

VMware AirWatch On-Premises Certificate Authority Guide

For VMware AirWatch

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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

On-Premises Certificate Authority	3
Insert Parameter in Subject Alternative Name (SAN) Extension	3
Attach Certificate Template	5
Certificate Revocation List versus Online Certificate Status Protocol	7
Configure VMware Identity Manager Certificate Adapter	7

On-Premises Certificate Authority

Digital certificates provide optimal protection for securing your corporate assets. Certificates offer a level of stability, security, and sophistication with which passwords cannot compete. Certificate Management by Workspace ONE UEM ensures security throughout the lifecycle of a device.

As you complete the configuration of Workspace ONE UEM and VMware Identity Manager, you are provided with the option to accept the default digital certificate authority, Workspace ONE UEM CA, which comes built-in to each Workspace ONE UEM installation.

However, you may prefer a third-party CA solution to handle device security. Workspace ONE UEM supports many third-party certificate authorities.

This guide gives you the instructions to configure the CA of your choice to work with VMware Identity Manager, Workspace ONE UEM, and Mobile Single Sign-On. Such instructions include the following.

- Inserting custom parameters in the SAN extension.
- Once the certificate template has been customized to accommodate your third-party CA, where to attach it.
- Explanations of CRL, OCSP, and how to use them with VMware Identity Manager certificate adapters.
- How to configure authentication methods so that VMware Identity Manager recognizes and trusts your third-party certificate authority.

Insert Parameter in Subject Alternative Name (SAN) Extension

Customizing the SAN is required when you need to identify the certificate in a unique way. Such customization means the certificate template needs to be customized too.

Prerequisites

Before customizing the SAN extension, you must have completed integrating your third-party certificate authority into Workspace ONE UEM, which may mean you have already saved a certificate template.

For step-by-step instructions on integrating your CA with Workspace ONE UEM, consult the online help system at <https://my.air-watch.com/help> and view the topic titled Supported Certificate Authorities.

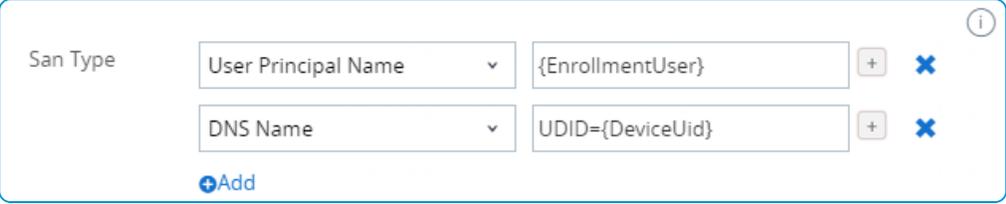
Once you have completed the integration of the third-party certificate authority, take the following steps to add a new parameter in the SAN and the template.

1. Log in to the Workspace ONE UEM console as an Administrator.
2. Navigate to **Devices > Certificates > Certificate Authorities**.
3. Select the **Request Templates** tab.
4. If you have not yet saved a certificate template, select **Add**.

If you have already saved a certificate template as part of the third-party CA integration with Workspace ONE UEM, then find your saved certificate template from the list and select the pencil icon () to the right of its listing. The **SAN Type** setting is the one to which you are adding a new parameter.

5. Complete the settings in the **Certificate Template - Add / Edit** screen.

Setting	Description
Name	Provide a simple one or two word name for the template.
Description	Enter a brief description of the certificate template including any customization you may have applied.
Certificate Authority	Select the CA to which the template applies.
Issuing Template	Enter the CA certificate template name exactly as you created in ADCS. For example, iOSKerberos.
Subject Name	Enter the Subject Name or Distinguished Name (DN) for the template. The text entered in this text box is the Subject of the certificate, which a network administrator can use to determine who or what device received the certificate. A typical entry in this text box is "CN=Workspace ONE UEM.{EnrollmentUser}" or "CN={DeviceUid}" where the {} entries are Workspace ONE UEM lookup values.
Private Key Length	Select the private key length from the drop-down menu. This value is typically 2048 and must match the setting on the certificate template used by DCOM.
Private Key Type	Select the Private Key Type using the applicable check box. This value must match the setting on the certificate template used by DCOM.

Setting	Description
SAN Type	<p>Select +Add to the right of SAN Type to include one or more Subject Alternate Names with the template.</p> <p>This value is used for extra unique certificate identification. Usually, this value needs to match the certificate template on the server.</p> <p>Use the drop-down menu to select the SAN Type and enter the subject alternate name in the corresponding data entry text box. Each text box supports lookup values.</p> <p>To make the template work with VMware Identity Manager and Single Sign-On, you must make at least one addition. Select User Principal Name in the left drop-down list. Its lookup value must be {EnrollmentUser}.</p> <p>If device compliance check is configured with Kerberos authentication, you must also set the SAN type DNS Name. The value must be UDID={DeviceUid}.</p> <p>In summary, the custom SAN Type parameters are the following.</p> <ul style="list-style-type: none"> • User Principal Name, {EnrollmentUser} • DNS Name, UDID={DeviceUid} (Kerberos device compliance) 
Automatic Certificate Renewal	<p>Renew certificates using this template automatically before their expiration date.</p> <p>In order for the auto renewal feature to function correctly, the device profile to which you upload this saved template must have the Assignment Type setting, located in the General tab, set to 'Auto'.</p>
Auto Renewal Period (Days)	<p>This is the number of days prior to expiration that the certificate is eligible for renewal.</p>
Enable Certificate Revocation	<p>Direct the certificates to be automatically revoked when applicable devices are unenrolled or deleted, or if the applicable profile is removed.</p>
Publish Private Key	<p>Publish the private key to the specified Web service endpoint (directory services or custom Web service).</p>

6. Select **Save**.

Attach Certificate Template

With the SAN extensions added to the certificate template, you must now attach your customized template to the device profile that was created during the Getting Started Wizard. Take the following steps to attach the template and adjust

the device profile.

1. Navigate to **Devices > Profiles & Resources > Profiles**.
2. Search for the device profiles that were automatically created by the Getting Started Wizard. Depending upon how many platforms your deployment supports, you may have up to three different device profiles to edit, one for each device platform. These profiles are named in the following manner.
 - Android_Vpn_XXXX (where xxxx is a three or four digit number)
 - IOS_Sso_XXXX (where xxxx is a three or four digit number)
 - Windows_Sso_XXXX (where xxxx is a three or four digit number)
3. Select either the name of the profile or the pencil icon (✎) to the left of the profile name to open the profile edit screen.
4. If the **Add Version** button is enabled, select it to begin editing the profile.
5. Select the **Credentials** tab on the left. This is where you attach your custom certificate template.
6. Select the **Configure** button.
7. Under **Credential Source**, select **Defined Certificate Authority** from the drop-down menu.
8. Under **Certificate Authority**, select the name of the third-party certificate authority you have chosen. This must be the same CA on which your customized certificate template is based.
9. Under **Certificate Template**, select the name of your customized certificate template you saved in the previous step. For more information, refer to [Insert Parameter in Subject Alternative Name \(SAN\) Extension on page 3](#).
10. If the automatically created device profile has a green **SCEP** tab on the left, then select it and select the minus button in the lower-right corner of the profile window.



This action removes the SCEP configuration from the device profile. It was created automatically by the Getting Started Wizard but since you have selected a third-party certificate authority, you do not need a SCEP solution.

11. Select **Save & Publish**.
12. Repeat steps 2 through 11 for each platform your deployment supports.

Certificate Revocation List versus Online Certificate Status Protocol

CRL

A certificate revocation list (CRL) is used to validate digital certificates before they are used to access sensitive online data. A CRL is issued by the certificate authority and is generated and published on a set schedule. CRLs are only valid within a specified time frame, usually 24 hours or less. During this validity period, the CRL is consulted to validate a certificate before it is used.

Therefore, in order for a Public Key Infrastructure to perform effectively, one must have access to accurate and up-to-date certificate revocation lists.

Certificates on Hold

A certificate with a 'held' status, while technically considered revoked, is reversible and is generally used to indicate a temporary invalidity of a certificate.

Expired Certificates

Affixing a certificate with an expiration date is not an adequate substitute for a CRL. While it is true that all expired certificates are invalid, not all unexpired certificates are trustworthy. Mistakes and human error in certificate vetting are natural occurrences in real world operations.

OCSP

Online Certificate Status Protocol is an alternative to using CRLs. OCSP uses less network bandwidth, which enables near real-time status checks. Such rapid status checks are advantageous in high volume mobile device operations like Workspace ONE UEM.

There is also less data to parse when responding to an OCSP request, which means client-side libraries designed to handle these requests are less complex.

Configure VMware Identity Manager Certificate Adapter

The final step to making Workspace ONE and mobile SSO functional in your deployment involves configuring authentication methods in the VMware Identity Manager Console. Configuring these authentication methods allows VMware Identity Manager to recognize and trust your third party certificate.

Take the following steps.

1. Open the VMware Identity Manager Console and navigate to the **Manage** screen for **Authentication Methods**.
2. You are presented with a list of all existing authentication methods for built-in identity providers. Depending upon how many platforms your deployment supports, you may have up to three different methods to configure, one for each device platform. These methods are named in the following manner.
 - "Mobile SSO (for iOS)"
 - "Mobile SSO (for Android)"
 - "Certificate (Cloud Deployment)" This method is for Windows
3. Select the configure icon for each applicable platform listed above. A new AuthAdapter screen appears.

4. Ensure the **Enable Certificate Adapter** check box is selected, which appears at the top of each AuthAdapter screen. For iOS, this field is labeled **Enable KDC Authentication**.
5. Next to the **Root and Intermediate CA Certificates** setting, select the **Select File** button. Then select the PEM certificate file you received from the third party CA.
6. Optionally, you can enable OCSP and CRL, where applicable, to enable active certificate validation. For more information, see [Certificate Revocation List versus Online Certificate Status Protocol on page 7](#).
7. Select **Save**.
8. Repeat steps 2 through 7 for each platform your deployment supports.