

VMware AirWatch Integration with GlobalSign 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

Chapter 1: Workspace ONE UEM Integration with GlobalSign Guide	3
System Requirements	3
High Level Design	3
Chapter 2: Install, Set Up, Configure Certificate	5
Step 1 Configure GlobalSign Certificate Authority	5
Step 2 Set Up Certificate Template for GlobalSign CA Type	5
Step 3 Deploy a Certificate Profile to a Device	6
Chapter 3: Testing Troubleshooting, Globalsign	8
Chapter 4: Verify Ability to Perform Certificate Authentication without Workspace ONE UEM	8
Chapter 5: Verify Ability to Perform Certificate Authentication with Workspace ONE UEM	8

Chapter 1:

Workspace ONE UEM Integration with GlobalSign 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 GlobalSign PKI services to issue certificates for your Workspace ONE UEM MDM solution.

System Requirements

- A GlobalSign instance that is configured for certificate deployment.
- Workspace ONE UEM console version 8.0 or higher.
- A service account with authentication permissions.

High Level Design

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



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 Configure GlobalSign Certificate Authority

After you obtain a service account with authentication permissions from GlobalSign, Workspace ONE UEM can be configured to communicate with GlobalSign.

1. Navigate to **Devices > Certificates > Certificate Authorities**.
2. Click **Add**.
3. Select **GlobalSign** from the **Authority Type** drop-down menu.
4. Enter a unique name and description that identifies the GlobalSign certificate authority in the **Certificate Authority** and **Description** fields.
5. In the **Server URL** field enter the URL of your GlobalSign instance.
This is the web endpoint that Workspace ONE UEM will use to submit requests and issue certificates.
6. Enter the **Username** and **Password** fields belonging to the service account with authentication permissions mentioned in System Requirements above.
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.
9. Click **Save**.

Step 2 Set Up Certificate Template for GlobalSign CA Type

Now that you have configured GlobalSign certificate authority, Workspace ONE UEM is able to communicate with GlobalSign. 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. Select **GlobalSign** from the **Certificate Authority** drop-down menu.
5. Enter the **Name** for the GlobalSign Request Template.
6. Enter a **Description** to help you identify the GlobalSign certificate template.
7. Enter the **Profile ID**, which corresponds to the GlobalSign 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 may be comprised of a maximum of one CN and up to three OUs.
11. Under **SAN Type**, select **Add** to include one or more Subject Alternate Names with the template. This is used for additional unique certificate identification. In most cases, this needs to match the certificate template on the server. Use the drop-down menu to select the SAN Type and enter the subject alternate name in the corresponding data entry field. Each field supports lookup values. **Email Address**, **User Principal Name**, and **DNS Name** are supported by GlobalSign templates by default, and Workspace ONE UEM recommends that you use them.
12. Select the **Automatic Certificate Renewal** checkbox if Workspace ONE UEM is going to automatically request the certificate to be renewed by GlobalSign when it expires. If you select this option, enter the number of days prior to expiration before Workspace ONE UEM automatically requests GlobalSign to reissue the certificate in the **Auto Renewal Period (days)** field. This requires the certificate profile on GlobalSign 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**.

Step 3 Deploy a Certificate Profile to a Device

Now that the GlobalSign 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 GlobalSign 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 GlobalSign CA you created previously in [Step 1 Configure GlobalSign Certificate Authority on page 5](#) from the **Certificate Authority** drop-down menu.
9. Select the certificate template for GlobalSign you created previously in [Step 2 Set Up Certificate Template for GlobalSign CA Type on page 5](#) 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, Globalsign

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,
- Retrieve a certificate from the Workspace ONE UEM console from the GlobalSign certificate authority.

The troubleshooting technique that usually resolves this problem is to...

- Add 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 the 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 GlobalSign certificate profile match the look up values in the Workspace ONE UEM console 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 GlobalSign.