

VMware AirWatch Integration with Entrust

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 Entrust IdentityGuard 3
 - System Requirements 3
 - High Level Design 4
- Chapter 2: Install, Set Up, Configure Certificate 5
 - Step 1: Configuring Entrust in Workspace ONE UEM 5
 - Step 2: Set Up Certificate Template for Entrust CA Type 6
- Chapter 3: Testing and Troubleshooting, Entrust 7

Chapter 1:

Workspace ONE UEM Integration with Entrust IdentityGuard

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 Entrust IdentityGuard services to issue certificates for your Workspace ONE UEM MDM solution.

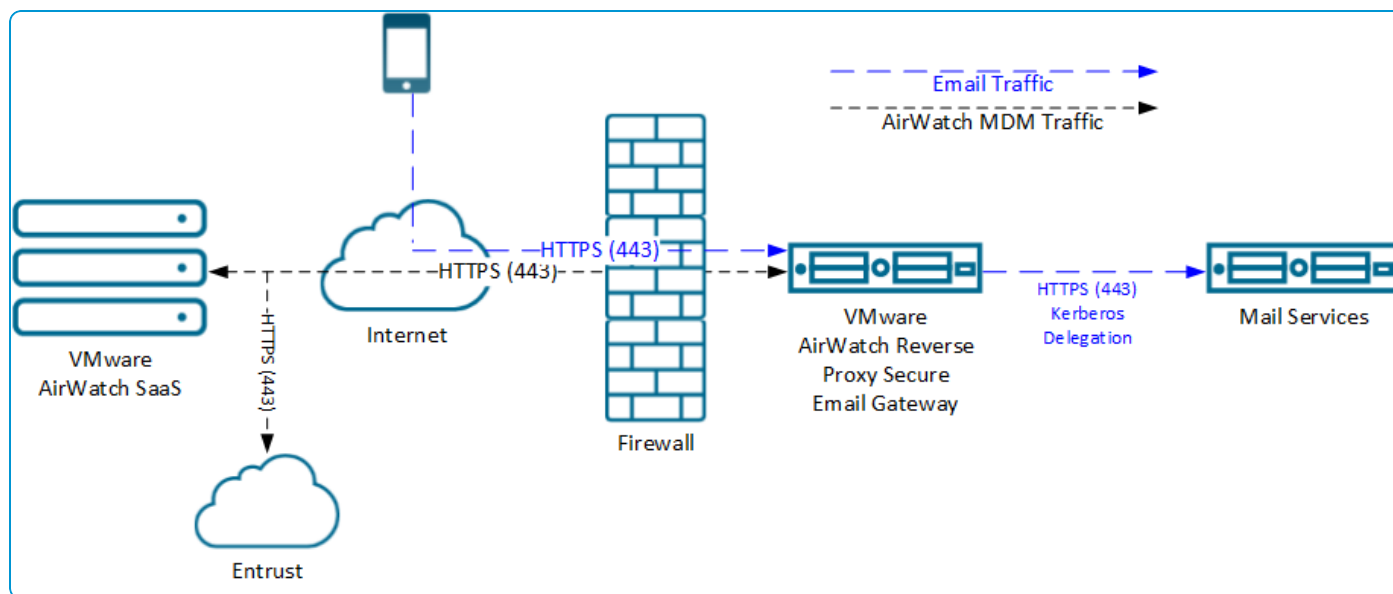
System Requirements

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

- Workspace ONE UEM version 8.0 or greater.
- VMware Enterprise Systems Connector is required if the Entrust IdentityGuard instance is installed behind a firewall.
- An Entrust IdentityGuard instance needs to be available.
- Configure Entrust IdentityGuard for mobile enrollment. Contact your Entrust representative to complete the following steps.
 1. Configure an Entrust Managed CA in Entrust IdentityGuard. Adding a Managed CA allows Entrust IdentityGuard to communicate with your Security Manager CA.
 2. Configure a Digital ID Configuration in Entrust IdentityGuard. A Digital ID Configuration is a template that Entrust IdentityGuard uses to issue digital IDs.
 3. Configure the Entrust IdentityGuard digital ID policies.
 4. Mirror the password rules set in Security Manager and Entrust IdentityGuard. If the password rules do not match, errors can occur when issuing digital IDs.
 5. Add an Entrust IdentityGuard administrator that your Workspace ONE UEM MDM will use to issue digital IDs.

High Level Design

This is an example of using Entrust IdentityGuard as a third-party certificate authority for Workspace ONE UEM in a SaaS environment. This diagram highlights one example of an entire communications flow, but for the purpose of this documentation, we are only discussing how a certificate is created and handled by OpenTrust, Workspace ONE UEM, and mobile devices. A detailed account of this interaction is shown below in the legend.



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: Configuring Entrust in Workspace ONE UEM

Now that you have configured Entrust IdentityGuard for mobile enrollment, Workspace ONE UEM can be configured to communicate with Entrust.

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. Enter in the **Name** field a unique name that identifies the Entrust certificate authority.
4. Select the **Authority Type** drop-down and select **Entrust**.
5. For **Protocol**, select either the **PKI** or **SCEP** radio button.
6. Enter in the **Server URL** field the URL of the Administration Services MDM Web Service or the Entrust IdentityGuard Administration Service. If you are using Entrust Managed Services PKI, this URL should have been provided to you by an Entrust representative. For example,
`https://mobile.example.com:19443/mdmws/services/AdminServiceV8.`
7. In the **Username** and **Password** settings, enter the user name of the Administration Services or Entrust IdentityGuard administrator you created while configuring Entrust. If you are using Entrust Managed Services PKI, this username and corresponding password should have been provided to you by an Entrust representative.
8. 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.

9. Select **Save**.

Step 2: Set Up Certificate Template for Entrust CA Type

Now that you have completed Step 1: Configuring Entrust in Workspace ONE UEM, Workspace ONE UEM is able to communicate with Entrust. 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 1: Configuring Entrust in Workspace ONE UEM.
4. Enter in the **Name** and **Description** fields the name you want to give the Entrust certificate template.
5. For **Managed CA**, select the name of the Certification Authority you configured in Entrust.
6. Click on the **Profile Name** drop-down and select the name of the Digital ID Configuration that you created while configuring Entrust. If you are using Entrust Managed Services PKI, this Digital ID Configuration should have been provided to you by an Entrust representative.
7. Configure **Subject Alternative Name (SAN)** attributes as required. These are used for additional unique identification of the device and need to match the Digital ID configuration.
8. If Workspace ONE UEM is going to automatically request the certificate to be reviewed by Entrust when it expires, check the **Automatic Certificate Renewal** check box and then enter in the **Auto Renewal Period (days)** setting the number of days prior to expiration before Workspace ONE UEM automatically requests Entrust to reissue the certificate.
9. If certificates need to be revoked either manually or when they are removed from the device, select **Enable Certificate Revocation**.
10. **Mandatory Fields** are used to form the common name of the distinguished name within the certificate. These fields can change depending on which Entrust profile you choose since the information within the profile may be different. The fields you see on the left side correspond to the data source fields you declared on the Entrust side. The values on the right are the Workspace ONE UEM variables. Enter **Lookup Values** in each of the fields that complement those fields in the Entrust profile. Make sure the lookup values you use match those used in the Digital ID configuration. If you are using Entrust Managed Services PKI, this information should have been provided to you by an Entrust representative.
11. Click **Save**.

Chapter 3:

Testing and Troubleshooting, Entrust

These testing and troubleshooting techniques are for SaaS, rather than on-premises deployments.

- If you are seeing the error, (40) Error AirWatch.CloudConnector.CertificateService.CertificateService.TestConnection, make sure you clean up stale profiles and increase the size of MaxReceivedMessageSize and MaxBufferSize to 2147483647.