VMware AirWatch Integration with RSA 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 RSA 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 RSA PKI services to issue certificates for your Workspace ONE UEM MDM solution.

System Requirements

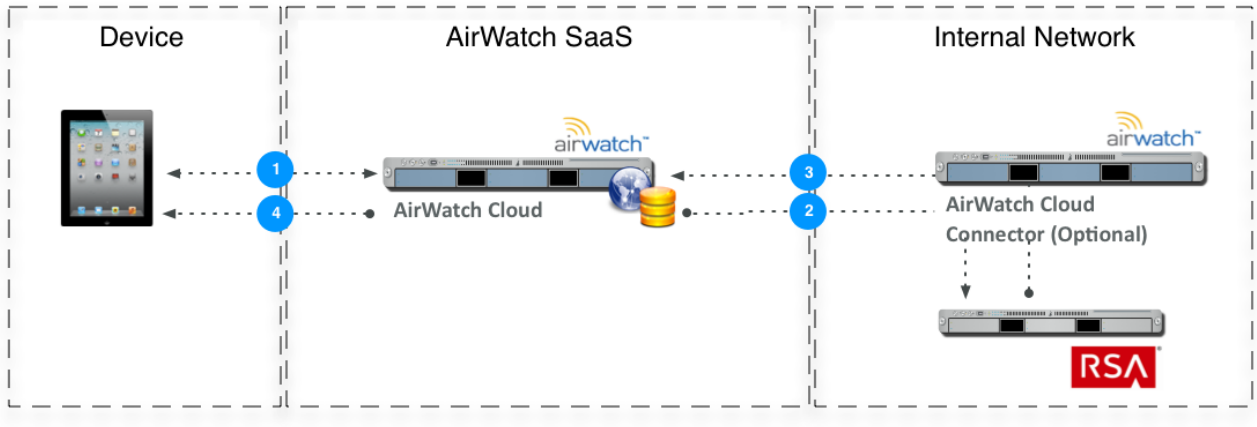
- RSA Certificate Manager 6.9 Build 555+ required.
- REST API support in RSA must be enabled.
- Workspace ONE UEM console version 7.3.1 or higher.
- If your RSA appliance is public-facing, it must be protected with a Public SSL Certificate. If you are using Workspace ONE UEM Cloud Connector (ACC) for enterprise integration, then ACC needs to be configured to trust the root certificate installed on your RSA appliance.

> **Important:** The Enterprise Integration Service (EIS) is not supported for integration between Workspace ONE UEM and RSA. You must be using the Workspace ONE UEM Cloud Connector.

High Level Diagram

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

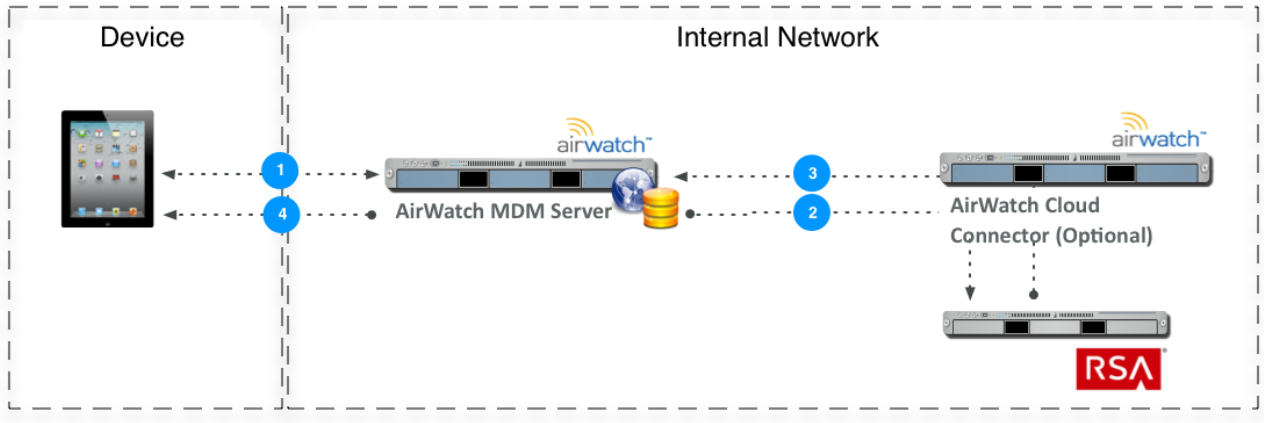
Scenario 1: AirWatch SaaS with RSA installed on-premise



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

Scenario 2: AirWatch and RSA both installed on-premise



1. Device enrolls with AirWatch.
2. AirWatch requests certificate from RSA endpoint (optionally through the ACC).
3. RSA 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 RSA 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 RSA appliance. See "Configuring ACC to Trust RSA" 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: Add the RSA Certificate Authority, Workspace ONE UEM Config

Now that you have the requisite information from RSA, you can perform the integration from the Workspace ONE UEM console. This includes adding the certificate authority, configuring a Request Template, and deploying a Wi-Fi, VPN or EAS profile leveraging each.

1. Navigate to **Devices > Certificates > Certificate Authorities**.
2. Click **Add**.
3. Select **RSA Certificate Manager** from the **Authority Type** drop-down menu.
4. Enter a unique name and description that identifies the RSA certificate authority in the **Name** and **Description** fields.
5. In the **Server URL** field enter the server URL of your RSA instance, for example, `https://rsa.acme.com`.
   This is the web endpoint that Workspace ONE UEM will use to submit requests and issue certificates.
6. Enter the **Port**, which is the port configured on your RSA instance that is listening for API calls. This is the port you noted from Obtaining your Port Number.
7. Select **Upload** to upload the certificate you generated from Requesting an Authentication Certificate.
8. Click **Test Connection** when complete to verify connectivity between Workspace ONE UEM and RSA for authentication purposes. This does not indicate successful authentication, but rather that Workspace ONE UEM can successfully establish a connection. An error message appears indicating the problem if the connection fails.
9. Click **Save**.

Step 2: Set Up Certificate Template for RSA CA Type, Workspace ONE UEM Config

The next step is to define which certificate will be deployed to devices by setting up a certificate template in Workspace ONE UEM.

1. Navigate to **Devices > Certificates > Certificate Authorities**.
2. Select the **Request Templates** tab.
3. Click **Add**.
4. Enter the **Name** for the RSA Request Template.

5. Enter a **Description** to help you identify the RSA certificate template.
6. Select your **RSA CA** from the **Certificate Authority** drop-down menu.
7. Enter the **Jurisdiction**, which you generated by following Obtaining Your Jurisdiction ID.
8. Enter the **External Profile**, which you generated by following Obtaining Your Profile ID.
9. Enter the **Subject Name**, which is the identity bound to the certificate.
10. Enter the **Private Key Length**, which defaults to **2048**.
11. For **Private Key Type**, select if the certificate can be used for signing and encryption operations or both.
12. Select the **Automatic Certificate Renewal** checkbox if Workspace ONE UEM is going to automatically request the certificate to be renewed by RSA when it expires. If you select this option, enter the number of days prior to expiration before Workspace ONE UEM automatically requests RSA to reissue the certificate in the **Auto Renewal Period (days)** field. This requires the certificate profile on RSA to have the **Duplicated Certificates** setting enabled.
13. Select the **Enable Certificate Revocation** checkbox if you want Workspace ONE UEM to be able to revoke certificates.
14. Click **Save**.

> **Note:** The **San Type** and **Publish Private Key** options do not do anything at this time.

Step 3: Deploy a Certificate Profile to a Device, Workspace ONE UEM Config

Now that the RSA 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). If in Retrieving Certificate from RSA Certificate Authority (referenced in the fourth bullet in System Requirements), you chose **PKI** then you only need to configure a **Credentials** profile. Once either of these profiles is created, you can create additional payloads that the RSA certificate can use, such as Exchange ActiveSync (EAS), VPN, or Wi-Fi services.

Configuring 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 RSA CA you created previously in Retrieving Certificate from RSA certificate authority from the certificate authority drop-down menu.
9. Select the **Certificate Template** for RSA you created previously in Setup Certificate Template for RSA CA Type from

the certificate template drop-down menu.

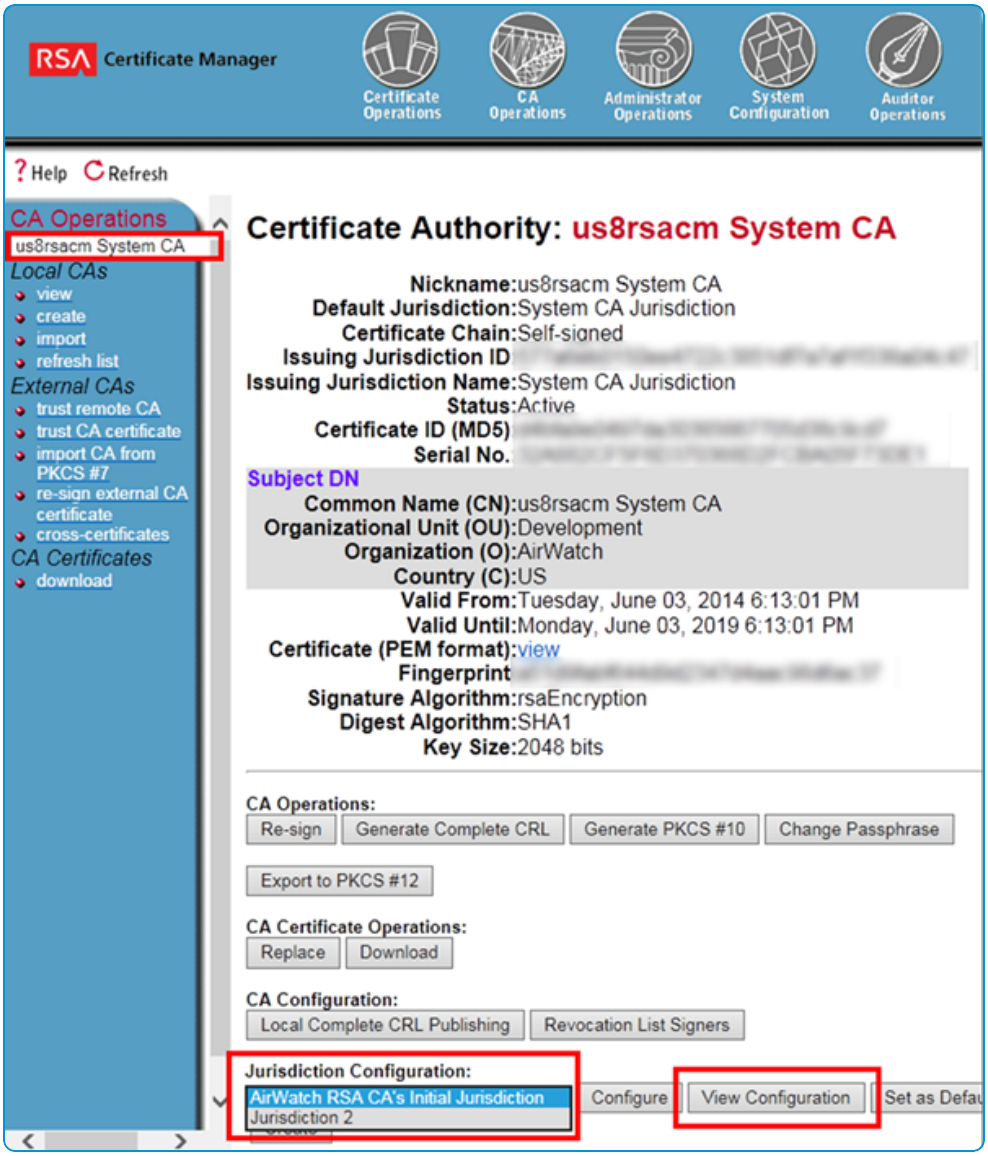
At this point, Saving and Publishing the profile would deploy a certificate to the device. However, if you plan on using the certificate on the device for Wi-Fi, VPN, or email purposes, then you should also configure the respective payload in the same profile to leverage the certificate being deployed.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

Step 1: Obtain Your Jurisdiction ID, RSA Config

The Jurisdiction ID is used by RSA to determine which CA to issue the certificate against. You will need this value when performing the next section's steps from the Workspace ONE UEM console.

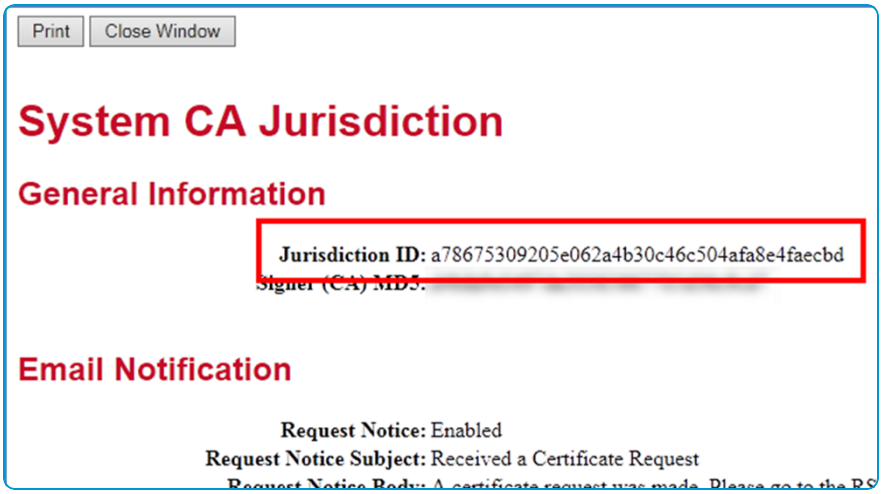
To view it:

1. Log in to the RSA CM Console.
2. Click on **CA Operations**.
3. On the left-hand column above **Local CAs**, select the appropriate CA from this drop-down list.:



4. Toward the bottom of the right-hand column under **Jurisdiction Configuration**, your jurisdictions appear in a drop-down listing. Select the appropriate jurisdiction and select the **View Configuration** button.

5. Copy the **Jurisdiction ID** that appears in the resulting **Jurisdiction** page.



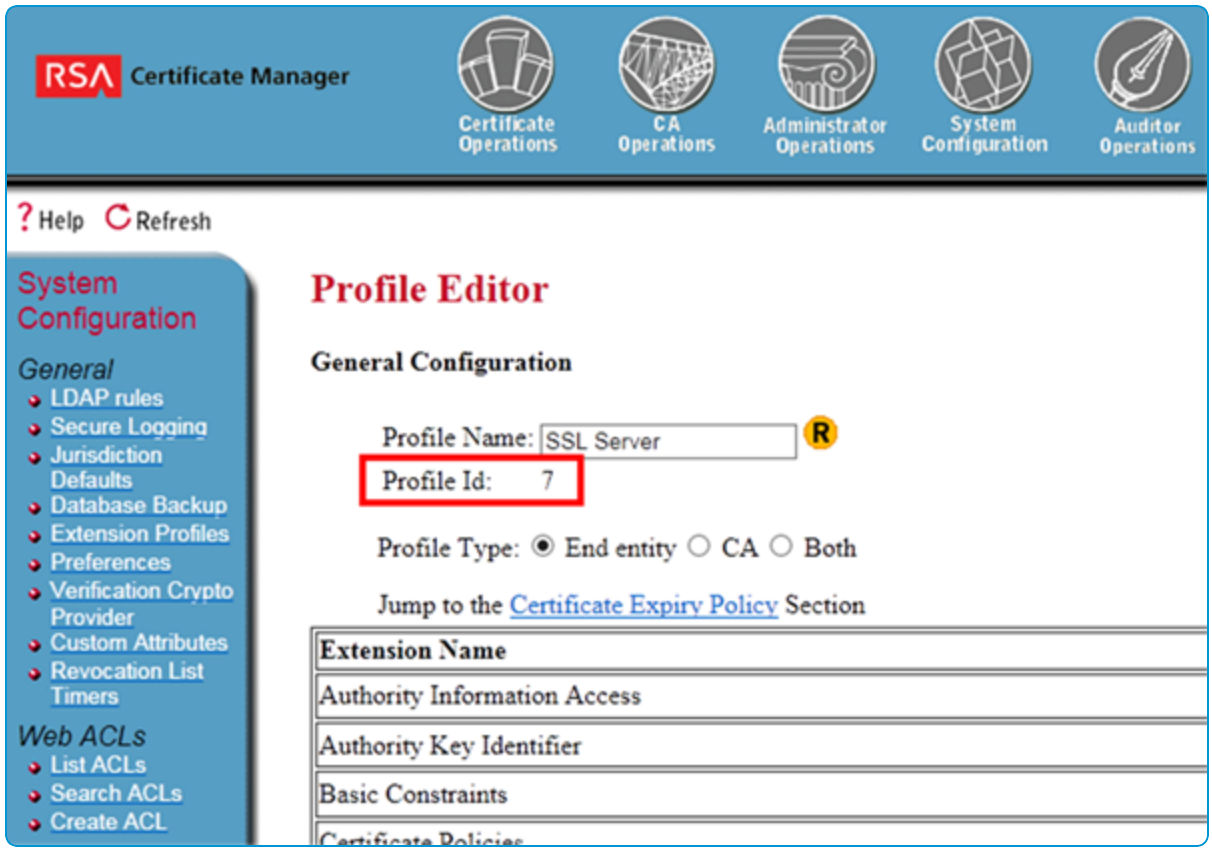
Step 2: Obtain Your Profile ID, RSA Config

The **Profile ID** is used by RSA to identify the profile you select in the **Profile Name** drop-down field. You will need this value when completing the next section's tasks.

Obtain the **Profile ID** by taking the following steps:

1. Log into the RSA CM Console.
2. Click on **System Configuration**.
3. On the left-hand column, select the General category menu item **Extension Profiles**.
4. Select a specific profile by choosing from the **Existing Profiles** drop-down field.
5. Click the **Edit** button.

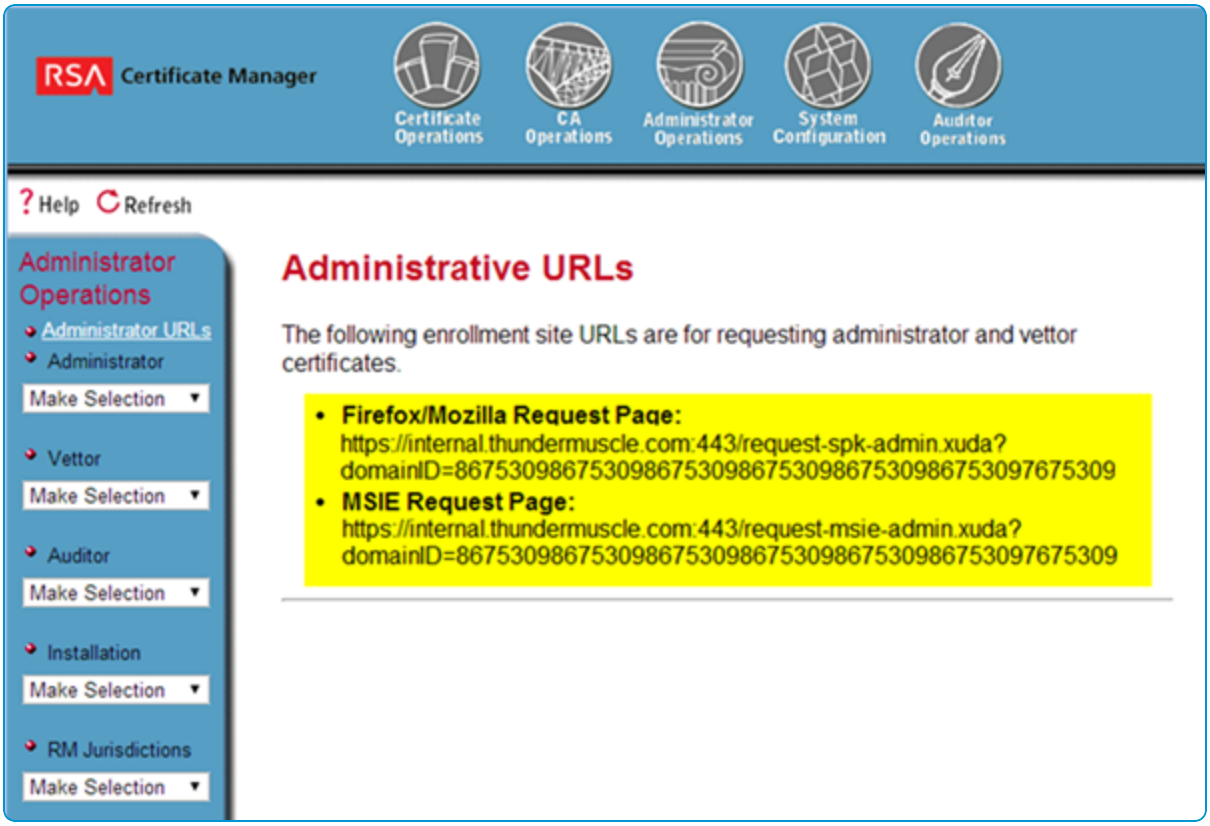
6. The **Profile ID** will be listed under the **Profile Name**. Take note of this number.



Step 3: Request an Authentication Certificate, RSA Config

The authentication certificate is used to authenticate requests from the Workspace ONE UEM console and needs to be uploaded when performing integration in the next section.

1. Log in to the RSA CM Console.
2. Click on **Administrator Operations**.
3. Click on **Administrator URLs**.
4. Copy either the **Firefox/Mozilla** URL if you intend to use Firefox or the **MSIE** URL if you intend to use Internet Explorer.



5. From either Firefox or IE (depending on which you copied) navigate to the URL you copied.
6. Complete the form that displays.
   a. For **Select Certificate Type**, select **Vettor Certificate**, which gives rights to request all non-admin CAs.
   b. Workspace ONE UEM recommends that you set the **key size** to **High Grade**.
   c. Your browser will generate the public and private key pair. Once it's complete, it will submit the request to your RSA CM. An administrator will need to manually approve this request. Once it's complete, you will receive an email with a link to proceed. If you are the administrator generating the certificate, perform the following:
7. Log in to the RSA CM Console.
8. Click on Administrator Options.
9. On the left-hand column, use the drop-down menu to select the appropriate CA.
10. Select **Request Active**.
11. Find the submitted request and select on the Common Name value that is in the **Request for** column.
12. Verify the submission is correct. Select the **appropriate jurisdictions** and then **Issue Certificate** at the bottom of the form.
13. Open the link that was emailed to the requestor using the same browser you used to submit the request. Then select on **Install Client Certificate**.

If successful, you should see a pop-up menu that says “Your personal certificate has been installed. You should keep a backup copy of this certificate.”

Next you need to export this certificate from your browser. The following steps are for Firefox.

a. Open the **Options** menu in your browser.

b. Click the **Advanced** tab.

c. Click **View Certificates**.

d. Select the appropriate certificate and select **Backup**.

e. Select where you want to save the file and name it.

f. Click **Save**.

g. Enter a password for the private key.

h. Finish the export process.

You have now generated your certificate. You will upload this into the Workspace ONE UEM console in the next section, where it will be used for submitting certificate requests.

Step 4: Obtain Port Number, RSA Config

The REST API listening port that you will need when performing integration in the next section can be found in your Apache httpd.conf file, provided that you are on RSA Certificate Manager 6.9 build 555 or higher. If you are not on this version, you will need to upgrade and follow RSA’s instructions to modify your Apache config file.

The port number you need to take note of is shown in the Apache config file, as shown below:

```
##########################################
###  RSA Rest Server configuration  ###
##########################################

###
# The following VirtualHost for a non-secure Web Server
###

Listen 450

<VirtualHost _default_:450>
ServerName rsa.airwlab.com
<Location /rcm>
SetHandler  rcm
</Location>

ErrorLog    logs/rest-error.log

SSLEngine on
SSLVerifyClient require
SSLVerifyDepth  10

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
SSLCipherSuite AES256-SHA
SSLProtocol +TLSv1
```

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 by selecting the Retrieve Profiles button or
- Retrieve a certificate from the Workspace ONE UEM console from the RSA 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 RSA 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 RSA.

Appendix:
Configure ACC to Trust the RSA Appliance

If you're using ACC and the RSA 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 RSA 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.