VMware AirWatch Integration with SecureAuth PKI Guide

For VMware AirWatch

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

Table of Contents

Chapter 1:
Workspace ONE UEM Integration with SecureAuth PKI Guide

Workspace ONE UEM is flexible with PKI integration by being able to request certificates from either internal or external certificate authorities (CA). This document explains how to integrate with SecureAuth PKI services to issue certificates for your Workspace ONE UEM MDM solution.

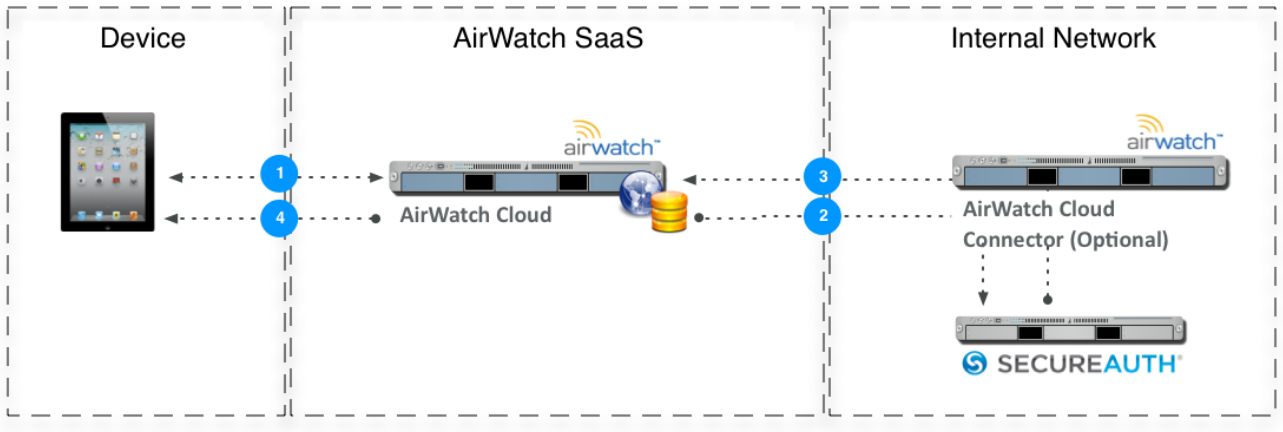
System Requirements

- A SecureAuth instance that is configured for certificate deployment.
- Workspace ONE UEM console version 7.2 or higher.
- If your SecureAuth 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 SecureAuth appliance.

High Level Design

In order for Workspace ONE UEM to communicate with SecureAuth for certificate distribution, you must have a SecureAuth instance configured and ready to issue certificates. You can then configure Workspace ONE UEM to communicate with SecureAuth 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 SecureAuth and Workspace ONE UEM can be deployed.

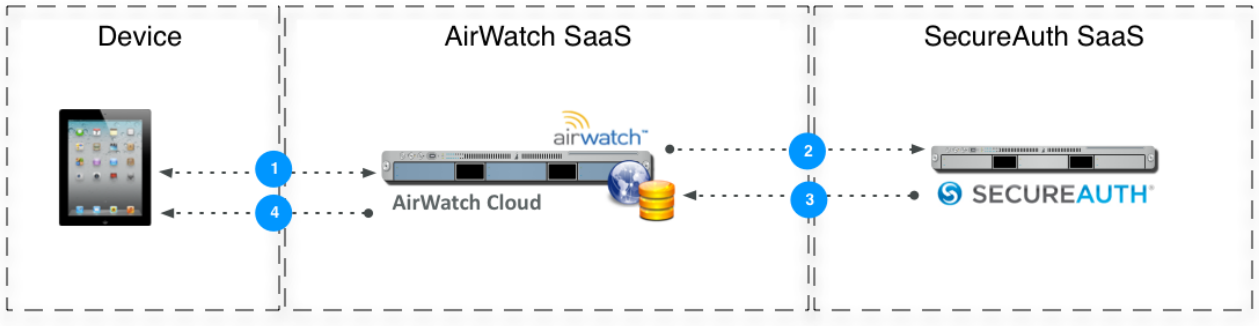
Scenario 1: AirWatch SaaS with SecureAuth installed on-premise



1. Device enrolls with AirWatch.
2. AirWatch requests certificate from SecureAuth endpoint (optionally through the ACC).
3. SecureAuth 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.

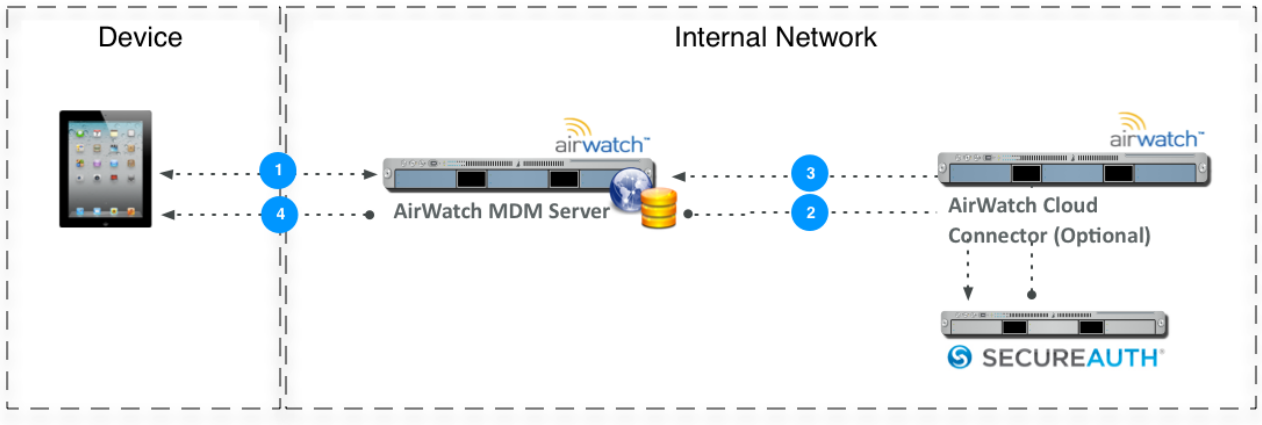
Note: If your SecureAuth endpoint is public-facing, then it must be protected by a Public SSL Certificate. If you are using AirWatch Cloud Connector (ACC), then ACC needs to be configured to trust the root certificate installed on your SecureAuth appliance. See "Configuring ACC to Trust SecureAuth" for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

Scenario 2: AirWatch SaaS and SecureAuth SaaS



1. Device enrolls with AirWatch.
2. AirWatch requests certificate from SecureAuth endpoint.
3. SecureAuth endpoint delivers the certificate to AirWatch.
4. AirWatch delivers the certificate to the device as part of an EAS, VPN, or Wi-Fi profile.

Scenario 3: AirWatch and SecureAuth both installed on-premise



1. Device enrolls with AirWatch.
2. AirWatch requests certificate from SecureAuth endpoint (optionally through the ACC).
3. SecureAuth 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 SecureAuth 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 SecureAuth appliance. See "Configuring ACC to Trust SecureAuth" for more information.

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: Retrieve Certificate from SecureAuth Certificate Authority

After you generate a SecureAuth MPKI RA certificate, Workspace ONE UEM can be configured to communicate with SecureAuth.

1. Navigate to **Devices > Certificates > Certificate Authorities**.
2. Click **Add**.
3. Select **SecureAuth** from the **Authority Type** drop-down menu.
4. Enter a unique name and description that identifies the SecureAuth certificate authority in the **Certificate Authority** and **Description fields**.
5. In the **Server URL** field enter `https://<SecureAuth_FQDN>/SecureAuthX/webservice/certificateissuerws.svc`, where `<SecureAuth_FQDN>` is the URL of your SecureAuth instance and the “X” in “SecureAuthX” is the realm instance number that is configured for certificates.

   This is the web endpoint that Workspace ONE UEM will use to submit requests and issue certificates.
6. Enter the **Company GUID**, which at the time of this writing can be found by logging in to your SecureAuth admin portal, navigating to the **System Information** tab, and scrolling down to the **License Info** section where you can view your **Company GUID**.
7. Enter the **Username** and **Password** fields, which can be found by logging in to your SecureAuth admin portal, navigating to the **Workflow** tab, and scrolling down to the **FBA WebService** section.
8. Click **Save**.
9. Click **Test Connection** when complete to verify the test is successful. An error message appears indicating the problem if the connection fails.
10. Click **Save**.

Step 2: Set Up Certificate Template for SecureAuth CA Type

Now that you have completed Retrieving Certificate from SecureAuth Certificate Authority, Workspace ONE UEM is able to communicate with SecureAuth. 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. Navigate to **Devices > Certificates > Certificate Authorities**.
2. Select the **Request Templates** tab.
3. Click **Add**.
4. Select **SecureAuth** from the **Certificate Authority** drop-down menu.
5. Enter the **Name** for the SecureAuth Request Template.
6. Enter a **Description** to help you identify the SecureAuth certificate template.
7. Enter the **Subject Name**, which is the identity bound to the certificate.
8. Select the **Key Pair Generation Location**, which can be either **Workspace ONE UEM** or **SecureAuth**. This is where the key pair is generated – either on the SecureAuth side or on the Workspace ONE UEM side. Workspace ONE UEM recommends selecting SecureAuth because it is the simpler configuration.
    - When you select SecureAuth, it will generate the certificate and the private key and return it back to Workspace ONE UEM with its root certificate. The root certificate and user certificate are combined into a single cert and sent to the device to install.
    - When you select Workspace ONE UEM, you have a few more fields to configure: the **Certificate Validity Period**, which is the length of time the certificate is valid for in days (Workspace ONE UEM recommends the value 365), and the **Private Key Length**, which is how secure you want the keys to be (Workspace ONE UEM recommends 2048 as the key length).
9. For **Private Key Type**, select if the certificate can be used for signing and encryption operations or both.
10. Select the **Automatic Certificate Renewal** checkbox if Workspace ONE UEM is going to automatically request the certificate to be renewed by SecureAuth when it expires. If you select this option, enter the number of days prior to expiration before Workspace ONE UEM automatically requests SecureAuth to reissue the certificate in the **Auto Renewal Period (days)** field. This requires the certificate profile on SecureAuth to have the **Duplicated Certificates** setting enabled.
11. Select the **Enable Certificate Revocation** checkbox if you want Workspace ONE UEM to be able to revoke certificates.
12. Click **Save**.

Step 3: Deploy a Certificate Profile to a Device

Now that the SecureAuth 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) for either PKI or SCEP. If in Retrieving Certificate from SecureAuth certificate authority, you chose PKI then you only need to configure a Credentials

profile. Once either of these profiles are created, you can create additional payloads that the SecureAuth 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 SecureAuth CA you created previously in Retrieving Certificate from SecureAuth Certificate Authority from the **Certificate Authority** drop-down menu.
9. Select the certificate template for SecureAuth you created previously in Setup Certificate Template for SecureAuth 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.

Chapter 3:
Testing & Troubleshooting

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

Chapter 4:
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.

Chapter 5:
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 byselecting the Retrieve Profiles button or
- Retrieve a certificate from the Workspace ONE UEM console from the SecureAuth 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 SecureAuth certificate profile match the look up values in the Workspace ONE UEM console's 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 SecureAuth.

Appendix:
Configure ACC to Trust the SecureAuth Appliance

If you are using ACC and the SecureAuth appliance is not public-facing, then you need follow the instructions below to ensure it trusts the appliance.

1. Open MMC by searching for it using Windows Search and launching the **mmc.exe** file.
2. Navigate to **File > Add/Remove Snap-in**. The Add or Remove Snap-ins screen displays.
3. Select the **Certificates** snap-in in the left pane and select **Add**.
4. Select **Computer account** as Snap in source. Select **Next**.
5. Select **Local computer**. Select **Finish**.
6. Select **OK**.
7. Expand the newly added **Certificates** tree.
8. Expand the **Trusted Root Certification Authorities** folder.
9. Right-click the **Certificates** folder here and select **All Tasks > Import**.
10. Proceed through the Certificate Import Wizard. You will be prompted to Browse and select the file of the root certificate used to generate the SecureAuth SSL certificate. Select Next.
11. Select Place all certs in the following store. Select **Next**.
12. Click **Finish**.

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