

Windows 10 Compliance Workspace One UEM + Workspace ONE Access

Part 1: Workspace One UEM Compliance Rules

WorkspaceOne allows administrators to check the device posture in addition to the credentials provided for authentication. This ensure's that not only the provided credentials are valid, but also the device being used to access corporate resources is deemed secure and compliant. WorkspaceOne UEM has a robust compliance engine that allows administrator to set a standard for security on devices.

First you will be configuring a standard for compliance on Windows 10 using WorkspaceOne UEM

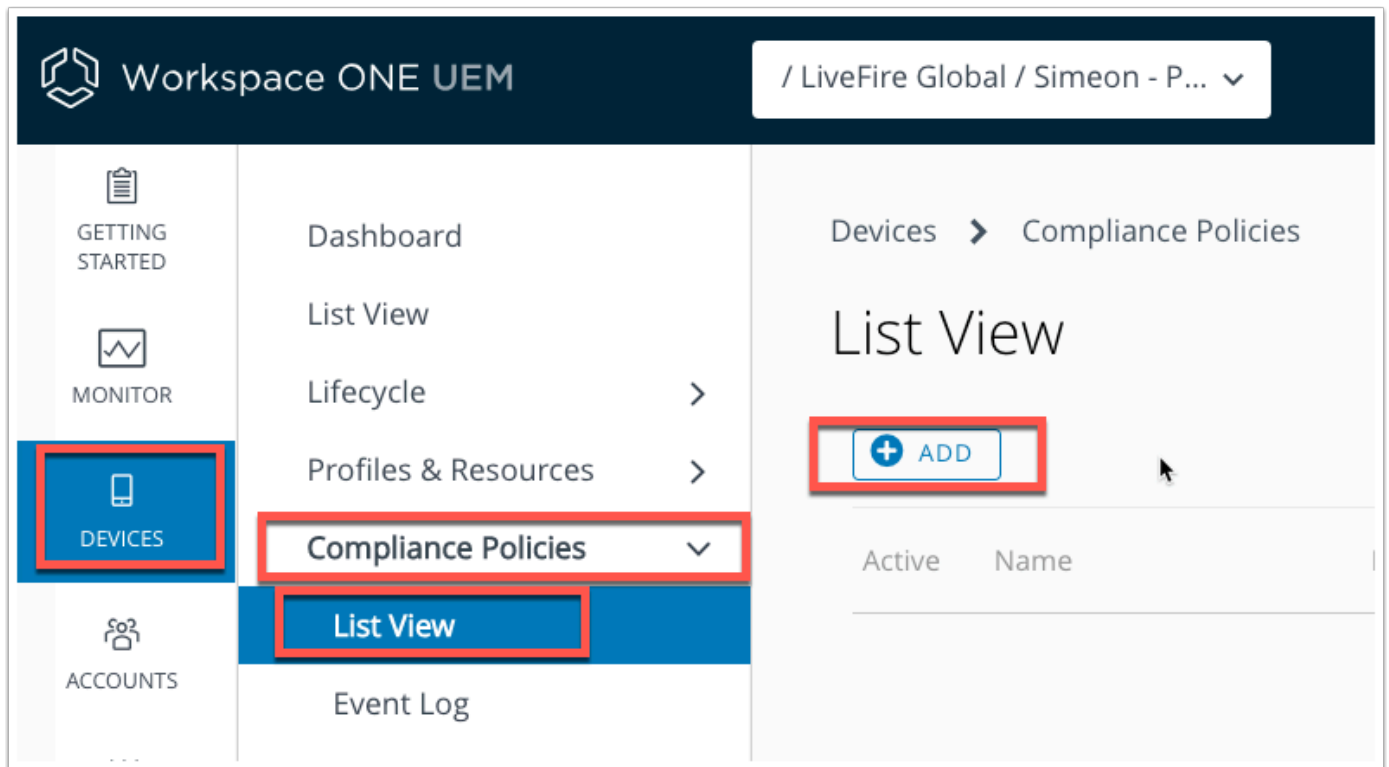
Second, you will be configuring Workspace ONE Access Access Policies to check the device compliance during the authentication process.

Third, you will bring this to life by authenticating to O365 using Workspace ONE Access certificate adapter in conjunction with device compliance.

1. Let's begin with configuring our UEM compliance rules for Windows 10.

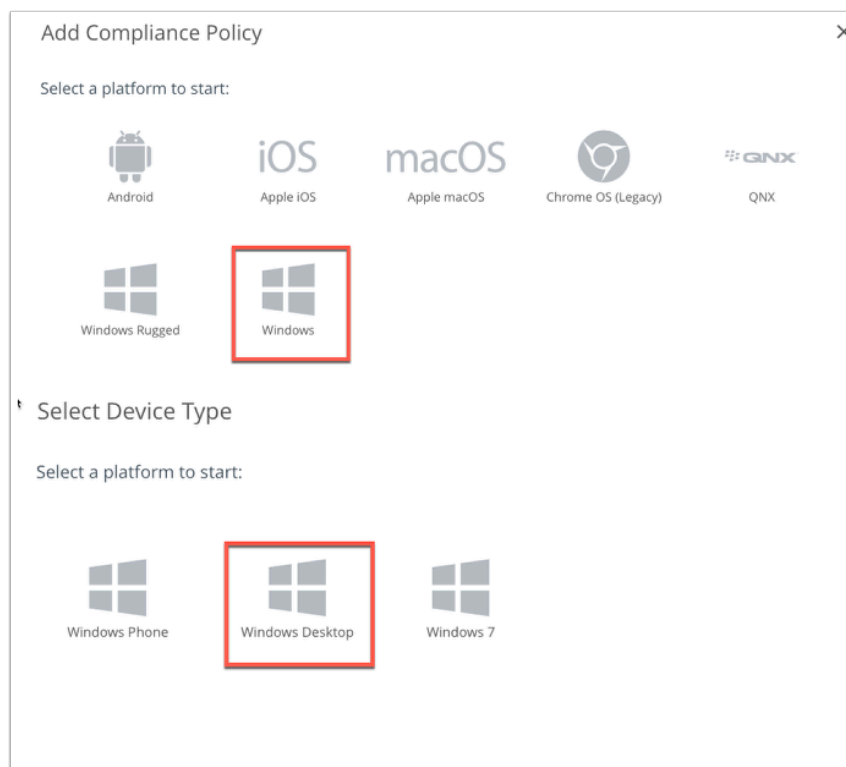
(**Note:** that the same procedure can be used for Android and iOS, but in our scenario we will be dealing with Windows 10)

- Open the Workspace One UEM console on **cn-livewire.awmdm.com** and authenticate using your unique credentials. Navigate to **Devices > Compliance Policies > List View** and click **+ ADD**



2. Select **Windows** from the "Select a platform to start:" window and select **Windows Desktop** from the next page as this one relates to Windows10 specifically.

- Select **NEXT** at the bottom of the page. We have now set our rule we will now select an action.



3. In the **Actions** tab validate the check box next to **"Mark as Not Compliant"** is selected.
- This will ensure that if our device does not follow the rules set in the previous page it will be flagged as not compliant. Now notice the drop down for the actions you can take. You could go as harsh as performing an enterprise wipe, or as subtle as notifying the user via a push notification.
 - In the left dropdown leave **Notify** as the default and change **Send Email to User** to **"Send Push Notification to Device"** from the the action dropdown.
 - Select **+ Add Escalation** and leave as default. Notice you the user will be e-mailed after 1 day of the rule still being broken. Click **NEXT** at the bottom of the page

Add Compliance Policy

1 Rules 2 **Actions** 3 Assignment 4 Summary

Immediately perform the following actions ☒ Mark as Not Compliant

Notify Send Push Notification to Devi ☒ Default Template

After 1 Days Perform the following actions: ☐ Repeat ☒ Mark as Not Compliant

Notify Send Email to User CC: ☒ Default Template

+ Add Escalation

4. In the **Add Compliance Policy** page notice all the rules your can set in the left hand drop down. These are all the parameters an admin can set to determine whether a device is compliant with the organizations security rules. For this particular lab we will be dealing with the **Firewall Status**. Configure the following:-

- On the left under **Match** select the **dropdown** and change **MDM Terms of Use Acceptance** to **Firewall Status**
- In the 2nd drop down, this should automatically change to **Is**
- in the 3rd dropdown change **Good** to **"Poor"**.

Edit Device Policy

1 Rules 2 Actions 3 Assignment 4 Summary

Match **All** Of The Following Rules

Firewall Status **Is** **Poor**

+ Add Rule

5. Under the **Assignment** tab next **Smart Groups** select your unique **Organization Group** marked with the **world** symbol.

Click **NEXT**

Add Compliance Policy

1 Rules 2 Actions 3 Assignment 4 Summary

Managed By **Simeon - PROD - Don't Delete**

Smart Groups **Simeon - PROD - Don't Delete (Simeon - PROD - Don't Delete)**

Start typing to add a group

Exclusions **NO** YES

VIEW DEVICE ASSIGNMENT

6. Under the **Summary** Tab change the default Name **Firewall Status** to - **Windows 10 - Firewall** and click **FINISH & ACTIVATE** at the bottom of the page.

① Rules ② Actions ③ Assignment ④ **Summary**

General

Name * Windows 10 - Firewall

Description * Firewall Status

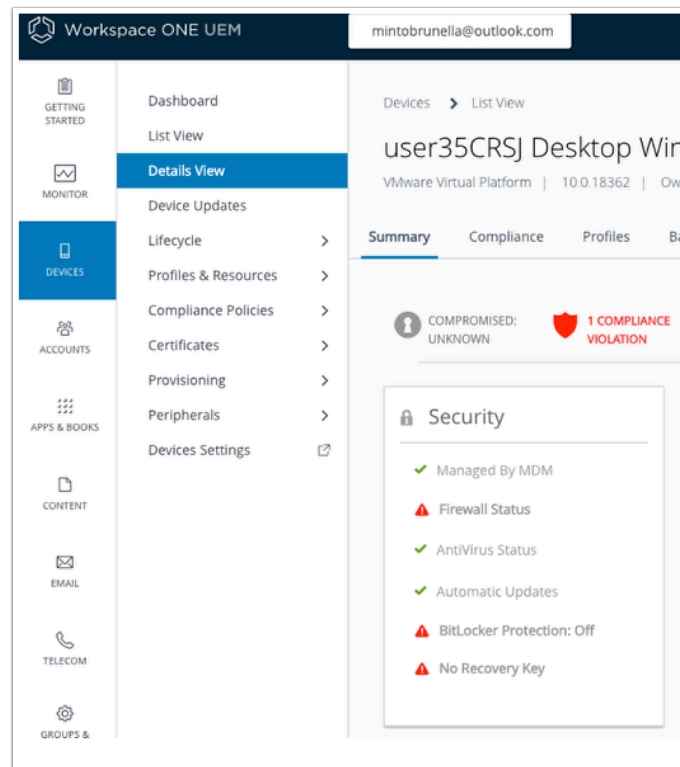
Device Summary

Assigned	1
Compliant	1
Non-Compliant	0

PREVIOUS FINISH **FINISH & ACTIVATE** CANCEL

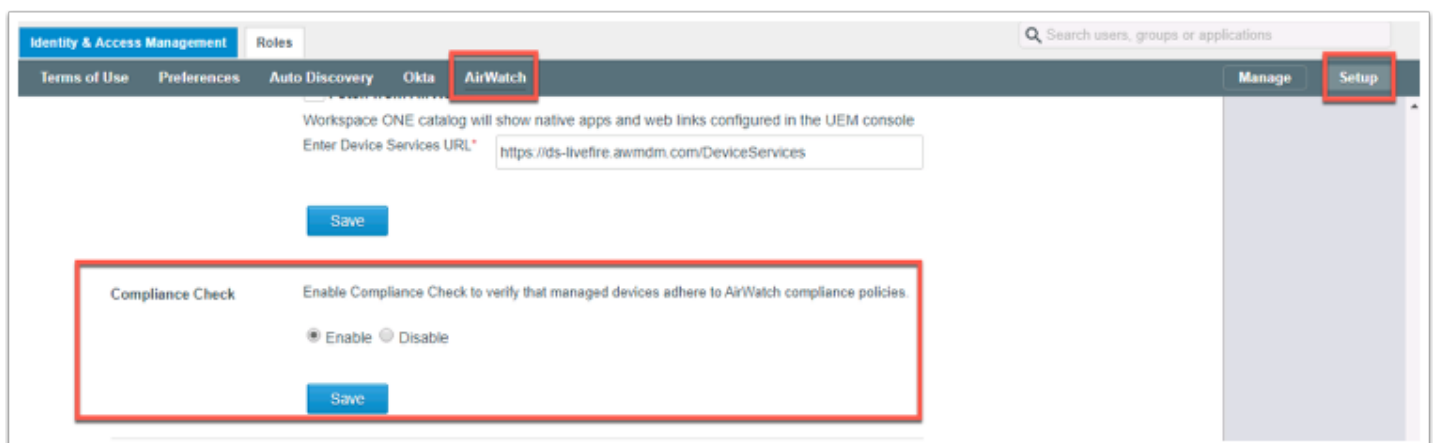
7. On your **Controlcenter** desktop, open the **Remote Desktop** folder.

- Select and RDP to the **W10Client01** with username **Administrator** and password **VMware1!**
 1. On the windows 10 desktop select **Start** > **Run**
 2. In the **Run** window type **WF.msc**
 3. In the **Windows Defender for Firewall for Advanced Security** select the **Domain**, **Private** and **Public Profile** and change the **Firewall state** from **ON (recommended)** to **OFF**, Select **OK** to close the **Windows Defender Firewall** window

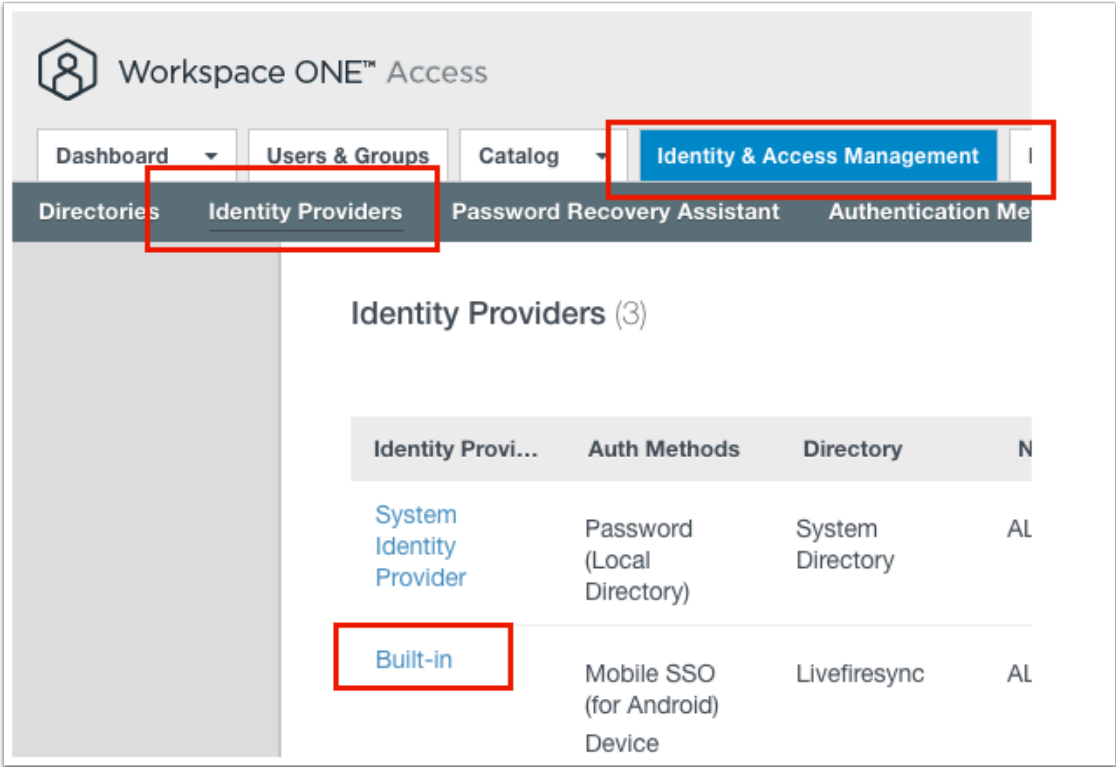


Part 2: Workspace ONE Access Access Policy Device Compliance


1.
 - Let's enable Device Compliance from AirWatch then enable Authentication Method in the **Built-In** Identity Providers .
 1. Navigate to your unique **Workspace ONE Access** tenant and authenticate as **System Admin**
 2. Navigate to **Identity & Access Management** Tab > **Setup** > **AirWatch**
 3. Scroll down to Compliance Check, select the **Enable** radio button and select **Save**



2. Open **Identity & Access Management** tab and select **Identity Providers**. On the page **Identity Providers** window select **Built-in**



3. Scroll down to **Authentication Methods** and enable the **Device Compliance (with AirWatch)** checkbox and scroll down and select **Save** at the bottom of the page.



Built-in

Type: EMBEDDED

Status: Enabled

Disable IdP

Delete IdP

Identity Provider Name

Built-in

Users

Select which users can authenticate using this IdP. Choose from the available directories from the list below.

System Directory

LiveFire Sync1

Network

Select which networks this IdP can be accessed from. Choose from the available network ranges from the list below.

ALL RANGES

Authentication Methods

Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	Associate Authentication Method
Device Compliance (with AirWatch)	<input checked="" type="checkbox"/>
Mobile SSO (for iOS)	<input checked="" type="checkbox"/>
Password (Local Directory)	<input checked="" type="checkbox"/>
Certificate (Cloud Deployment)	<input checked="" type="checkbox"/>

KDC Certificate Export

Download Certificate

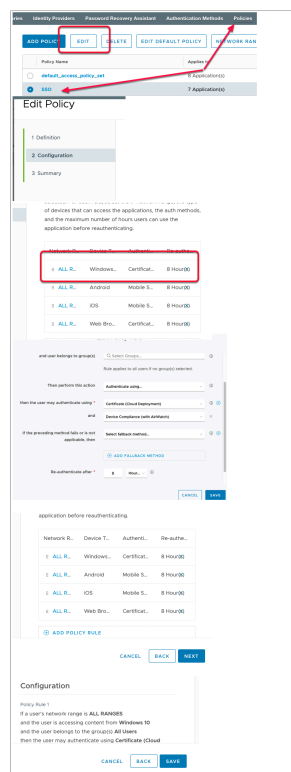
Export the KDC server root certi

Save

Cancel

4.

- Now Navigate and select **Policies** in the **Identity & Access Management** tab
 1. Next to the **SSO** policy select the **radio button** and select **EDIT**
 2. In the **Edit Policy** window select **Configuration**
 3. Select **ALL RANGES** next to the policy that applies to **"Windows 10"**
 4. In this policy you will see that **Certificate (Cloud Deployment)** is the primary authentication method that is being used. We will now add device compliance, as an additional Access requirement, to allow user access. Select the **+** next to **Certificate (Cloud Deployment)**
 5. Next to **If the preceding method fails or is not applicable, then** CHANGE **Password (cloud deployment)** to **Select fallback method....**
 6. You will now have an **"and"** clause. In the dropdown select **Device Compliance (AirWatch)**.
 7. Select **SAVE** at the bottom of the page.
 8. Select **NEXT** on the following page and **SAVE** again on the **Summary** of the **Edit Policy** page.

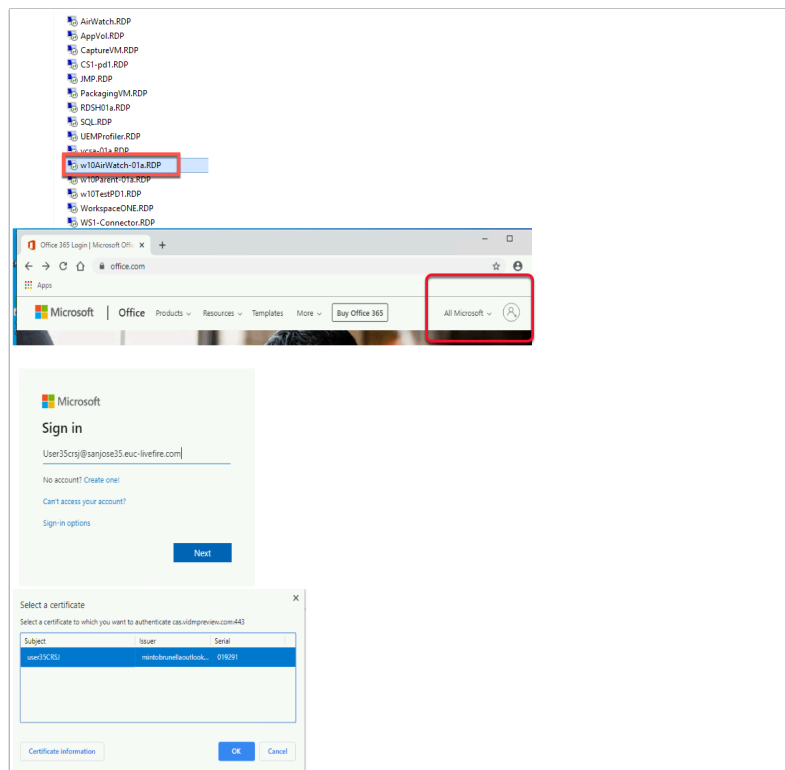


Part 3: Windows 10 Compliance in Action

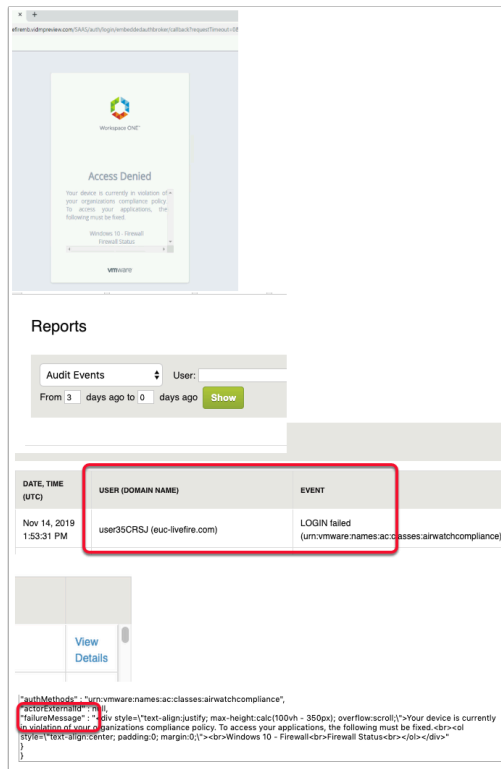
1. Windows 10 Compliance in Action

- We will now test for Compliance as an authentication method.
 1. Navigate to the Desktop of the **ControlCenter2** and open the **Remote Desktop** folder and launch an RDP session using the **W10client01.RDP** client.
 2. Open **Chrome** within the **W10** machine that was enrolled. Now type in **Office.com**. Select the **sign-in to your account ICON** on the right-hand side of the page.

3. On the **Sign In** window type your **custom user** eg user35crsj@sanjose35.euc-liveware.com, select **Next**
 - You will get a **pop up** from Chrome that will request you to select the appropriate certificate to use for authentication.
 4. On the **Select a certificate** window select **OK**
- At this point Workspace ONE Access will check the validity of the certificate, but also send an API compliance query to Workspace ONE UEM to ensure the device is compliant (This is using the **UDID** that is present to vIDM in the certificate)

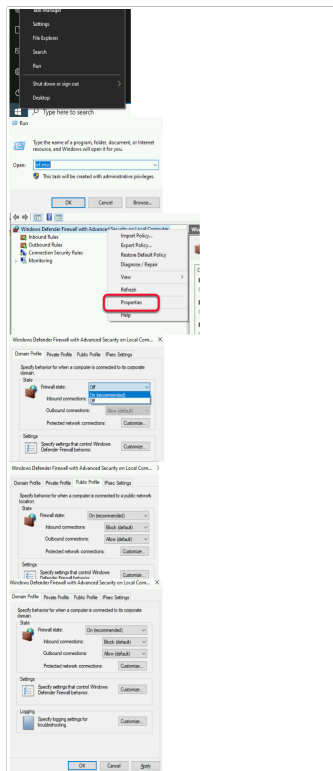


2.
 - You will notice an **Access Denied** message. We can also see this in the Event audits in Workspace ONE Access.
 1. In your Workspace ONE Access tenant. Navigate to **Dashboard** > **Reports** > **Audit Events** and select **Show**
 2. Look for an event that is **LOGIN failed** with your custom user,
 3. To the right select **View Details**. Scroll down until you find the area "**failuremessage**" and read what it says.



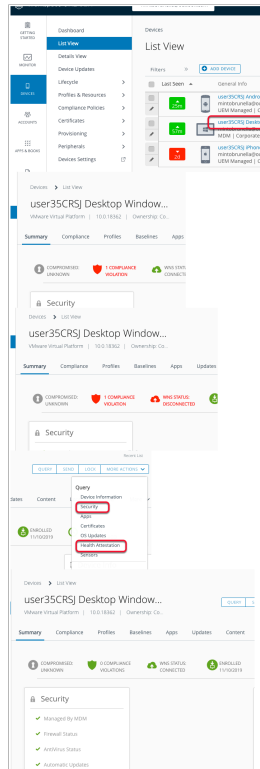
3. Windows 10 Compliance in Action continued...

- Use your RDP connection and go back and enable the Windows Firewall on the Windows 10 machine.
 1. Select **Start** > **RUN** and type **wf.msc**
 2. Right click **Windows Defender Firewall with Advanced Security on Local Computer** and select **Properties**
 3. Re-enable the **Domain**, **Private** and **Public Profiles** by selecting the **dropdown** next **Firewall state** and change **Off** to **On (recommended)**
 4. Select **OK** to close the **Windows Defender Firewall with Advanced Settings on Local Computer**



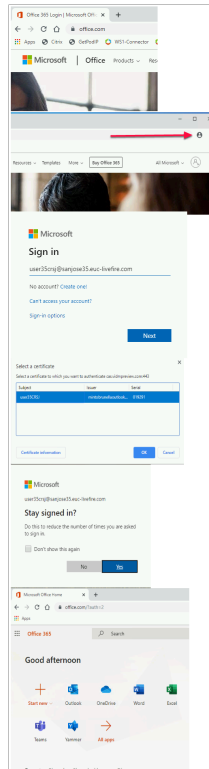
4.

- Navigate back to your Workspace ONE UEM Console
 1. Select **Devices** > **List View** > and select your **Windows 10 device**
 2. It take about 5 minutes for your Status to change in Workspace ONE UEM. **Keep refreshing** your screen
 1. If **WNS status: Disconnected** shows then try rebooting your Windows 10 machine.
 2. If this does not work Select **Query** > **Security** and **Query** > **Health Attestation**
 3. You should now see the device listed as **compliant** and the **Firewall status** as **green** in the WorkspaceOne UEM console.



5

- Revert back to your Windows 10 virtual machine
 1. Open a browser and type **Office.com**
 2. On the right of the page select the **Sign into your accounts** **ICON**
 3. On the **Sign in** type your **custom user email address** eg. user35crsj@sanjose35.euc-livewire.com select **Next**
 4. On the **Select a certificate** window select **OK**
 5. On the **Stay signed In?** window select **NO**
 6. Notice the Single Sign-On using the **Certificate + the Compliance Check** against UEM worked successfully and you now have access to the application



6.

- If you go to Workspace ONE Access , select the **Dashboard > Reports > Audit Events**
 1. Select **Show** ,
 - notice the **EVENT** is **LAUNCH** and your **User** , the **OBJECT** is **Office365 with Provisioning**,
 2. Select **View Details**
 3. Notice Audit Events are reporting a successful login using Certificate (Cloud Deployment) and Device Compliance (with AirWatch).

•

This completes the **Windows 10 Compliance** with **Workspace ONE Access** and **Workspace ONE UEM Lab**. This is a single example of the many options for compliance that could be used not restricted to Windows 10, but also other platforms

Reports

Audit Events ↓ User:
From 1 days ago to 0 days ago [Show](#)

Audit Events

DATE, TIME (UTC)	USER (DOMAIN NAME)	EVENT	OBJECT
Nov 14, 2019 5:25:34 PM	user35CRSJ (euc-livfire.com)	LAUNCH (WSFed12)	Office365 with Provisioning

[Export as CSV](#)

OBJECT

Office365 with Provisioning

[View Details](#)[View Details](#)

View audit events detail

```
{
  "tenantId": "AW-LIVEFIREMB",
  "actorId": 7220359,
  "actorUserName": "user35CRSJ",
  "actorDomain": "euc-livfire.com",
  "actorUuid": "2a519433-e11d-4ede-83c7-9c1db1f26fdd",
  "clientId": null,
  "deviceId": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36",
  "workspaceId": "E26A81027A400146AA784F08C75A3759",
  "sourceIp": "207.189.188.115",
  "objectType": "LAUNCH",
  "objectId": "b30ec050-10a5-43fd-9f20-1352a72c803a",
  "objectName": "Office365 with Provisioning",
  "values": {
    "deviceType": "browser",
    "success": "true",
    "actorExternalId": "6c7e6c71-a579-43da-b8f3-4cd0e5a5e2d0",
    "resourceType": "WSFed12"
  }
}
```