Workspace ONE UEM Integration with EJB Certificate Authority

VMware Workspace ONE UEM 1811

vmware®

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 EJBCA

1

Workspace ONE UEM is flexible with PKI integration by being able to request certificates from either internal or external certificate authorities (CA). This documentation explains how to integrate with Enterprise Java Beans Certificate Authority (EJBCA) services to issue certificates for your Workspace ONE UEM MDM solution.

This chapter includes the following topics:

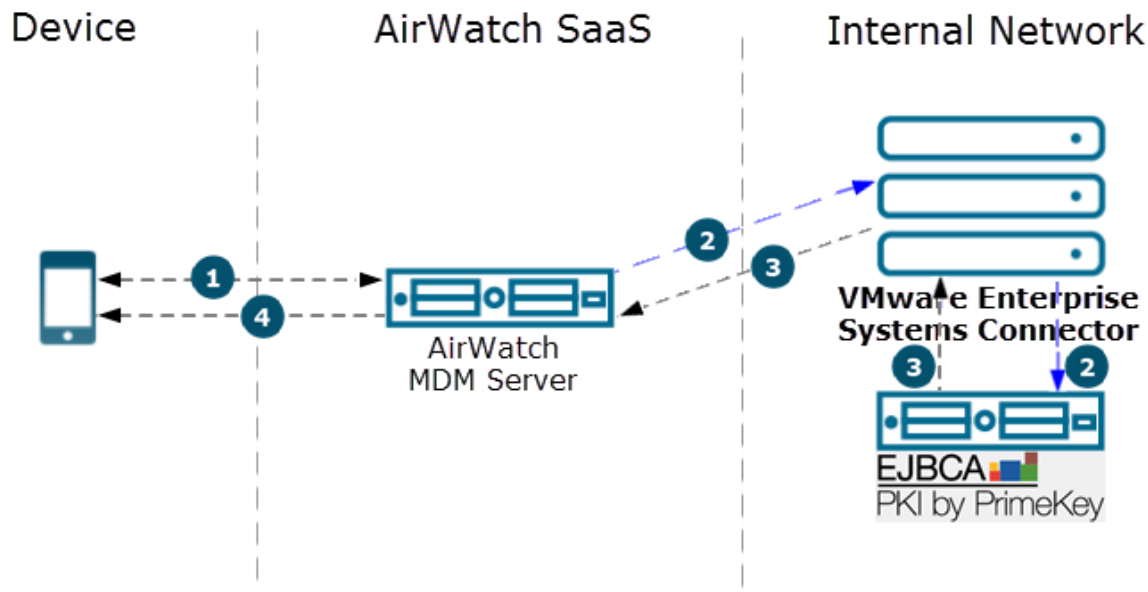
System Requirements

- A EJBCA instance that is configured for certificate deployment.
- Workspace ONE UEM console version 9.1 or higher.
- If your EJBCA appliance is public-facing, it must be protected with a Public SSL Certificate. If you are using VMware Enterprise System Connector for enterprise integration, then it needs to be configured to trust the root certificate installed on your EJBCA appliance.

High Level Design

In order for Workspace ONE UEM to communicate with Enterprise Java Beans Certificate Authority (EJBCA) for certificate distribution, you must have an EJBCA instance configured and ready to issue certificates. You can then configure Workspace ONE UEM to communicate with EJBCA using certificate based authentication. Once communication is successfully established, you can define how to deploy certificates to devices. Below are some of the examples of how EJBCA and Workspace ONE UEM can be configured.

Scenario 1: Workspace ONE UEM SaaS with EJBCA installed on-premises



1 Device enrolls with Workspace ONE UEM.

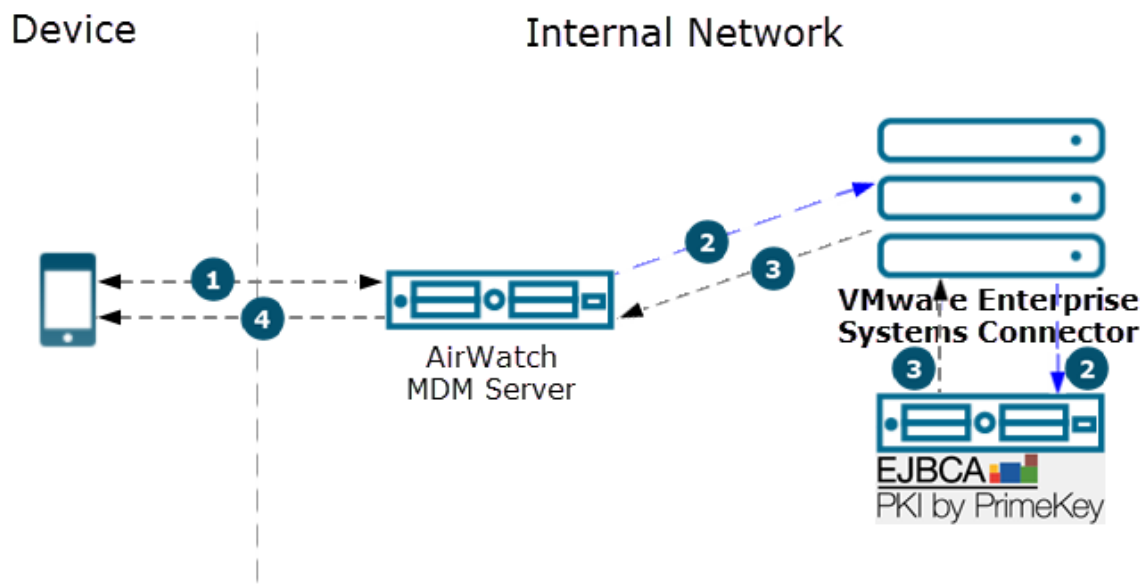
2 Workspace ONE UEM requests certificate from EJBCA endpoint (optionally through the VMware Enterprise System Connector).

3 EJBCA endpoint delivers the certificate to Workspace ONE UEM (optionally through the VMware Enterprise System Connector).

4 Workspace ONE UEM delivers the certificate to the device as part of an EAS, VPN, or WiFi profile.

If your EJBCA endpoint is public-facing, then it must be protected by a public SSL certificate. If you are using VMware Enterprise Systems Connector, then it needs to be configured to trust the root certificate installed on your EJBCA appliance. See Configuring VMware Enterprise Systems Connector to trust EJBCA for more information.

Scenario 2: Workspace ONE UEM and EJBCA both installed on-premises



1 Device enrolls with Workspace ONE UEM.

2 Workspace ONE UEM requests certificate from EJBCA endpoint (optionally through the VMware Enterprise System Connector).

3 EJBCA endpoint delivers the certificate to Workspace ONE UEM (optionally through the VMware Enterprise System Connector).

4 Workspace ONE UEM delivers the certificate to the device as part of an EAS, VPN, or WiFi profile.

If your EJBCA endpoint is public-facing, then it must be protected by a public SSL certificate. If you are using VMware Enterprise Systems Connector, then it needs to be configured to trust the root certificate installed on your EJBCA appliance. See Configuring VMware Enterprise Systems Connector to trust EJBCA for more information.

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: Configure EJBCA Certificate Authority

After you generate an EJBCA certificate, Workspace ONE UEM can be configured to communicate with EJBCA.

1 Navigate to **Devices > Certificates > Certificate Authorities**.

2 Click **Add**.

3 Select **EJBCA** from the **Authority Type** drop-down menu.

4 Enter a unique name and description that identifies the EJBCA certificate authority in the **Certificate Authority** and **Description** fields.

5 In the **Server URL** field enter the URL of your EJBCA instance.

This is the web endpoint that Workspace ONE UEM will use to submit requests and issue certificates.

6 Select the **Upload** button in the **Client Certificate** field and upload the new certificate from the location on your PC to which it has been saved.

7 Click **Save**.

8 Click **Test Connection** when complete to verify the test is successful. An error message appears indicating the problem if the connection fails.

Step 2: Set Up Certificate Template for EJBCA Type

Now that you have configured EJBCA, communication with Workspace ONE UEM is possible. 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 to set up a template.

1 Navigate to **Devices > Certificates > Certificate Authorities**.

2 Select the **Request Templates** tab.

3 Click **Add**.

4 Select **EJBCA** from the **Certificate Authority** drop-down menu.

5 Enter the **Name** for the EJBCA Request Template.

6 Enter a **Description** to help you identify the EJBCA certificate template.

7 Select the **End Entity Profile**, which defines those parts of the DN that require registration.

8 Select the **Certificate Profile**, which defines the actual certificate profile/template.

9 Select the **Available CA** which is the CA that issues the certificates.

10 Enter the **Subject Name**, which is the identity bound to the certificate.

11 Select the **Automatic Certificate Renewal** checkbox if Workspace ONE UEM is going to automatically request the certificate to be renewed by EJBCA when it expires. If you select this option, enter the number of days prior to expiration before Workspace ONE UEM automatically requests EJBCA to reissue the certificate in the **Auto Renewal Period (days)** field. This requires the certificate profile on EJBCA to have the **Duplicated Certificates** setting enabled.

12 Select the **Enable Certificate Revocation** checkbox if you want Workspace ONE UEM to be able to revoke certificates.

13 Click **Save**.

Step 3 Deploy a Certificate Profile to a Device

Now that the EJBCA certificate authority and certificate template settings have been properly configured in Workspace ONE UEM, configure Workspace ONE UEM profiles (payloads). Once either of these profiles is created, you can create additional payloads that the EJBCA certificate can use, such as Exchange ActiveSync (EAS), VPN, or Wi-Fi services.

Procedure

1 Navigate to **Devices > Profiles > List View**.

2 Click **Add**.

3 Select the applicable platform for the device type.

4 Specify all **General** profile parameters for organization group, deployment type, etc.

5 Select **Credentials** from the payload options.

6 Click **Configure**.

7 Select **Defined Certificate Authority** from the **Credential Source** drop-down menu.

8 Select the external EJBCA certificate you created previously in Step 1: Configure EJBCA Certificate Authority from the **Certificate Authority** drop-down menu.

9 Select the certificate template for EJBCA you created previously in Step 2: Set Up Certificate Template for EJBCA Typefrom the **Certificate Template** drop-down menu.

What to do next

Saving and publishing the profile would deploy a certificate to the device. If you plan on using the certificate on the device for Wi-Fi, VPN, or email purposes, you should also configure the respective payload in the same profile to leverage the certificate being deployed.

Note For step-by-step instructions on configuring these payloads, refer to the applicable Platform Guides.

Testing and Troubleshooting, EJBCA

3

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

Verify Ability to Perform Certificate Authentication without Workspace ONE UEM

Remove Workspace ONE UEM from the configuration and manually configure a device to connect to your network server using certificate authentication. This should work outside of Workspace ONE UEM and until this works properly, Workspace ONE UEM will not be able to configure a device to connect with a certificate.

Verify Ability to Perform Certificate Authentication with Workspace ONE UEM

You can confirm that the certificate is usable by pushing a profile to the device and testing whether or not the device is able to connect and sync to the configured EAS, VPN, or Wi-Fi access-point. If the device is not connecting and shows a message that the certificate cannot be authenticated or the account cannot connect then there is a problem in the configuration. Below are some helpful troubleshooting checks.

If SSL TLS errors are received while creating a template

This error can occur when you attempt to:

- Create a Workspace ONE UEM certificate template by selecting the Retrieve Profiles button or
- Retrieve a certificate from the Workspace ONE UEM console from the EJBCA certificate authority.

The troubleshooting technique that usually resolves this problem is:

- Adding the required server certificate chain in the console servers trusted root key store.

If the Workspace ONE UEM Certificate Profile fails to install on the device

- Inform Workspace ONE UEM Professional Services of the error and request they:
  - Turn on Verbose Mode to capture additional data.

    - Retrieve web console log.
- Workspace ONE UEM analyzes the log and works with customer to resolve the problem.

If the certificate is not populated in the View XML option of the profile

- Confirm that lookup values configured on the EJBCA certificate profile match the look up values in the Workspace ONE UEM console Request Template.
- Confirm that lookup values in Workspace ONE UEM Request Template are actually populated in the user information being pulled from AD.
- Confirm you are pointing to the right profile in EJBCA.

Configuring VMware Enterprise Systems Connector to Trust the EJBCA Appliance

4

If you are using VMware Enterprise Systems Connector and the EJBCA appliance is not public-facing, then you need to follow the instructions below to ensure the VMware Enterprise Systems Connector configuration trusts the appliance.

1 Open the EJBCA console certificate and view the **Certificate Path** tab.
   a If multiple certificates are listed, they will need to be separated and added to the appropriate stores.
   b The remaining steps address adding the root certificate to the Trust Root Store.
2 Open MMC by searching for it using Windows Search and launching the **mmc.exe** file.
3 Navigate to **File > Add/Remove Snap-in**. The Add or Remove Snap-ins screen displays.
4 Select the **Certificates** snap-in in the left pane and select **Add**.
5 Select **Computer account** as Snap-in source. Select **Next**.
6 Select **Local computer** and then select **Finish**.
7 Select **OK**.
8 Expand the newly added **Certificates** tree.
9 Expand the **Trusted Root Certification Authorities** folder.
10 Right-click the **Certificates** folder here and select **All Tasks > Import**.
11 Proceed through the Certificate Import Wizard. You will be prompted to Browse and select the file of the root certificate used to generate the EJBCA Console certificate. Select **Next**.
12 Select Place all certs in the following store and then select **Next**.
13 Click **Finish**.
14 Repeat steps 8-13 for all other intermediate and child certificates to add them to their associated stores.

The import completes and the Certificate Store displays, where you can see the certificate you just installed.