

Windows 10 Certificate Single Sign On using an AirWatch Certificate Authority

In this lab you will be deploying a certificate to an enrolled Windows 10 virtual machine. This certificate will be generated by the built-in CA in Workspace ONE UEM.

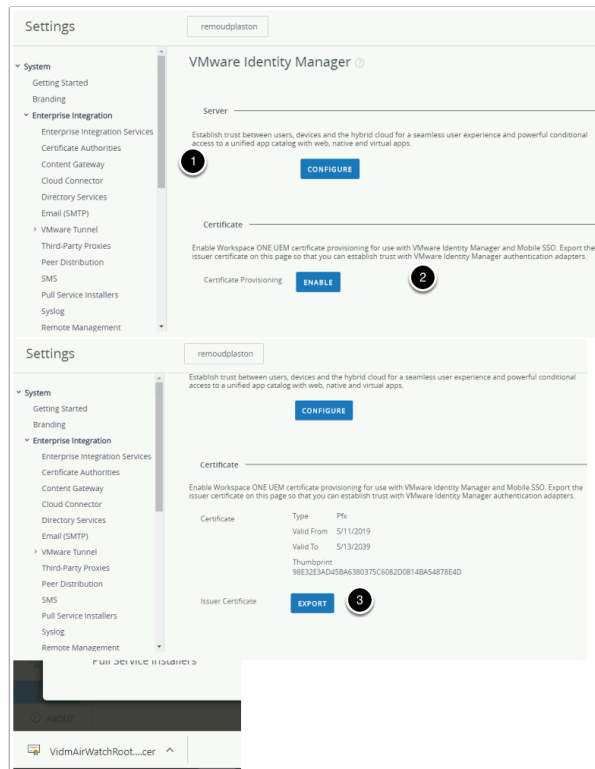
We will later configure Workspace ONE Access to trust certificates issues by UEM and configure the Certificate (Cloud Deployment) authentication adapter.

Finally we will test everything on a Windows 10 Machine to ensure we are able to have a seamless authentication experience.

Part 1: WorkspaceOne UEM - Certificate Profile

1

- Open Chrome on your **ControlCenter2** jumpbox and navigate to <https://cn-livefire.awmdm.com> Authenticate using your **e-mail address** and unique **password**
 1. Navigate to **Groups & Settings > All Settings > Enterprise Integration > VMware Identity Manager > Configuration**
 2. Under Certificate select **ENABLE** (this should be enabled from a previous lab)
 3. Under **Certificate** next to **Issuer Certificate** select **EXPORT**



2. WorkspaceOne UEM - Certificate Profile continued...

1. Then navigate to **Devices** > **Profiles & Resources** > **Profiles** > **ADD** > **Add Profile** > **Windows** > **Windows Desktop** > **User Profile** Give it a name : **W10 - SCEP - SSO** .
2. Select your **Smart Group** with the **World icon** for the Smart Group
3. Select the **SCEP** payload on the left hand navigation panel.
4. Select **CONFIGURE**
5. Set the following
 - Credential Source: **AirWatch Certificate Authority**
 - Certificate Template: **Certificate (Cloud Deployment)**
 - Issuer: **LiveFire**
 - Click **SAVE AND PUBLISH**
6. In the **Device Assignment** notice your device in the list of device being added. Then click **PUBLISH**

Workspace ONE UEM / LiveFire Global / Simeon - P... Add

GETTING STARTED
MONITOR
DEVICES
ACCOUNTS

Dashboard
List View
Details View
Lifecycle
Profiles & Resources
Profiles
Resources
Batch Status
Profiles Settings

Profiles

Filters » ADD LAYOUT

Profile Details	Managed By	Assignment Type	Assignment
android_udid_cert Android Credentials	Simeon - PROD - Don't Delete	Auto	S
iOS - Mobile SSO Apple iOS Credentials, SCEP, S...	Simeon - PROD - Don't Delete	Auto	S

Add Profile

Select a platform to start:

Android iOS macOS tvOS Tizen
Windows Rugged Windows Android (Legacy) Chrome OS (Legacy)

Select Device Type

Windows Phone Windows Desktop Windows 7

Select Context

User Profile Device Profile

General

Name *	W10 - SCEP - SSO
Version	1
Description	
Deployment	Managed
Assignment Type	Auto
Allow Removal	Always
Managed By	mintobrunella@outlook.com
Smart Groups	<div>🌐 mintobrunella@outlook.com (mintobrunella@outlook.com) ✕</div> <div>Start typing to add a group 🔍</div>
Exclusions	<div>NO YES</div>

Add a New Windows Desktop Profile

General

VPN

Credentials

Windows Hello

Single App Mode

Web Clips

Exchange ActiveSync

SCEP

Exchange Web Services

Custom Settings

SCEP


Credential Source	AirWatch Certificate Authority
Certificate Authority *	AirWatch Certificate Authority
Certificate Template *	Certificate (Cloud Deployment)
Issuer *	LiveFire

SAVE AND PUBLISH

CANCEL

View Device Assignment

As

Assignment Status	Friendly Name	User	Platform
 Unchanged	user35CRSJ Desktop Wind...	user35CRSJ	Windows

Items 1-1 of 1

Part 2: Configuring Workspace ONE Access Certificate (Cloud Deployment) Authentication

1. Configuring Workspace ONE Access Certificate (Cloud Deployment) Authentication

- In this next section, we will configure Workspace ONE Access Certificate Auth Adaptor to trust the certificates being presented by the devices.
 - On your **ControlCenter** server, use your **unique Workspace ONE Access** server and authenticate to the local directory using administrator account and password.
 - Under **Identity & Access Management > Manage** select **Authentication Methods**
 - Click on the **Pencil** to Configure the **Certificate (Cloud Deployment)** authentication method.
 - Select the **checkbox Enable Certificate Adapter** and click **Select File** to **upload the Certificate (VidmAirWatchRootCertificate.cer)** you downloaded above in the UEM console.
 - On the **Update Auth Adapter** window select **OK**
 - Leave everything else in here as default and click **Save**.
 - Now navigate **Identity Providers** under **Identity & Access Management** click on **Built-in**
 - Navigate to the **Authentication Methods** area and select the **check box** next to **Certificate (Cloud Deployment)** and select **Save** at the bottom of the page.

Workspace ONE™ Access

Dashboard

Users & Groups

Catalog

Identity & Access Management

Roles

Directories

Identity Providers

Password Recovery Assistant

Authentication Methods

Authentication Methods for Built-in Identity Provider

Important: When you disable an authentication method, the authentication policy rules to select another authentication method.

Authentication Methods	Configure
Airwatch External Access Token	
Password (AirWatch Connector)	
Device Compliance (with AirWatch)	
VMware Verify	
Mobile SSO (for iOS)	
Password (Local Directory)	
Mobile SSO (for Android)	
Certificate (Cloud Deployment)	

Certificate (Cloud Deployment)

Enable Certificate Adapter

Root and intermediate CA certificates*

Select File

Uploaded CA Certificates

CN=mintobrunellaoutlookcom
(4BEBE1DAAE597AC58B32F597EE3C6C0E0A6F09840A649A030E7A33CFB4E61968) ✖

User Identifier Search Order

upn | subject

Validate UPN Format

Request Timeout

0

Certificate Policies Accepted

✖

Cancel

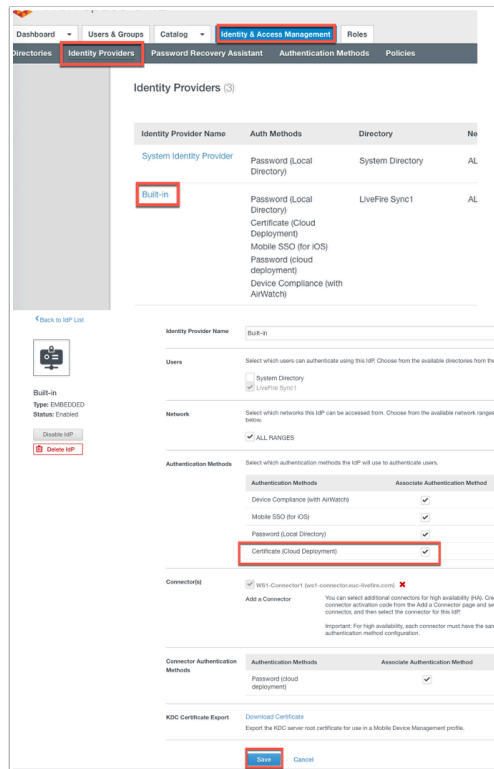
Save

Update Auth Adapter

Please click OK to confirm and upload file.

Cancel

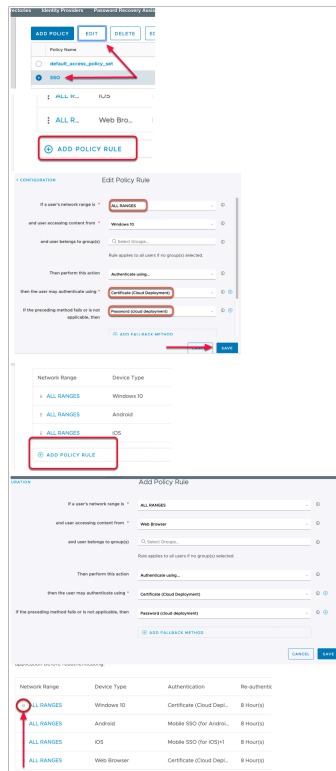
OK



2.

• Configuring Workspace ONE Access Certificate (Cloud Deployment) Authentication....continued

1. Navigate to **Policies** under **Identity & Access Management** then click on the **SSO** policy.
2. Select **Edit**
3. Next to **Configuration** select **+ADD POLICY RULE.**
4. In the **Add Policy Rule** window add the following, next to : -
 - 'and user accessing content from' to Select **Windows 10** from the drop down
 - then the user may authenticate using* change to **Certificate (Cloud Deployment)**
 - "if the preceding method fails or is not applicable, then" change **Select fallback method...** to **Password (Cloud Deployment)**
5. Select **SAVE**
6. Select **+ADD POLICY RULE.**
7. In the **Add Policy Rule** window add the following, next to : -
 - 'and user accessing content from' select **Web Browser** from the drop down
 - then the user may authenticate using* change to **Certificate (Cloud Deployment)**
 - "if the preceding method fails or is not applicable, then" change **Select fallback method...** to **Password (Cloud Deployment)**
8. Select **SAVE,**
9. Next to **ALL RANGES for Windows 10** on the left select the **6 DOTS** and drag to the top
10. Select **NEXT,** select **SAVE.**



Part 3: Windows 10 Single Sign On using Certificates

- Now that the administrative elements are in place we will now test the authentication flow from our Windows 10 VM.
 - On the **ControlCenter2** VM on the desktop you will find the **Remote Desktop** folder. In this folder click double click on **w10client01.RDP**
 - Inside the Windows 10 Virtual Machine **open Microsoft Edge** from the desktop and type **OFFICE.COM** in the address bar
 - In the **Office.com** page select **Sign In**
 - In the **Sign in** window, type your **email address**. eg user35crsj@sanjose35.euc-livfire.com.
 - Select **Next**
 - Notice now that you are being re-directed to **cas.vidmpreview.com** in the URL field and you are prompted for a **Certificate**.
 - Click **OK** on the pop-up for your certificate and notice your are straight into your WorkspaceOne bookmarks Tab.
 - Now click on any one of your **Office365 deeplinks** and notice your are authenticated without further credentials. If you get prompted to "Stay Signed in?" simply click **No**.
 - You are now authenticated to your O365 environment using a certificate based authentication method.

This completes this lab.

