate from OpenTrust Certificate Authority](#), 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: Retrieving Certificate from OpenTrust Certificate Authority](#).
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](#).
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**.

Deploying OpenTrust S/MIME Certificates

Overview

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.

Workflow

1. Separate primary and secondary devices by assignment group.
 - Different assignment groups will need to be created 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. Navigate to **Devices > Certificates > Certificate Authorities > Request Templates** and select **Add**.
 - b. Select OpenTrust CA as the **Certificate Authority** and under **Profile Name** choose the corresponding OpenTrust profile for primary devices.
 - c. Configure any other settings required and select **Save**.
 - d. Similarly, 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.