

Workspace ONE UEM Certificate Authority Integration with JCCH

VMware Workspace ONE UEM 1902



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

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1** Workspace ONE UEM Integration with JCCH 4
 - System Requirements 4
 - High Level Design 4
- 2** Install, Set Up, Configure Certificate 6
 - Step 1 Configure JCCH Certificate Authority 6
 - Step 2 Set Up Certificate Template for JCCH CA Type 7
 - Step 3 Deploy a Certificate Profile to a Device 7
- 3** Testing and Troubleshooting, JCCH 9
- 4** Configuring VMware Enterprise Systems Connector to Trust the JCCH Appliance 11

Workspace ONE UEM Integration with JCCH

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 JCCH Gléas services to issue certificates for your Workspace ONE UEM EMM solution.

This chapter includes the following topics:

- [System Requirements](#)
- [High Level Design](#)

System Requirements

- A JCCH instance that is configured for certificate deployment.
- Workspace ONE UEM console version 8.0 or higher.
- If your JCCH appliance is public-facing, it must be protected with a Public SSL Certificate. If you are using Workspace ONE UEM Cloud Connector (ACC) for enterprise integration, then ACC needs to be configured to trust the root certificate installed on your JCCH appliance.

High Level Design

In order for Workspace ONE UEM to communicate with JCCH for certificate distribution, you must have a JCCH instance configured and ready to issue certificates. You can then configure Workspace ONE UEM to communicate with JCCH using basic authentication. Once communication is successfully established, you can define how to deploy certificates to devices. Below are some of the examples of how JCCH and Workspace ONE UEM can be deployed.

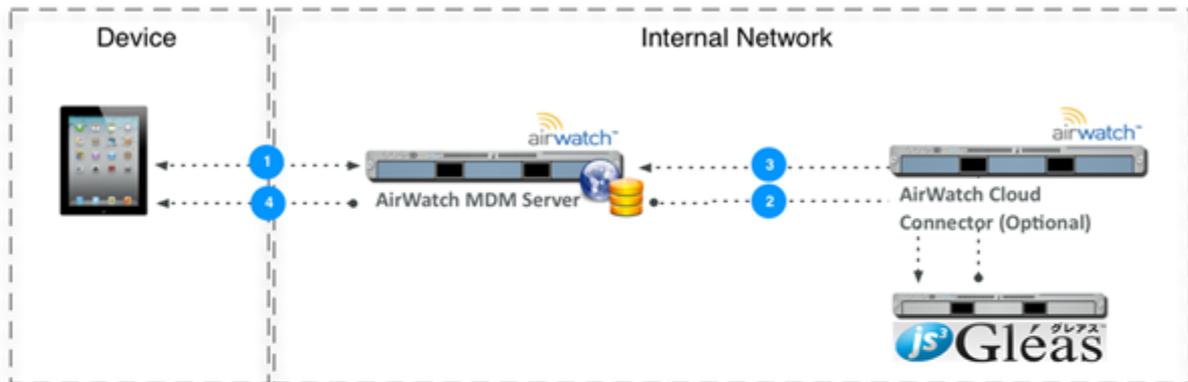
Scenario 1: AirWatch SaaS with JCCH Gléas installed on-premise



1. Device enrolls with AirWatch.
2. AirWatch requests certificate from JCCH Gléas endpoint (optionally through the ACC).
3. JCCH Gléas endpoint delivers the certificate to AirWatch (optionally through the ACC).
4. AirWatch delivers the certificate to the device as part of an EAS, VPN, or Wi-Fi profile.

Note: If your JCCH Gléas endpoint is public-facing, then it must be protected by a Public SSL Certificate. If you are using AirWatch Cloud Connector (ACC), then ACC needs to be configured to trust the root certificate installed on your JCCH Gléas appliance. See "Configuring ACC to Trust JCCH Gléas" for more information.

Scenario 2: AirWatch and JCCH Gléas both installed on-premise



1. Device enrolls with AirWatch.
2. AirWatch requests certificate from JCCH Gléas endpoint (optionally through the ACC).
3. JCCH Gléas endpoint delivers the certificate to AirWatch (optionally through the ACC).
4. AirWatch delivers the certificate to the device as part of an EAS, VPN, or Wi-Fi profile.

Note: If your JCCH Gléas endpoint is public-facing, then it must be protected by a Public SSL Certificate. If you are using AirWatch Cloud Connector (ACC), then ACC needs to be configured to trust the root certificate installed on your JCCH Gléas appliance. See "Configuring ACC to Trust JCCH Gléas" 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 JCCH Certificate Authority](#)
- [Step 2 Set Up Certificate Template for JCCH CA Type](#)
- [Step 3 Deploy a Certificate Profile to a Device](#)

Step 1 Configure JCCH Certificate Authority

After you generate a JCCH Gléas certificate, Workspace ONE UEM can be configured to communicate with JCCH.

- 1 Navigate to **Devices > Certificates > Certificate Authorities**.
- 2 Click **Add**.
- 3 Select **JCCH Gléas** from the **Authority Type** drop-down menu.
- 4 Enter a unique name and description that identifies the JCCH certificate authority in the **Certificate Authority** and **Description** fields.
- 5 In the **Server URL** field enter the URL of your JCCH 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 JCCH CA Type

Now that you have configured JCCH Certificate Authority, Workspace ONE UEM is able to communicate with JCCH. 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 **JCCH Gléas** from the **Certificate Authority** drop-down menu.
- 5 Enter the **Name** for the JCCH Request Template.
- 6 Enter a **Description** to help you identify the JCCH certificate template.
- 7 Enter the **Profile ID**, which corresponds to the profile identity bound to the certificate.
- 8 Enter the **Product Code**, which is the code bound to the certificate/template/license.
- 9 Select the **Validity Period** in years, which is the time period the certificate/template/license will be valid.
- 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 JCCH when it expires. If you select this option, enter the number of days prior to expiration before Workspace ONE UEM automatically requests JCCH to reissue the certificate in the **Auto Renewal Period (days)** field. This requires the certificate profile on JCCH 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 JCCH certificate authority and certificate template settings have been properly configured in Workspace ONE UEM, the final step is to configure Workspace ONE UEM profiles (payloads). Once either of these profiles is created, you can create additional payloads that the JCCH certificate can use, such as Exchange ActiveSync (EAS), VPN, or Wi-Fi services.

Configure a PKI Credential Payload

- 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 JCCH CA you created previously in [Step 1 Configure JCCH Certificate Authority](#) from the **Certificate Authority** drop-down menu.
- 9 Select the certificate template for JCCH you created previously in [Step 2 Set Up Certificate Template for JCCH CA Type](#) from the **Certificate Template** drop-down menu.

At this point, saving and publishing the profile would deploy a certificate to the device. However, if you plan on using the certificate on the device for Wi-Fi, VPN, or email purposes, then you should also configure the respective payload in the same profile to leverage the certificate being deployed. For step-by-step instructions on configuring these payloads, refer to the applicable Platform Guides.

Testing and Troubleshooting, JCCH

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 JCCH 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 JCCH certificate profile match the look up values in the Workspace ONE UEM console Request Template.
- Confirm that lookup values in the 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 JCCH.

Configuring VMware Enterprise Systems Connector to Trust the JCCH Appliance

4

If you are using VMware Enterprise Systems Connector and the JCCH 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 JCCH 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 JCCH 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.