VMware AirWatch Integration with Symantec MPKI 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 Symantec MPKI Guide

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 Symantec MPKI services to issue certificates for your Workspace ONE UEM MDM solution.

System Requirements

- Symantec version 8.0 or higher
- A Symantec MPKI account
- Workspace ONE UEM version 7.0 +
- When using PKI protocol, verify the Symantec certificate profile(s) under Primary certificate options.

  Ensure Enrollment Method is set to PKI Web Services and Authentication method is set to 3rd party application. This gives Workspace ONE UEM the ability to deploy certificate profiles through APIs.
- When using SCEP protocol, verification that the Symantec certificate profile(s), under Primary certificate options, within Authentication method, has Enrollment Code selected. This gives the SCEP server the ability to deploy certificate profiles through APIs.

Implementation Approach

In order for Workspace ONE UEM to communicate with Symantec as a Registration Authority (RA), you must first establish an account with Symantec. After your Symantec account is active, you can generate an RA certificate and store it on the RA server.

Workspace ONE UEM can then be configured to use the certificate to communicate with the Symantec MPKI CA. Once communication is successfully established, you can define which certificate Workspace ONE UEM will deploy to the device.

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.

Generate a Symantec Registration Authority Certificate

First, use the Symantec PKI portal to generate a Registration Authority (RA) certificate. After Symantec creates the certificate, it is stored on the server, which can be any server you choose.

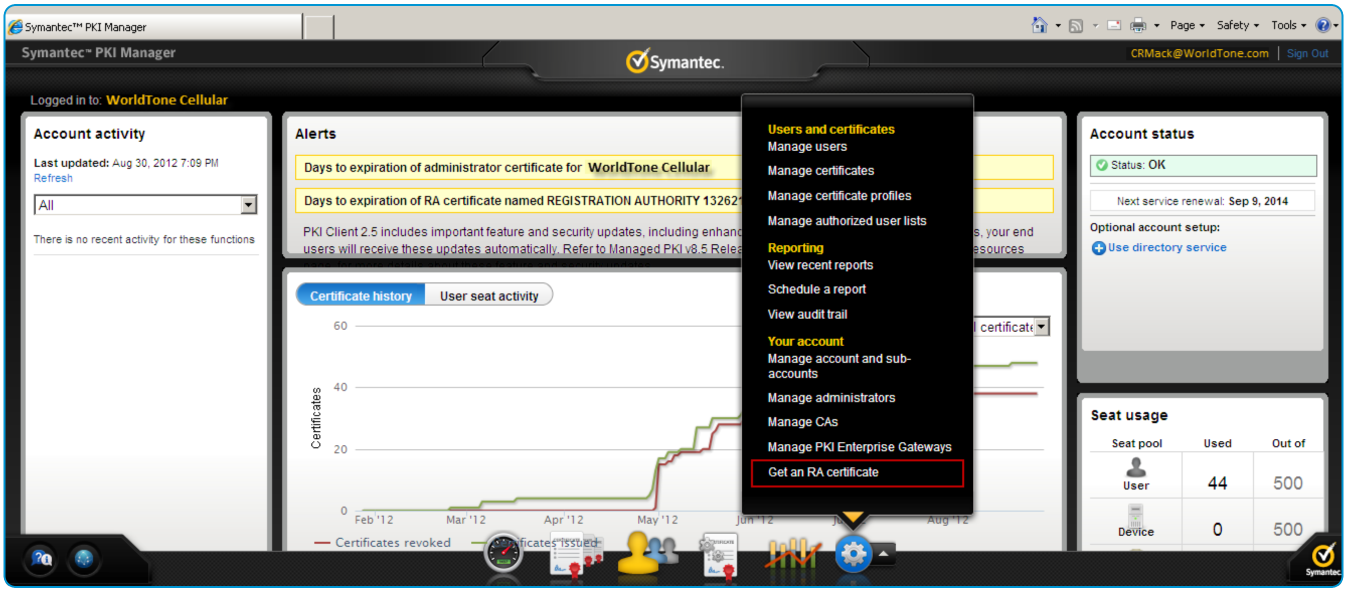
Generate a New RA Certificate using OpenSSL

1. Generate a new RSA key pair.

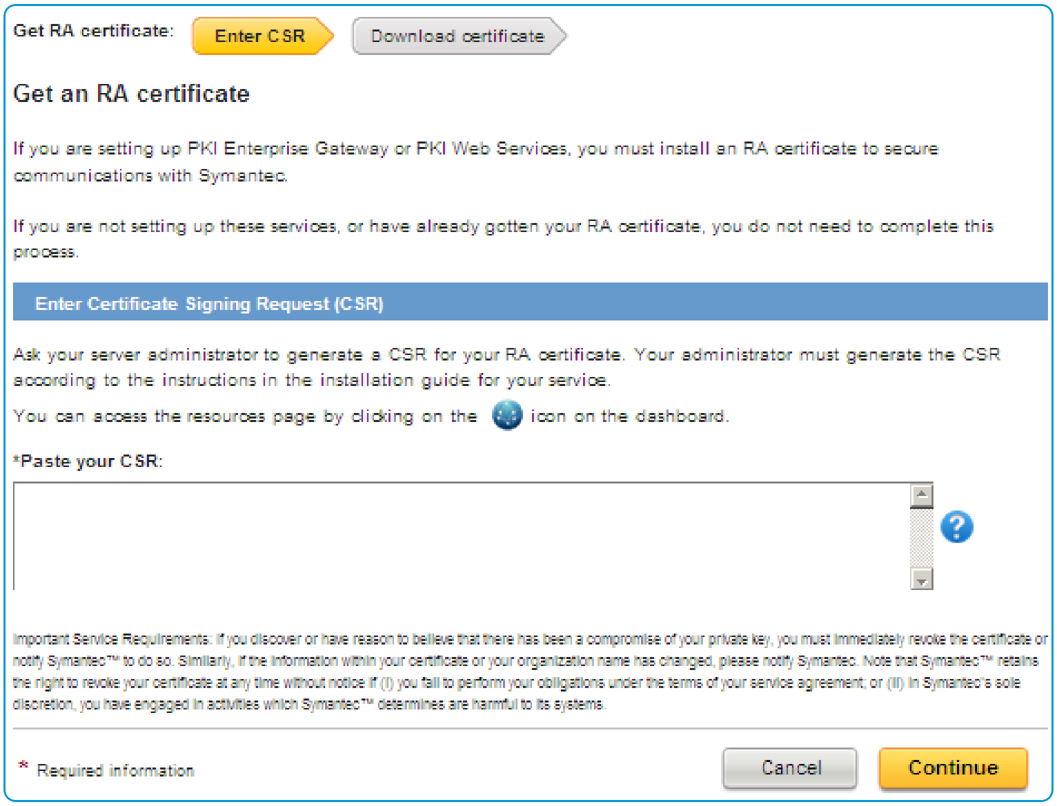
   Command:
   ```
   openssl req -new -newkey rsa:2048 -nodes -out AirWatch.csr -keyout
   AirWatch.key -subj
   /C=US/ST=Georgia/L=Atlanta/O=R&D/OU=R&D/CN=AirWatch
   ```

2. Log in to the Symantec PKI portal.

3. Click on **Tasks** (gear icon). Click on **Get a RA Certificate**.


Symantec™ PKI Manager
Page ▾ Safety ▾ Tools ▾
Symantec™ PKI Manager
Symantec.
CRMack@WorldTone.com | Sign Out
Logged in to: WorldTone Cellular
Account activity
Last updated: Aug 30, 2012 7:09 PM
Refresh
All
There is no recent activity for these functions
Alerts
Days to expiration of administrator certificate for WorldTone Cellular
Days to expiration of RA certificate named REGISTRATION AUTHORITY 13262
PKI Client 2.5 includes important feature and security updates, including enhanc… s, your end users will receive these updates automatically. Refer to Managed PKI v8.5 Relea… esources
Certificate history
User seat activity
Certificates
60
40
20
0
Feb '12
Mar '12
Apr '12
May '12
Jun '12
Aug '12
Certificates revoked
Certificates issued
Users and certificates
Manage users
Manage certificates
Manage certificate profiles
Manage authorized user lists
Reporting
View recent reports
Schedule a report
View audit trail
Your account
Manage account and sub-accounts
Manage administrators
Manage CAs
Manage PKI Enterprise Gateways
Get an RA certificate
Account status
Status: OK
Next service renewal: Sep 9, 2014
Optional account setup:
Use directory service
Seat usage
Seat pool
Used
Out of
User
44
500
Device
0
500
Symantec

4. Paste the CSR into the field, submit, and download a new certificate.



Get an RA certificate

If you are setting up PKI Enterprise Gateway or PKI Web Services, you must install an RA certificate to secure communications with Symantec.

If you are not setting up these services, or have already gotten your RA certificate, you do not need to complete this process.

Enter Certificate Signing Request (CSR)

Ask your server administrator to generate a CSR for your RA certificate. Your administrator must generate the CSR according to the instructions in the installation guide for your service.

You can access the resources page by clicking on the icon on the dashboard.

*Paste your CSR:

Important Service Requirements: If you discover or have reason to believe that there has been a compromise of your private key, you must immediately revoke the certificate or notify Symantec™ to do so. Similarly, if the information within your certificate or your organization name has changed, please notify Symantec. Note that Symantec™ retains the right to revoke your certificate at any time without notice if (i) you fail to perform your obligations under the terms of your service agreement; or (ii) in Symantec's sole discretion, you have engaged in activities which Symantec™ determines are harmful to its systems.

* Required information

5. Convert the .p7b format certificate into .pem.

   Command: `openssl pkcs7 -print_certs -in certificate.p7b -out certificate.pem`

6. Create a pkcs12 with the private key and pem.

```
openssl pkcs12 -export -out certificate.pfx -inkey AirWatch.key -in
certificate.pem
```

Configure CA and Certificate Template in Workspace ONE UEM

Now that you have generated a Symantec MPKI RA certificate, Workspace ONE UEM can be configured to communicate with Symantec.

Configure CA

1. Navigate to **Devices > Certificates > Certificate Authorities**.
2. Click **Add**.
3. Select **Symantec** from the **Authority Type** drop-down menu.
4. Enter a unique name and description that identifies the Symantec certificate authority in the **Name** and **Description** fields.
5. Enter `https://pki-ws.symauth.com/pki-ws` in the Server URL field if it is not populated by default. This allows Workspace ONE UEM to have sufficient access to request and issue certificates.:

   The URL is the same for all customers.
6. Select either the **PKI** or **SCEP**radio button to specify the **Certificate Authority Protocol**. If you select SCEP, enter the URL for the **SCEP End Point** in the data entry field that appears. This allows your SCEP server to have sufficient access to request and issue certificates.
7. In the **RA Certificate** field, select the **Upload** button and select the RA certificate (PFX file) that you completed in the step above, Instructions for Generating a New RA Certificate using OpenSSL, in order to communicate with Symantec.
8. Enter the password Symantec provided previously in the **Certificate Password** field.

   The password you need in this step was created when you completed and exported the CSR process.
9. Click **Save**.
10. Click **Test Connection** when complete to verify the test is successful. An error message appears indicating the problem if the connection fails.

Configure Certificate Template

Now that you have completed Configuring CA, Workspace ONE UEM is able to communicate with Symantec. 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 the Symantec **Certificate Authority** you created in Configuring CA from the **Certificate Authority** drop-down menu.
5. Enter the name for the Symantec **Request Template**.

6. Enter a **Description** to help you identify the Symantec certificate template.
7. Select the Symantec profile OID from the **Profile Name** drop-down menu.
8. Select the **Automatic Certificate Renewal** checkbox if Workspace ONE UEM is going to automatically request the certificate to be renewed by Symantec when it expires. If you select this option, enter the number of days prior to expiration before Workspace ONE UEM automatically requests Symantec to reissue the certificate in the **Auto Renewal Period (days)** field. This requires the certificate profile on Symantec to have **Duplicate Certificates** enabled.
9. Select the **Enable Certificate Revocation** checkbox if Workspace ONE UEM should automatically remove the certificate if the device is unenrolled, if the applicable profile is removed, or if the device is deleted from Workspace ONE UEM. When you delete a profile or a device the SCEP certificate is removed from the device but it is not automatically revoked from the CA.
10. For **Key Type**, configuration occurs in the Symantec PKI Manager. This indicates whether the public-private key pair is generated by Workspace ONE UEM or by Symantec. Workspace ONE UEM loads this setting from Symantec based on the selected OID and uses this value to determine the type of certificate request to send. Absolutely no configuration in Workspace ONE UEM is needed by the customer.
11. Enter Lookup Values in each of the **Mandatory Fields** that complement those fields in the Symantec profile. These fields can change depending on which Symantec profile you choose since the information within the Symantec profile may be different.
12. Click **Save**.

Deploy a Certificate Profile to a Device

Now that the Symantec 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 Configuring CA, you chose **PKI** then you only need to configure a **Credentials** profile, but if you chose **SCEP**, you only need to configure a **SCEP** profile. Once either of these profiles is created, you can create additional payloads that the Symantec 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 Symantec CA you created previously in Configuring CA from the **Certificate Authority** drop-down menu.

9. Select the certificate template for Symantec you created previously in Configuring Certificate Template 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.

Configure a SCEP Payload

To configure a SCEP payload, follow all instructions in Configuring a PKI Credential Payload, except for one modification:

1. Select **SCEP** from the payload area on the left rather than configuring **Credentials**.
2. Select **Defined Certificate Authority** from the **Credential Source** drop-down menu.
3. Select the external Symantec CA you created for using SCEP previously in Configuring CA from the **Certificate Authority** drop-down menu.
4. Select the certificate template for Symantec you created for using SCEP previously in Configuring Certificate Template 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.

Chapter 3:
Testing and Troubleshooting, Symantec MPKI

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 MaxRecievedMessageSize and MaxBufferSize to 2147483647.

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 Symantec 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 Symantec 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 Symantec.