

Securing Applications with Per APP VPN Tunnelling

Introduction

Workspace ONE Tunnel enables secure access for mobile workers and devices. Users have a simple experience and need not enable or interact with Tunnel, and IT organization's may take a least-privilege approach to enterprise access, ensuring only defines apps and domains have access to the network.

Tunnel provides industry-best security and builds on TLS 1.2+ libraries, implements SSL Pinning to ensure no MITM attacks, and client certificate whitelisting, to ensure identity integrity. Combined with explicit definitions of managed applications and integration with Workspace ONE compliance engine, Tunnel can help customers attain Zero Trust goals for their workforce.

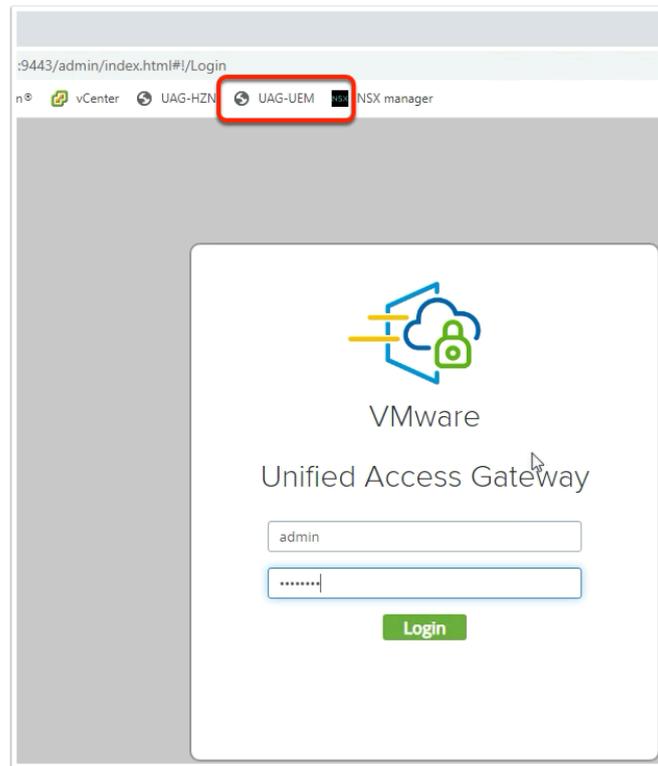
Prerequisites

Before you can perform the steps in this tutorial, you must install and configure the following components:

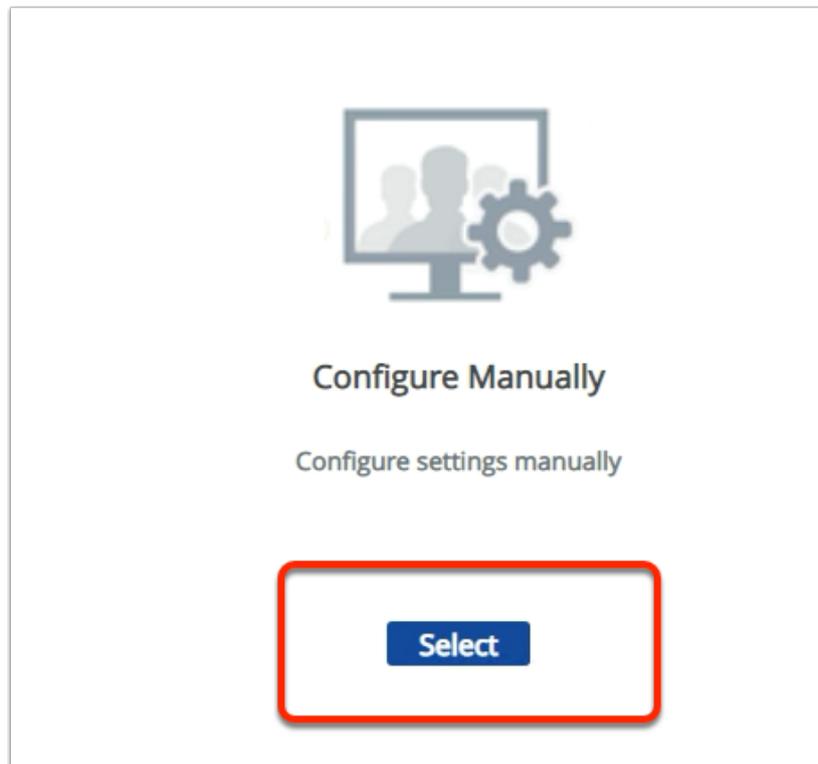
- VMware Unified Access Gateway with VMware Tunnel edge service configured
 - UAG has been deployed. We will configure the Edge service
 - Your UAG is on representative on-premises infrastructure and is UAG-UEM.euc-liveware.com.
 - It is on an NSX-T managed 172.16.20.x subnet. This subnet is representative of DMZ infrastructure
- Workspace ONE UEM 1909 and later
 - You have a Workspace ONE UEM Tenant.
- A device for the platform you plan to use (Windows 10, macOS, Android, or iOS)
 - You will be using the W10Ext01a virtual machine for testing purposes (This was enrolled to Workspace ONE UEM on Day1)
 - This virtual machine is on a VPN segment (172.16.30.x) which is NSX-T managed and we will refer to it as External

Note! Due to constraints in VMware Firewall rules we are not able configure a client outside the training environment and W10EXT01a will represent this.

Part 1- Configuring VMware Tunnel Settings in the Unified Access Gateway UI

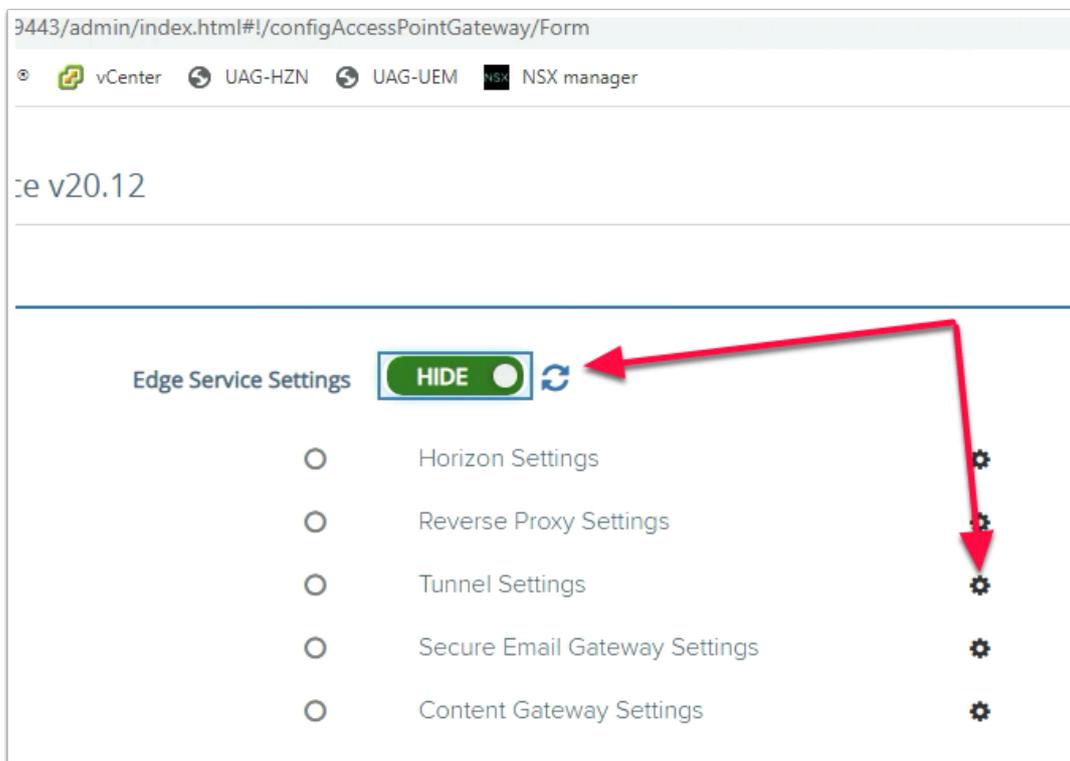


1. On your **ControlCenter** server, open your **Chrome Browser** and select the **UAG-UEM** shortcut.
 - In the **UAG Admin Console** Login
 - Enter **admin** for **username**
 - Enter **VMware1!** for **password**
 - Select **Login**



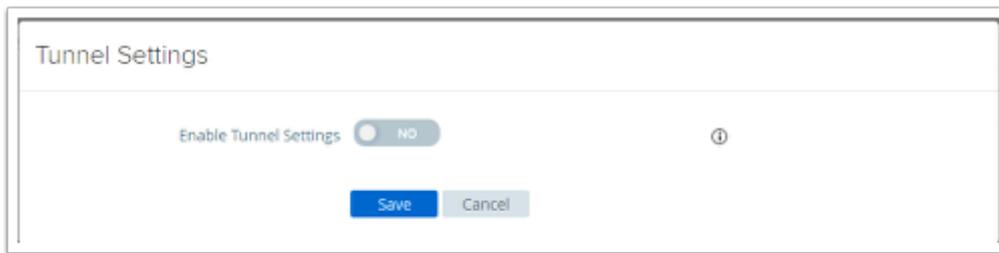
2. Under **Configure Manually**

- Click the **Select** button

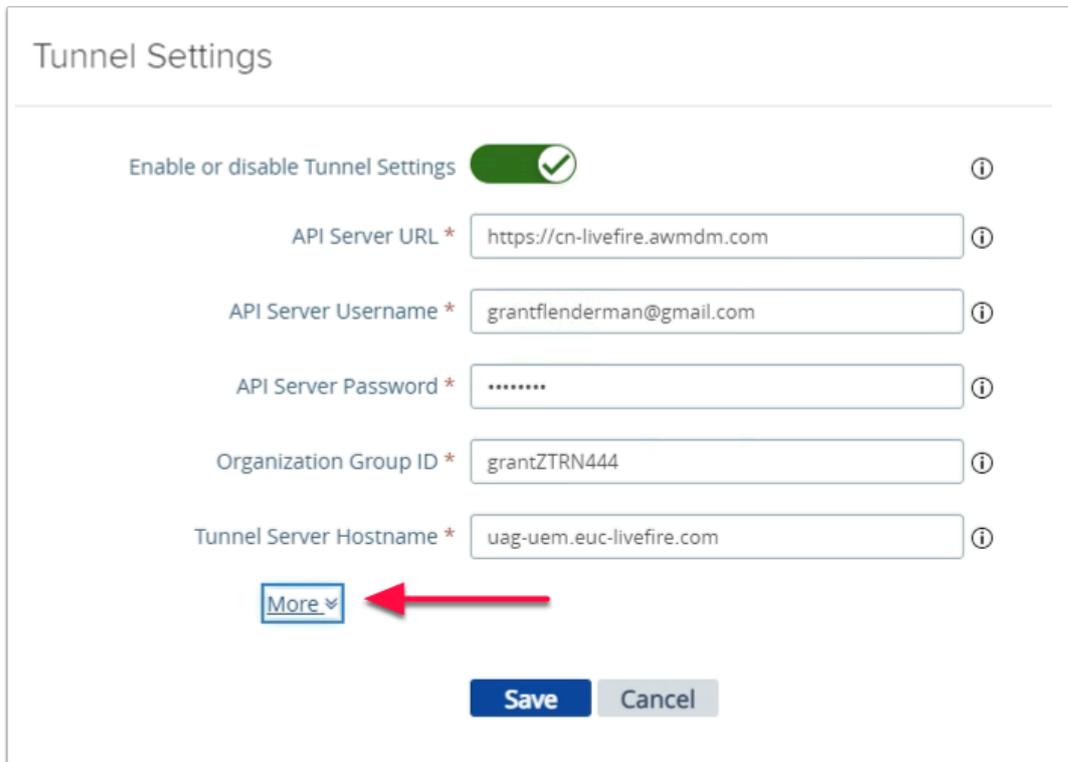


3. Next to **Edge Service Settings**

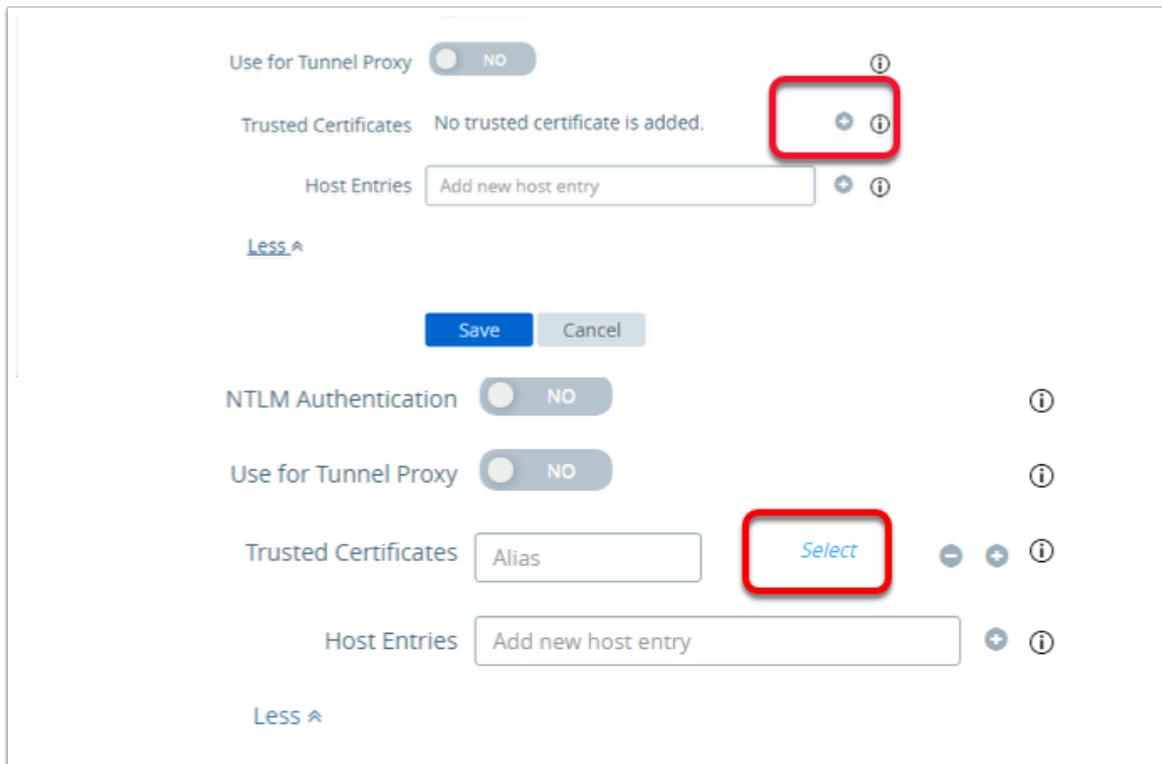
- Select **Show**
- Next to **Tunnel Settings** the **Gear icon**



4. In the **Tunnel Settings** window, next to **Enable Tunnel Settings**, change the setting from **NO** to **YES**

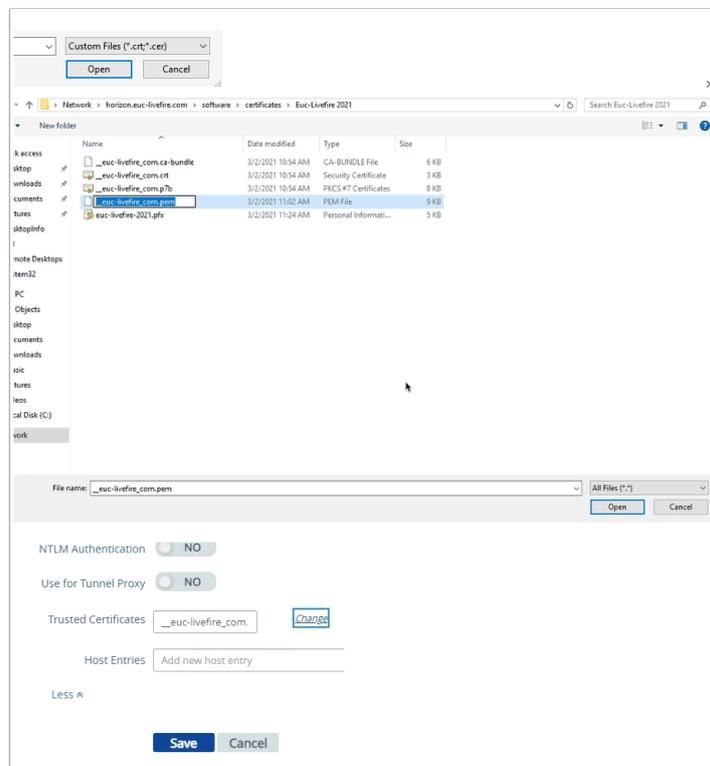


5. Now that Tunnel Settings are enabled, we have a list of configurations to do, Use your Datasheet to get this information
- Enter the following next to:
 - **API Server URL *** enter : <https://cn-livefire.awmdm.com>
 - **API Server Username *** enter : your custom **UEM Admin account**
 - **API Server Password *** enter : your custom **UEM Admin password**
 - **Organization Group ID*** enter : your custom **UEM Group ID**
 - **Tunnel Server Hostname *** enter uag-uem.euc-livefire.com
 - At the bottom of the **Tunnel Settings** window, expand **More**



6. Find the **Trusted Certificates**, section

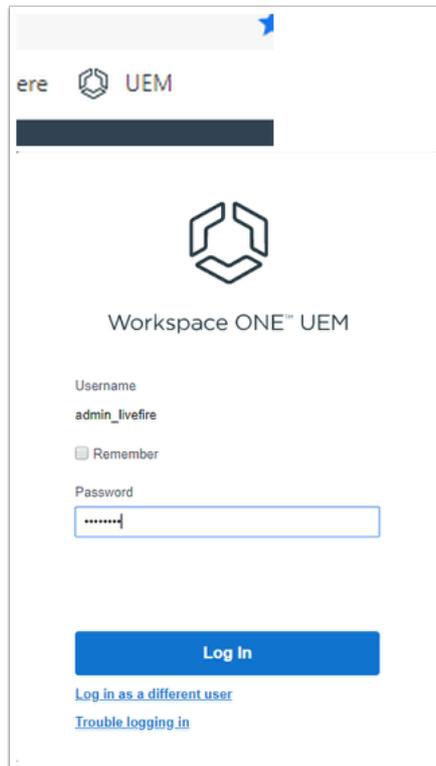
- To the right of **Trusted Certificates**, click the **+ icon**
- Click the **Select** button



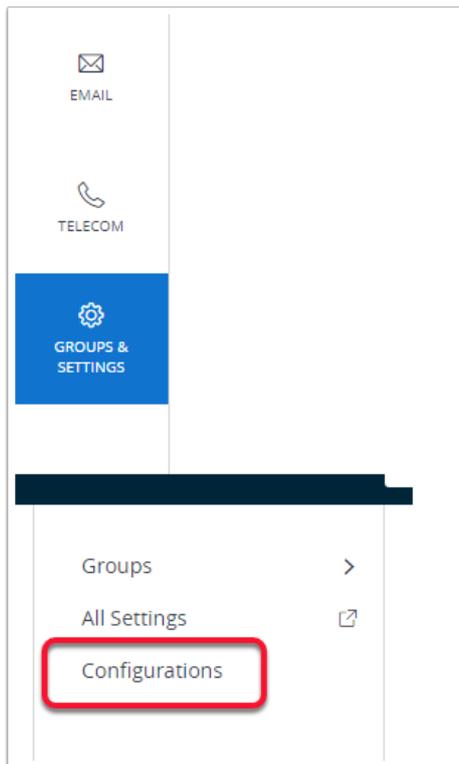
7. In the **address bar**,

- Enter the following path [\\Horizon.euc-livefire.com\software\certificates\Euc-Livefire 2021](#)
- In **Open Files** window, change **Custom Files (*.crt;*.cer)** to **All Files (*.*)**
- Select the [_euc-livefire_com.pem](#) file and select **Open**
- At the bottom of the **Tunnel Settings** window select **Save**

Part 2: - Configuring the VMware Tunnel Edge Service

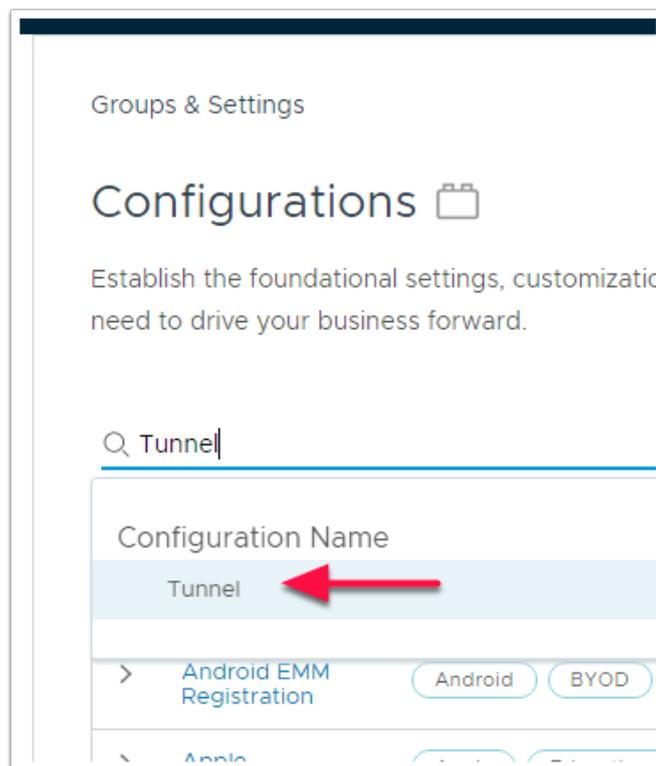


1. On your **ControlCenter** server,
 - Open your **Chrome** browser
 - In the address bar type <https://cn-livefire.awmdm.com> .
 - Under **Username** enter your custom **UEM username**
 - Select **Next**
 - Under **Password** enter **VMware1!** and select **Log In**



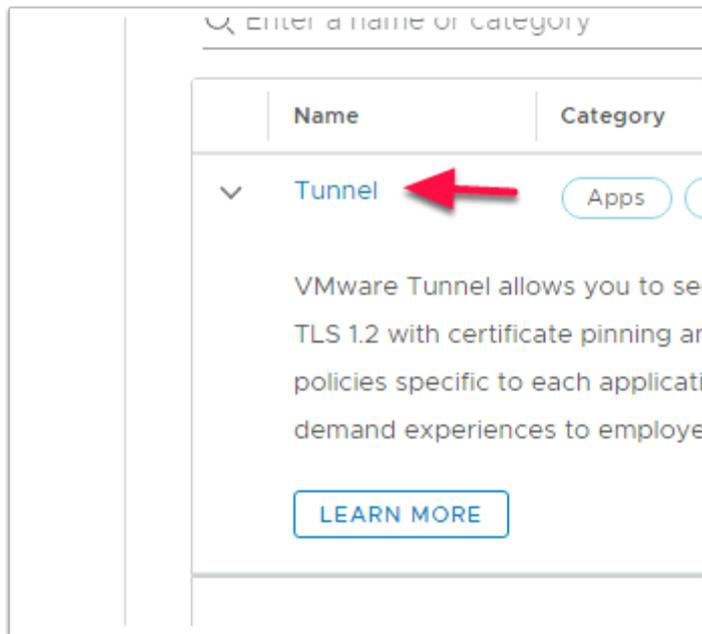
2. In the **Workspace ONE UEM** Console:

- Select **Groups & Settings**.
- Select **Configurations**.

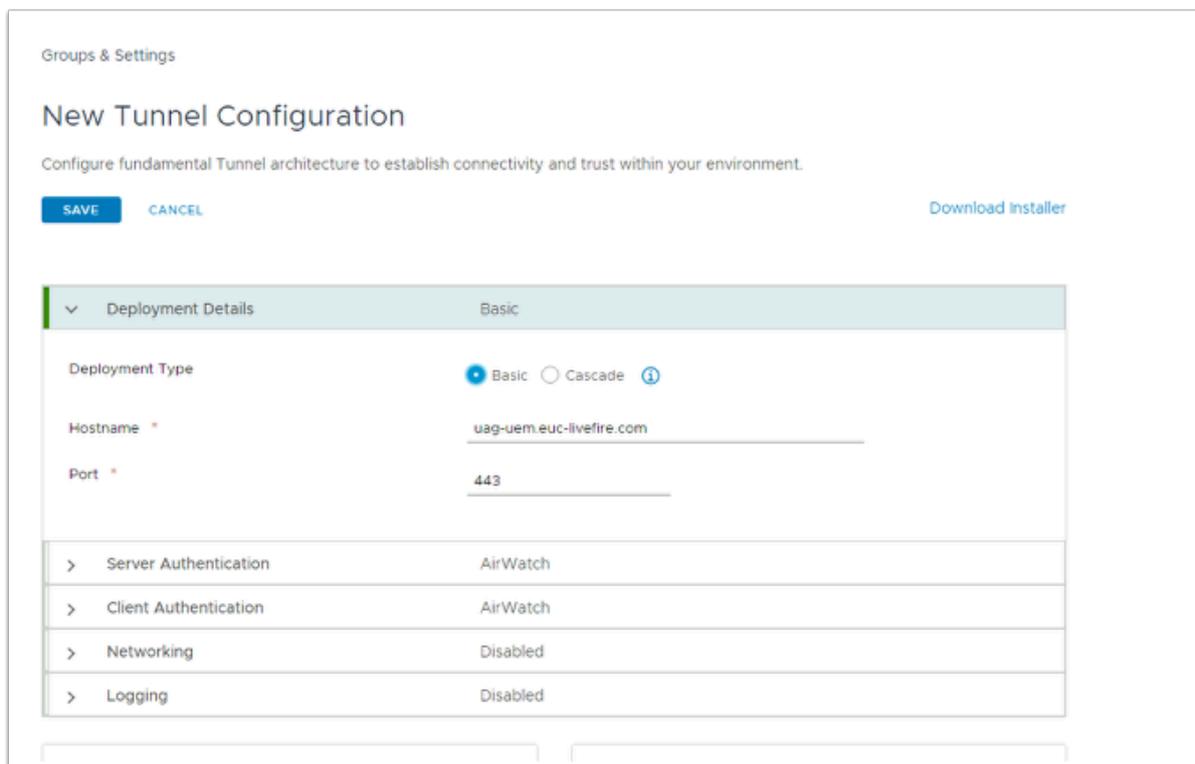


3. Under **Configurations**, in the **Enter a name or category** type **Tunnel**

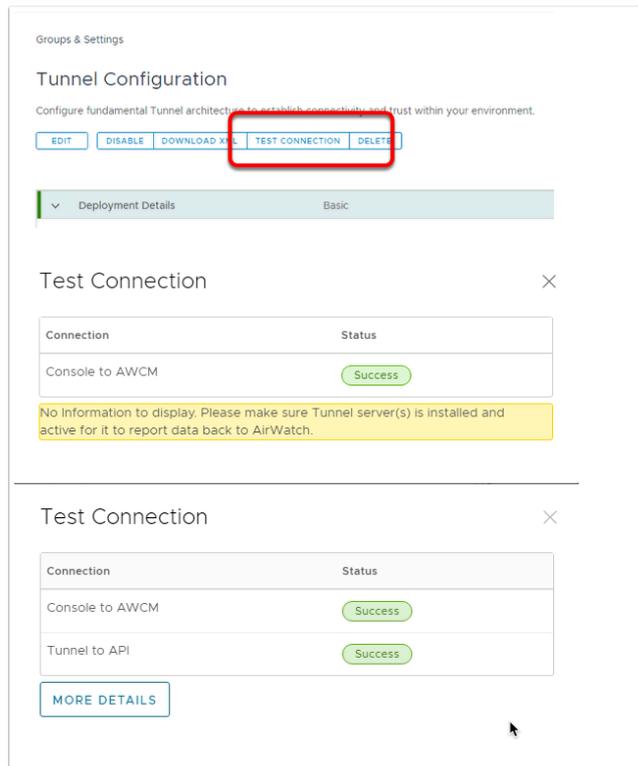
- When **Tunnel** shows under **Configuration Name** select **Tunnel**



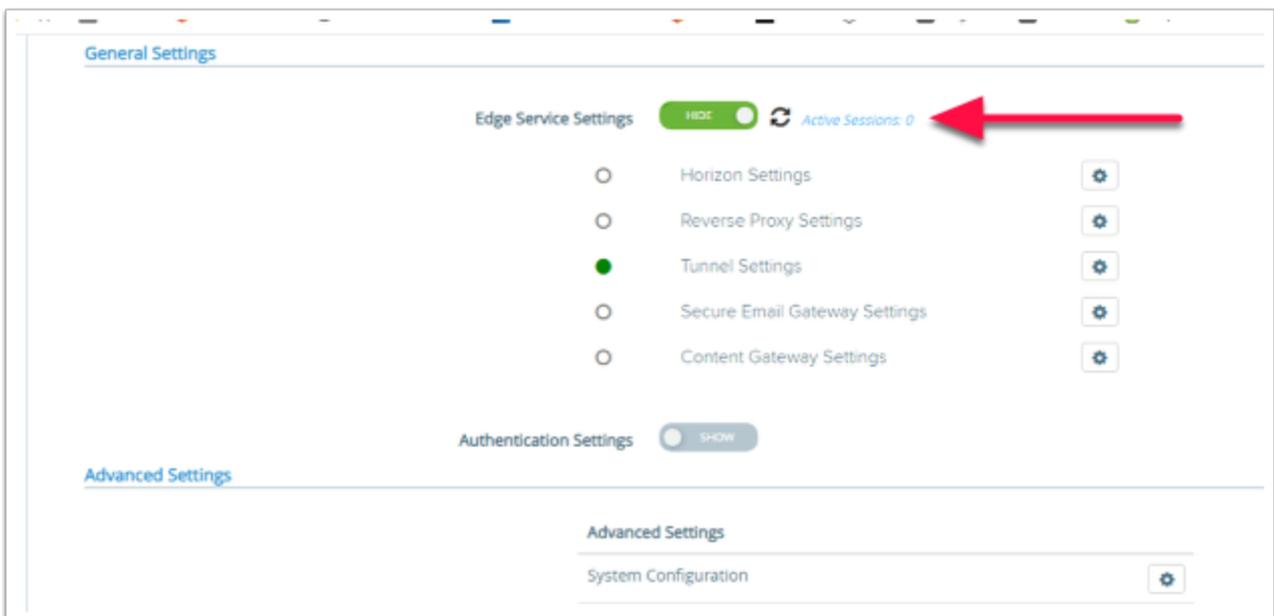
4. Under **Name** select **Tunnel**



5. In the **New Tunnel Configuration** add the following:
- Next to **Hostname** enter **uag-uem.euc-livefire.com**
 - Next to **Port** enter **443**
 - Select **SAVE** in the top left of the page



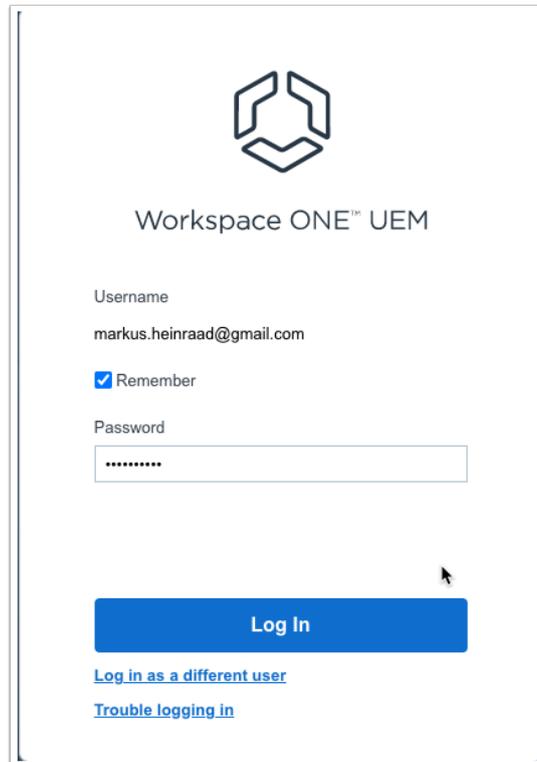
6. In the **Tunnel Configuration** page select **TEST CONNECTION**,
- You should have two responses
 - Console to AWCM**
 - Tunnel to API**
 - Status** should read **Success** on both, but if you see one, carry on with your labs, it can take a while for this to show



7. Revert back to your **UAG Console Edge Service** settings and select the **refresh** next to **Active Sessions**.

- You will now notice you have a **green light** next to **Tunnel Settings**
 - **Note! Sometimes it takes a while for this to show green. Move on and come back to check your status if necessary.**

Part 3: Configuring Device Traffic Rules for Windows 10



Workspace ONE™ UEM

Username
markus.heinraad@gmail.com

Remember

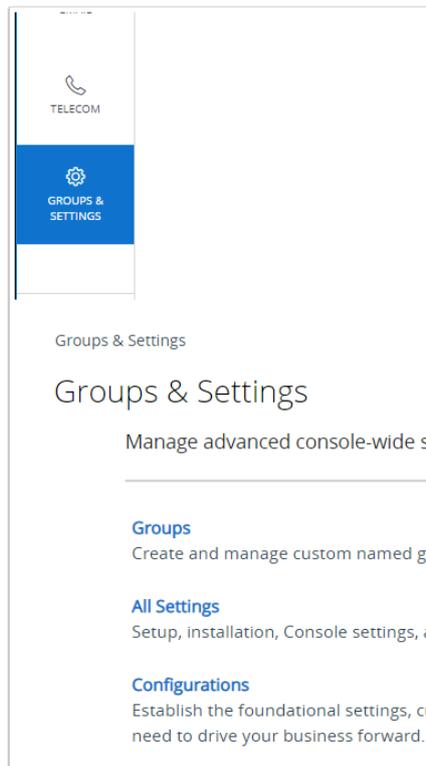
Password
.....

[Log In](#)

[Log in as a different user](#)

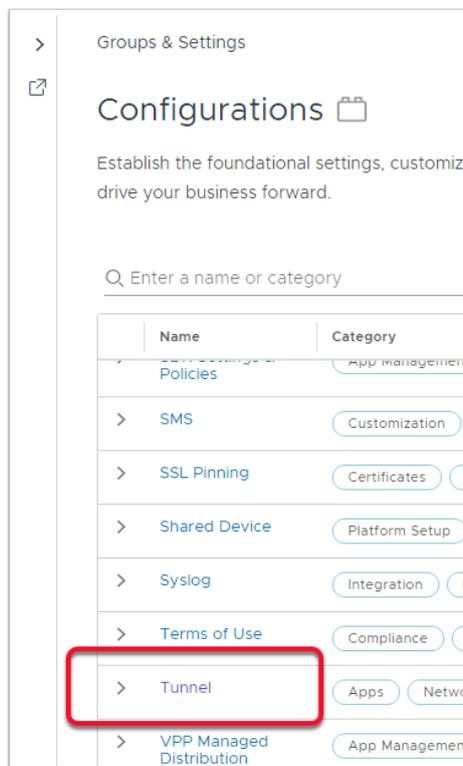
[Trouble logging in](#)

1. If necessary log in to your **Workspace ONE UEM** console
 - Log in using your custom username **custom username** and password **custom password**
 - Select **Log In**



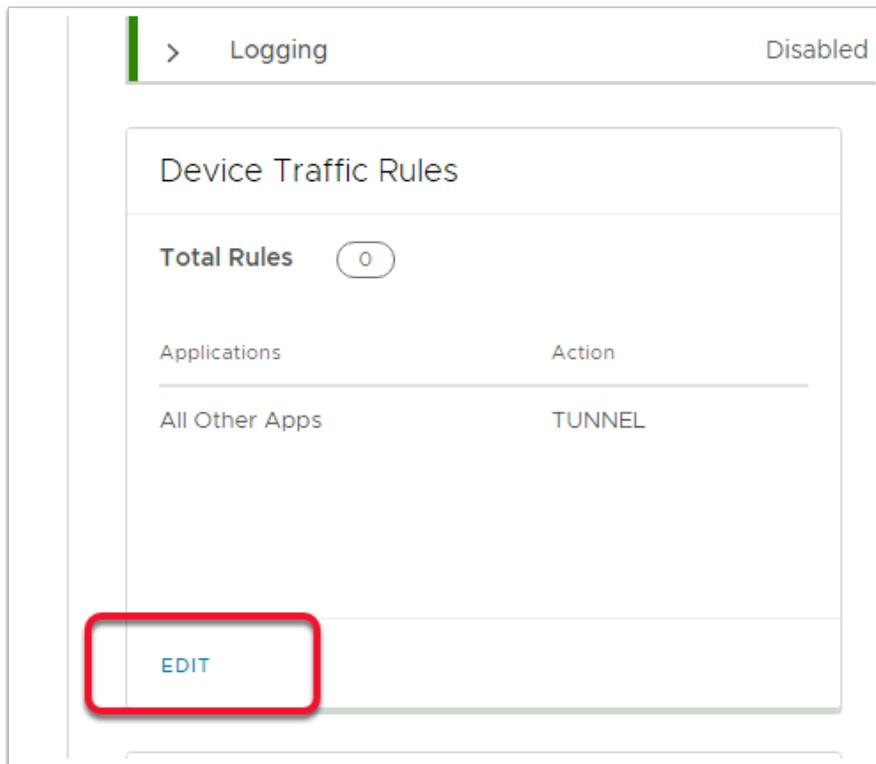
2. In the **UEM Console**,

- Select **GROUPS & SETTINGS**,
- Select **Configurations**

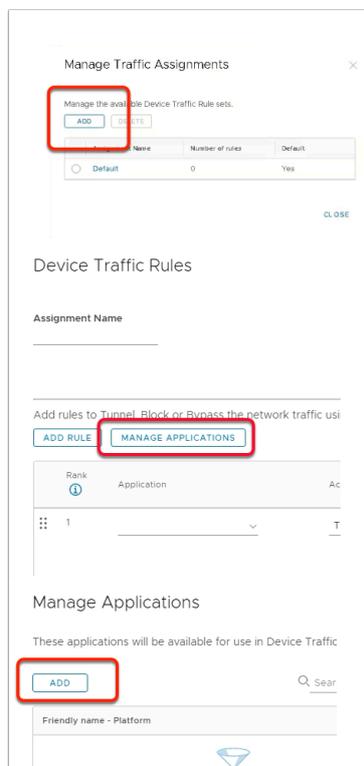


3. In the **Configurations** for **Groups & Settings**, **scroll down** until you find **Tunnel**,

- Select **Tunnel**



4. In the **Tunnel Configuration** window under **Device Traffic Rules** select **EDIT**



5. Under **Manage Traffic Assignments**

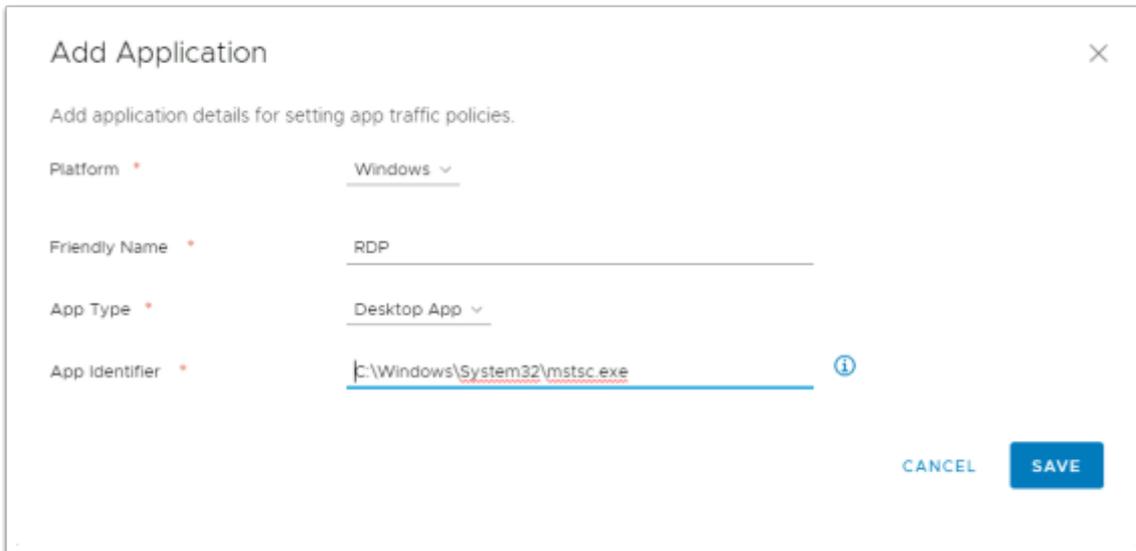
- Select **ADD**
- Select **MANAGE APPLICATIONS**

- In **Manage Applications** window
 - Select **ADD**

6. In the **Add Application** window we have to add the following information, next to:-
- **Platform *** (Leave as default) **Windows**
 - **Friendly Name *** type **Livefire Chrome Tunnel**
 - **App Type *** select **Desktop App**
 - **App Identifier *** **C:\Program Files\Google\Chrome\Application\chrome.exe**
 - Select **SAVE**

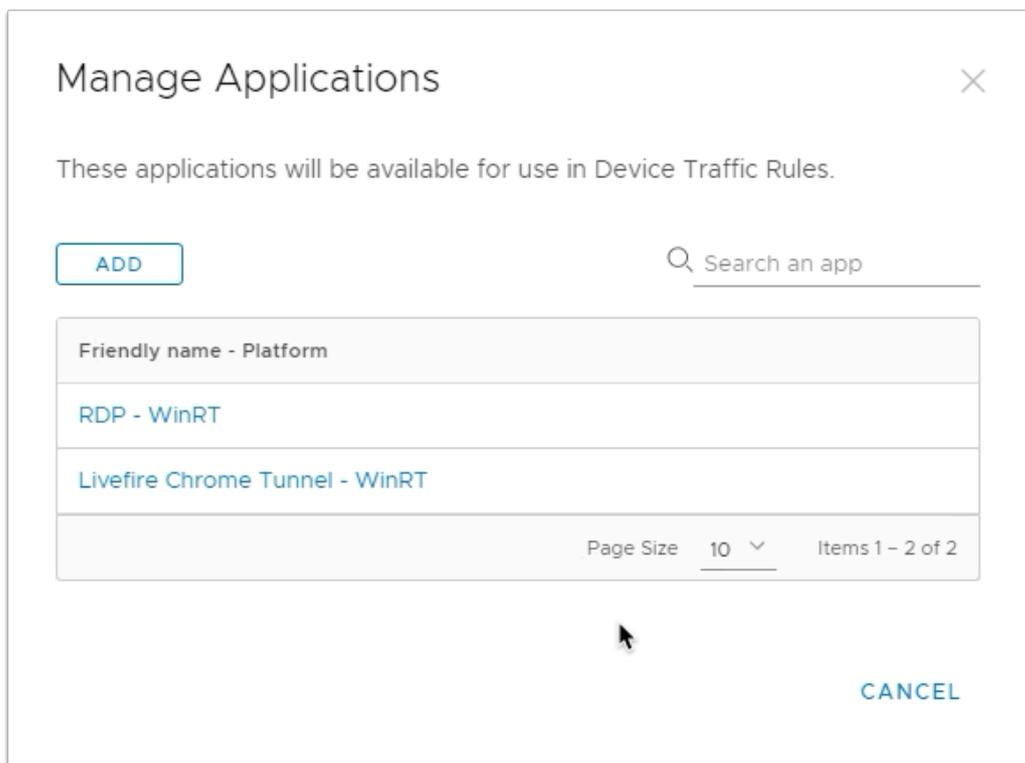
7. In the **Manage Applications** window

- Select **ADD**



8. We will now add the Remote Desktop client. This allows end users to connect to Remote Desktop Hosts located behind the corporate firewall.

- In the **Add Application** window we have to add the following information, next to:-
 - **Platform *** (Leave as default) **Windows**
 - **Friendly Name *** type **RDP**
 - **App Type *** select **Desktop App**
 - **App Identifier *** type: **C:\Windows\System32\mstsc.exe**
 - Select **SAVE**



9. In the **Manage Applications** window

- Select **ADD**

Add Application [X]

Add application details for setting app traffic policies.

Platform * Windows ▾

Friendly Name * System

App Type * Desktop App ▾

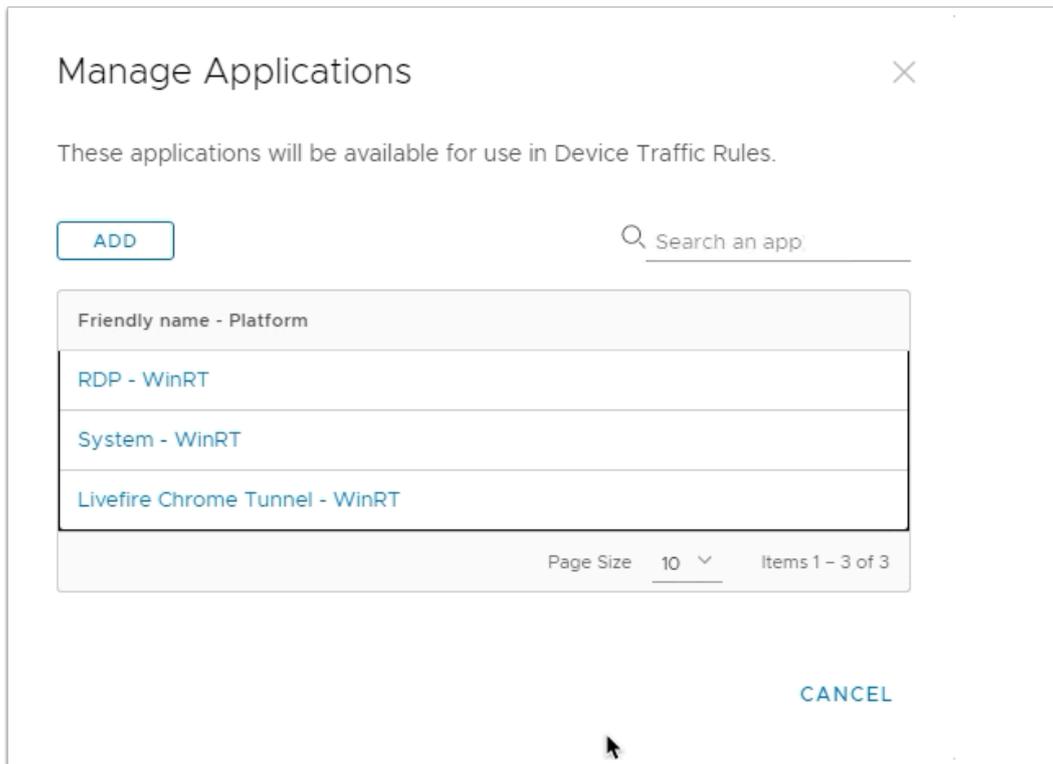
App Identifier * System ⓘ

CANCEL SAVE

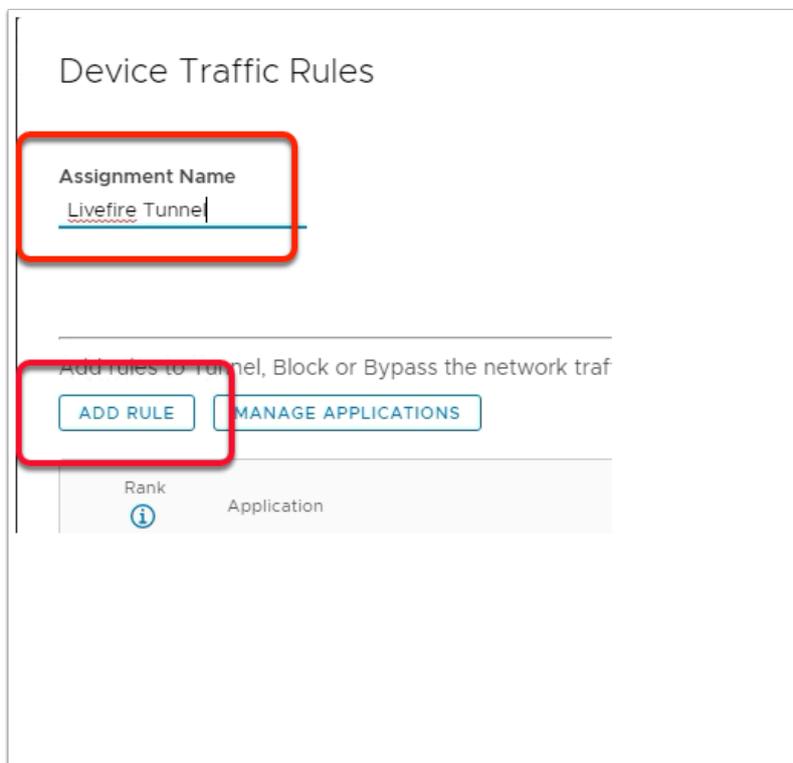
10. We add support for tunneling SMB traffic from system to allow users to map network shares and network printers. This allows end users to connect to file shares and printers that are located behind the corporate firewall. As the SMB protocol built into the Windows Operating system, the App Identifier is not an executable, instead you defined System as the App Identifier.

In the **Add Application** window we have to add the following information, next to:-

- **Platform *** (Leave as default) **Windows**
- **Friendly Name *** type **System**
- **App Type *** select **Desktop App**
- **App Identifier * type:** **System**
- Select **SAVE**

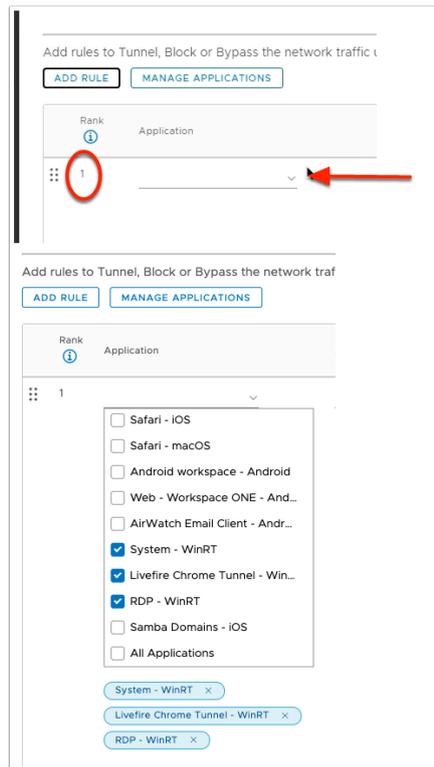


11. In the **Manage Applications** window,
- Select **CANCEL**



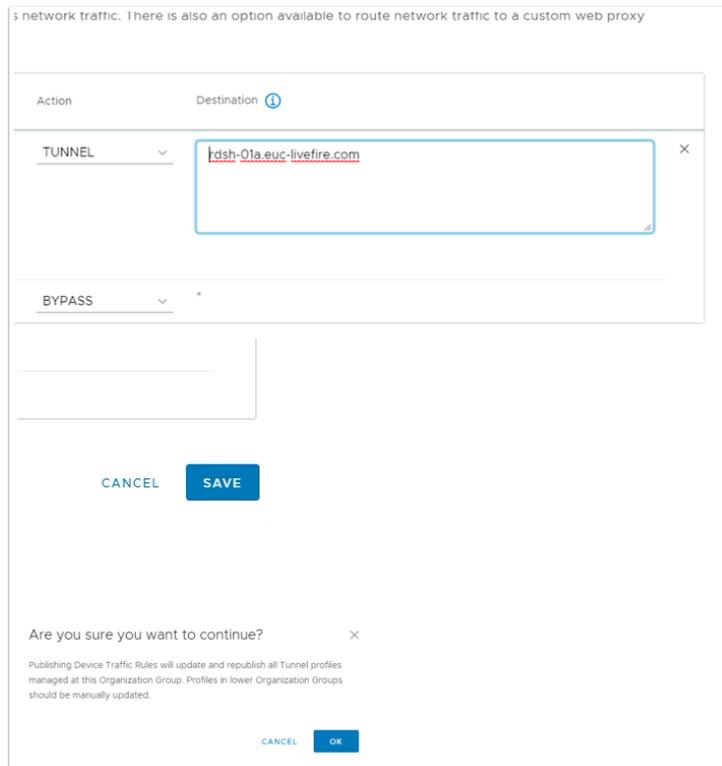
12. In the **Device Traffic Rules** window,
- Under Assignment Name
 - Type **Livefire Tunnel**

- Select **ADD RULE**



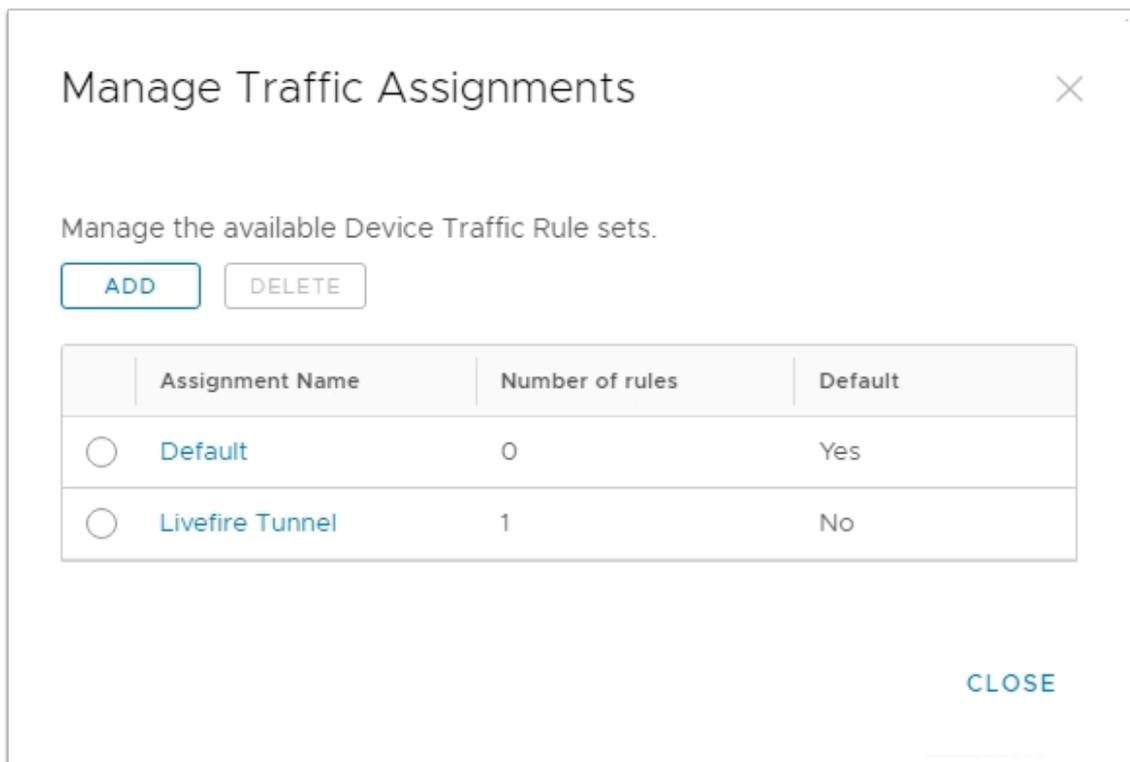
13. In the row of **Rank 1** under **Application**

- Select the **drop-down**
 - Select the following **checkboxes**
 - **Livefire Chrome Tunnel**
 - **RDP - Livefire**
 - **System - Livefire**



17. Under **Destination** enter the following:-

- Type: **rdsh-01a.euc-livefire.com**
- Select **SAVE**
 - In the **Are you sure you want to continue?** window
 - select **OK**

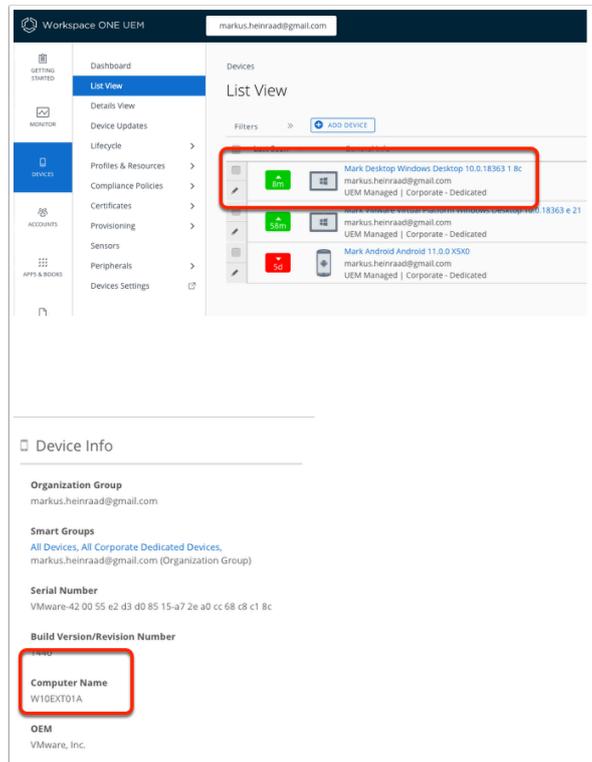


18. In the **Manage Traffic Assignments** window

- Select **CLOSE**

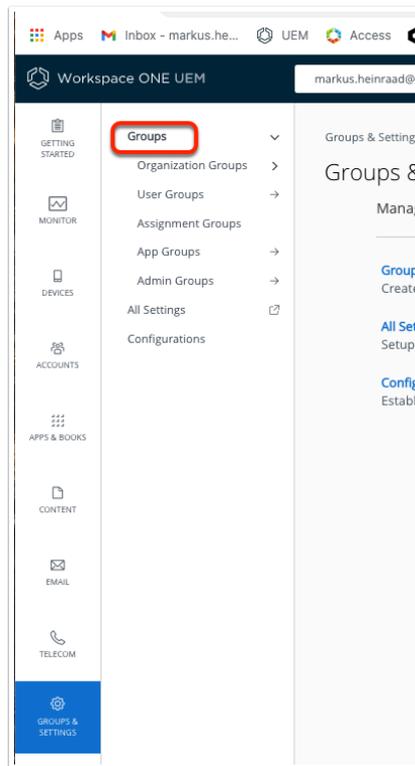
Part 4: Distributing Workspace ONE Tunnel Application, for Windows 10

The Goal of the first few steps is to Identify the Windows Desktop W10EXT01a



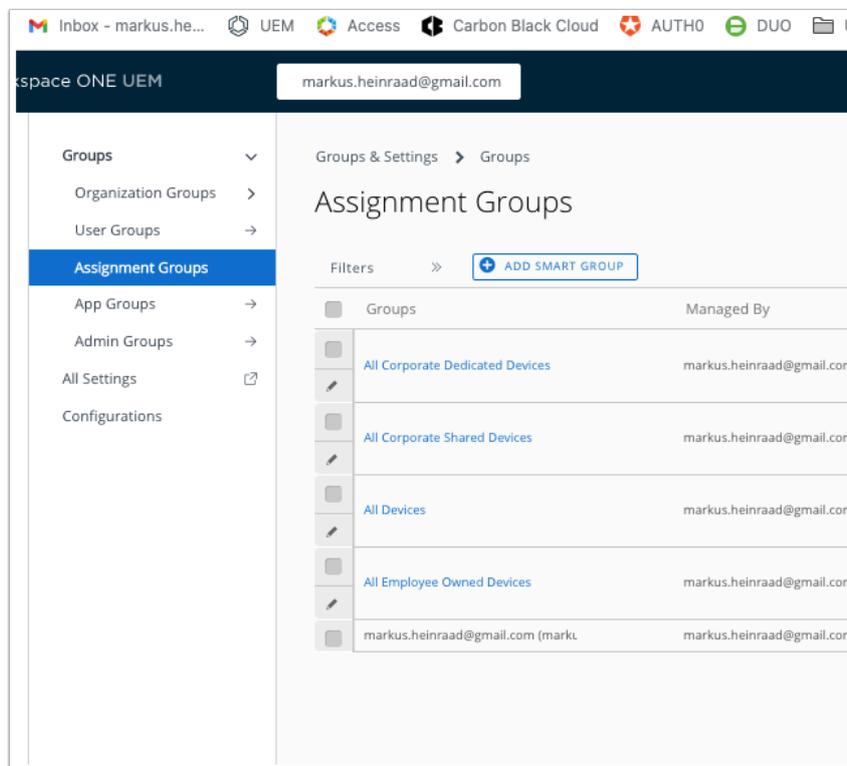
1. On your **ControlCenter** server

- Log in to **Workspace ONE UEM** with your custom credentials
- Select **Devices** > **List View**
- Select the equivalent of your xxxx **Desktop Windows Desktop 10.0.18363 1 8c**
- Under **Device Info**, confirm that the computer name is **W10EXT01a**
 - Once validated, make a note of the computer Device Enrollment under **List View**. In this example its
 - **Mark Desktop Windows Desktop 10.0.18363 1 8c**



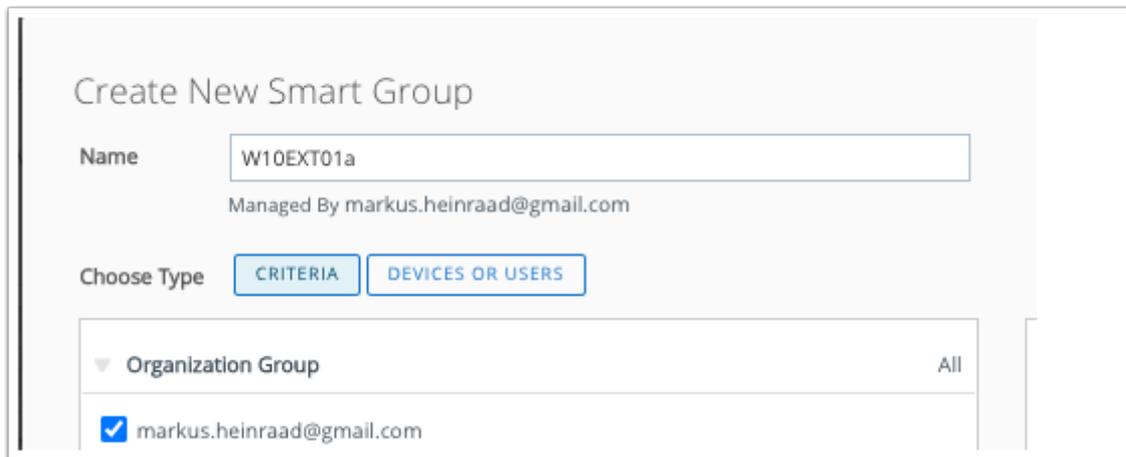
2. In the Workspace ONE UEM admin console

- Select **GROUPS & SETTINGS > Groups > Assignment Groups**



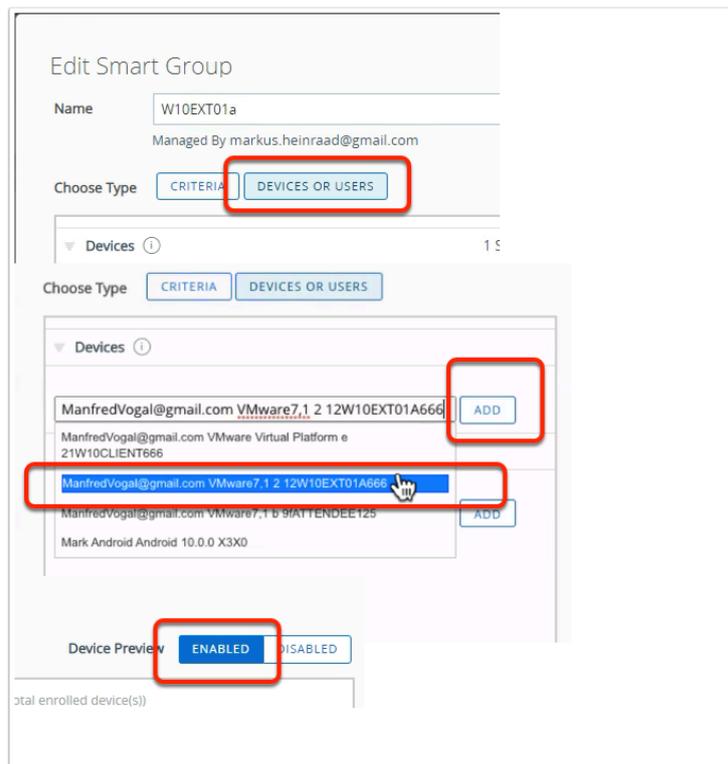
3. In the **Assignment Groups** window

- Select **ADD SMART GROUP**



4. In the **Create New Smart Group** window

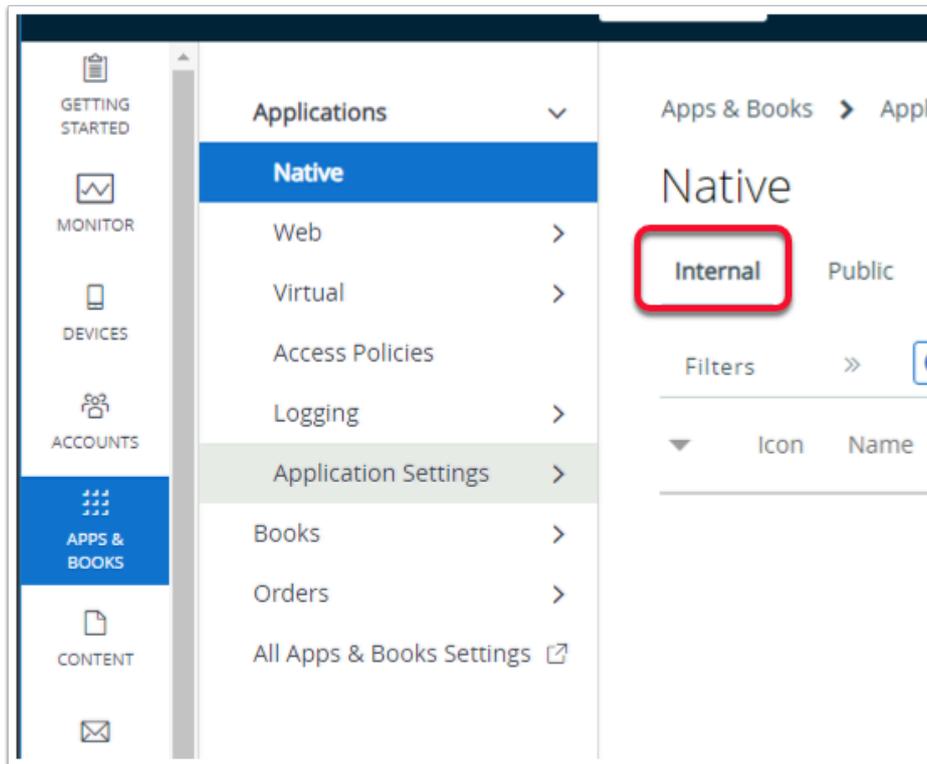
- Add the following, next to:
 - Name: **W10EXT01a**



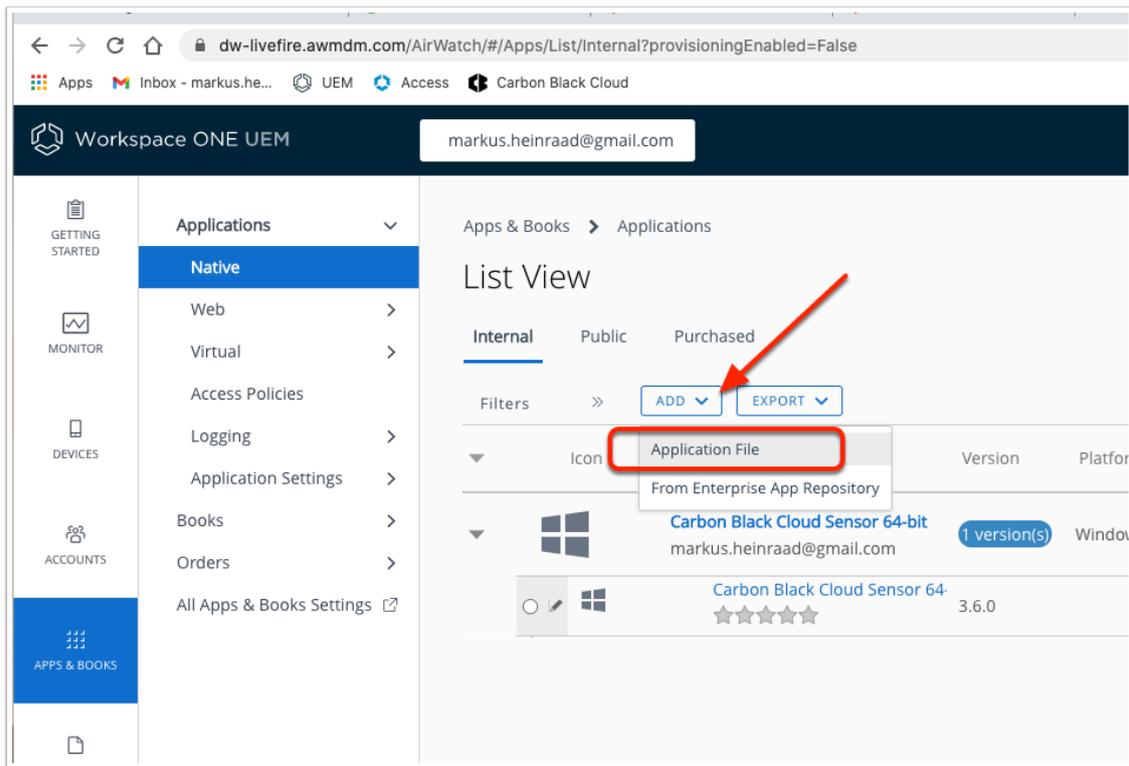
5. Next to **Choose type**

- Select **DEVICES OR USERS**
 - Under **Devices**, in the box, select **your eg Mark Windows Desktop** (for W10EXT01a)
 - (The example in the screenshot is what this test environment looks like, ensure you are select yours)
 - Select **ADD**
- To the right of the window,

- Next to **Device Preview**, select **ENABLED**
- Select **SAVE**

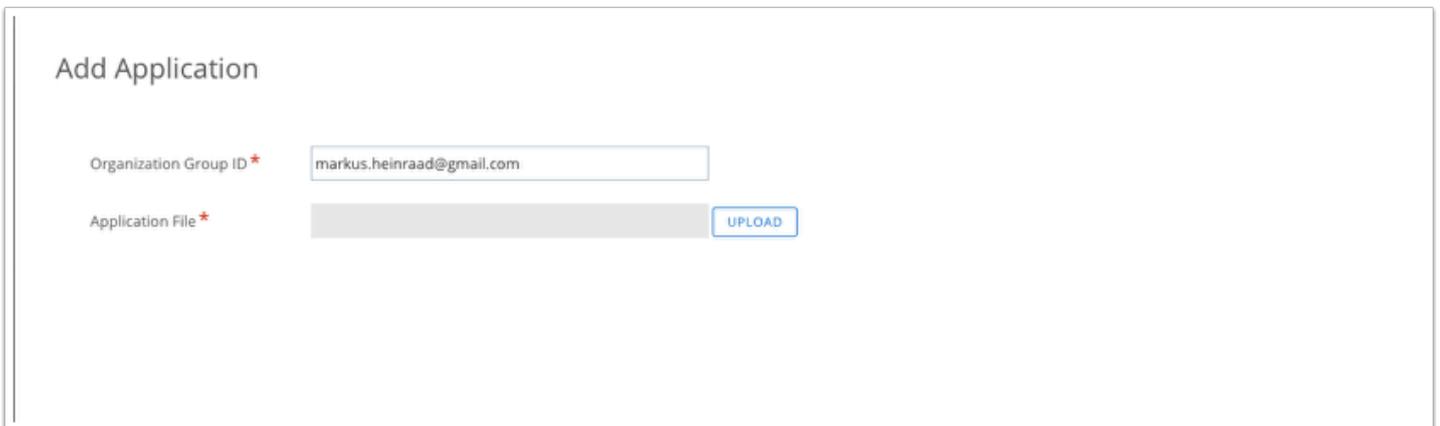


6. On your ControlCenter server
 - If necessary Login <https://cn-livefire.awmdm.com>
 - with your custom username and password
 - Select **APPS & BOOKS** > **Native**
 - Under **Native**, select **Internal**



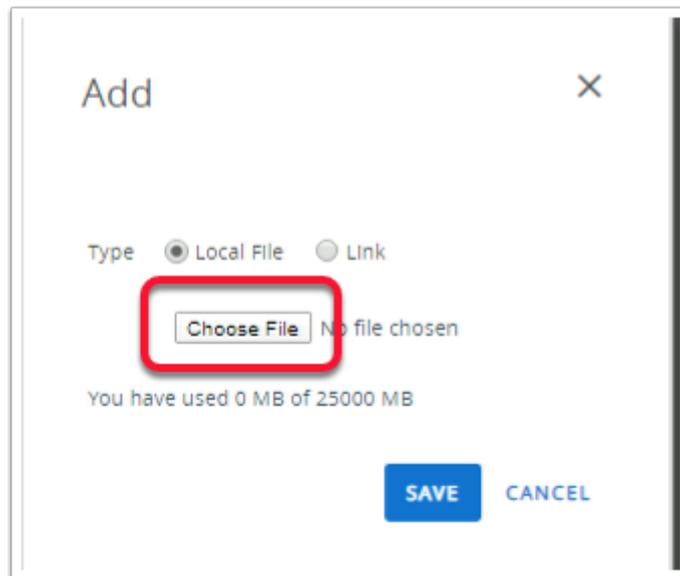
7. Under **Internal**

- Select the dropdown next to **ADD**
- Select **Application File**

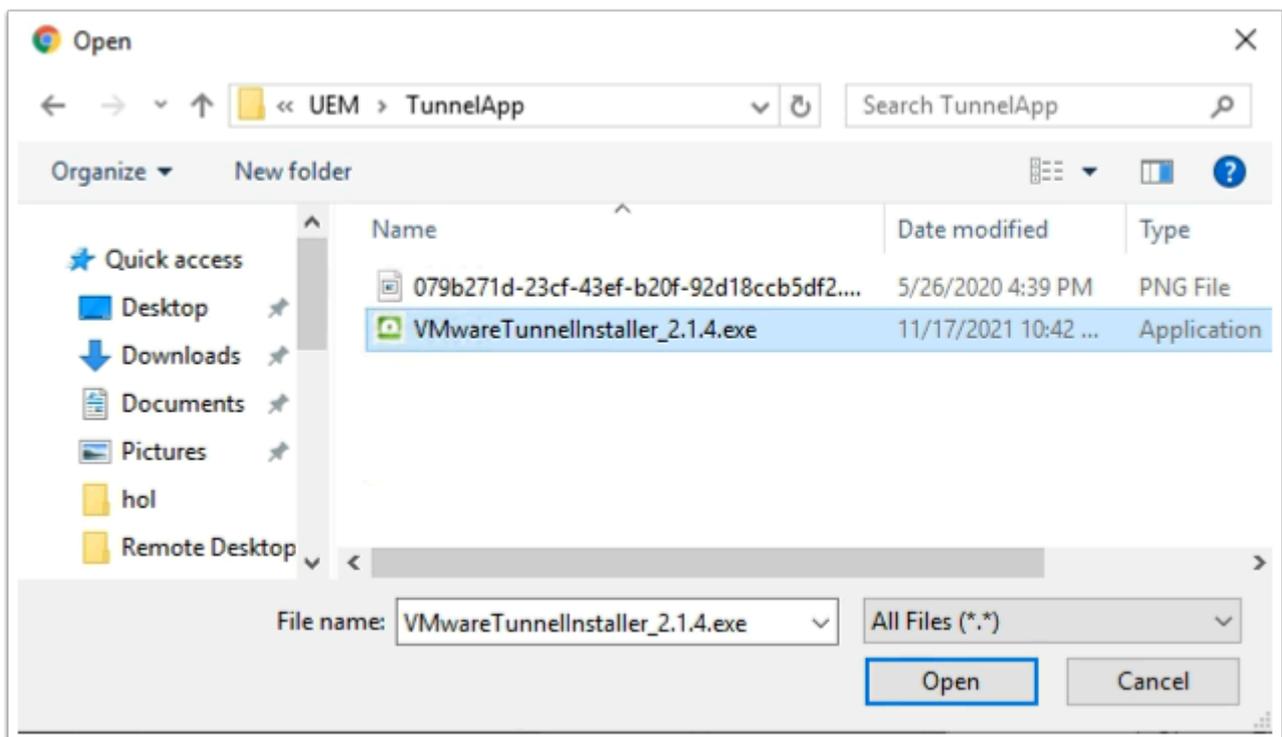


8. In the **Add Application** window,

- Select **UPLOAD**

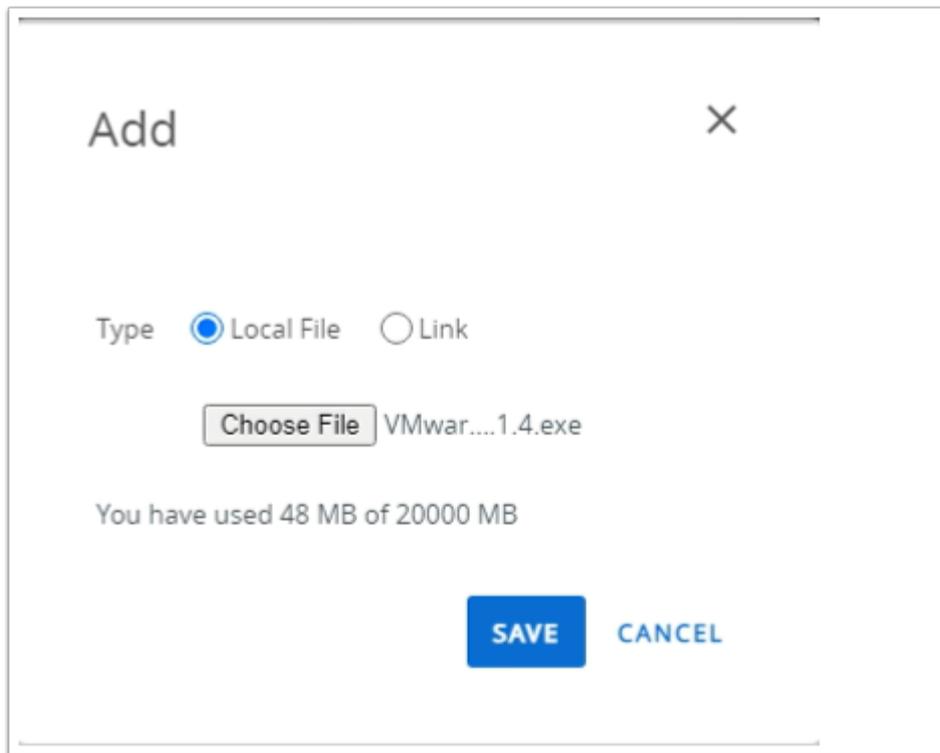


9. In the **Add** window select the **Choose File** button

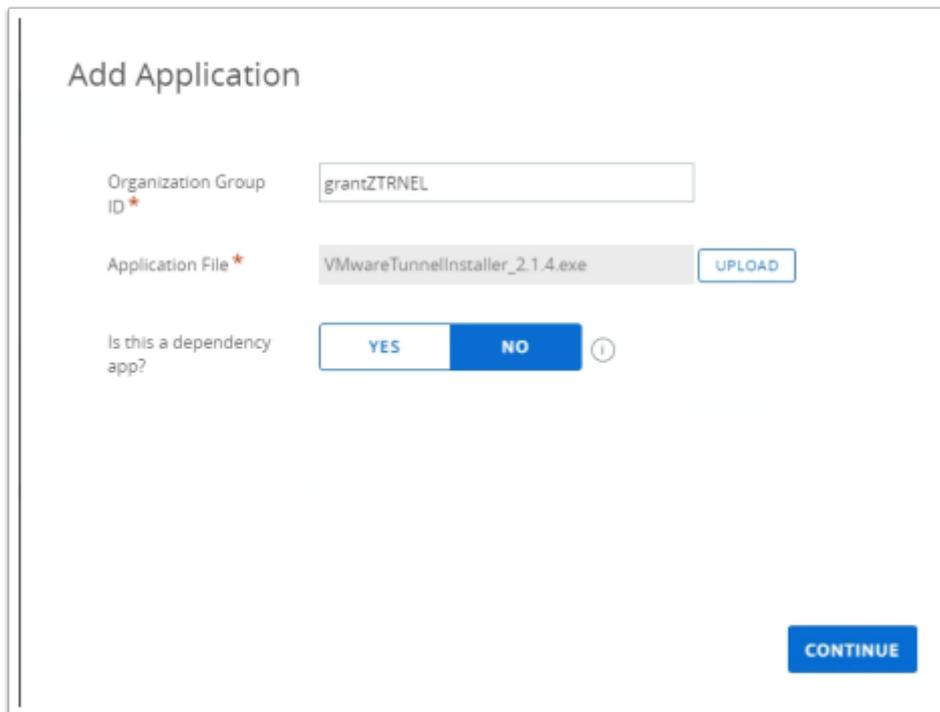


10. In the File upload window

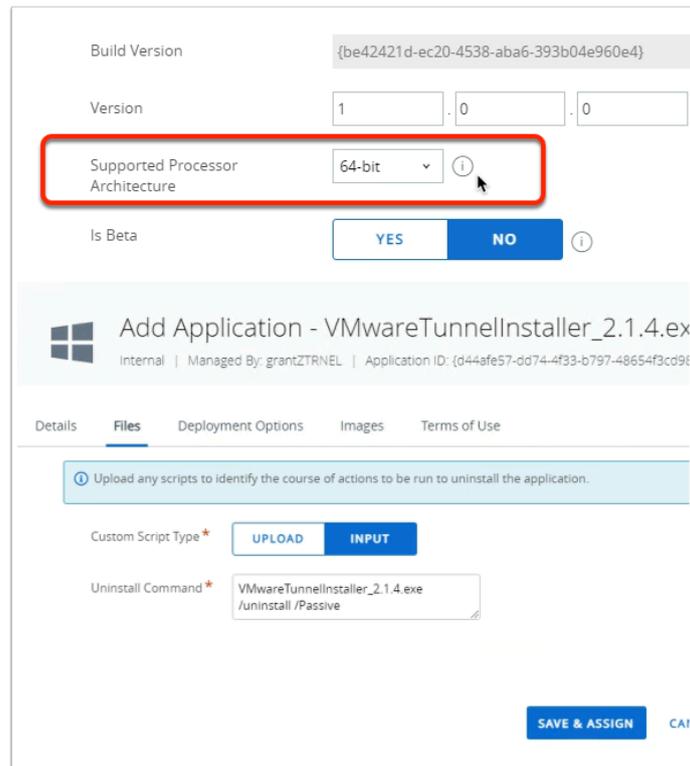
- Browse to **\\horizon.euc-livewire.com\software\UEM\TunnelApp**
- Select the **VMwareTunnelInstaller_2.1.4.exe** APP
- At the bottom of the window select **Open**



11. In the **Add** window ,
- Select **SAVE**



12. In the **Add Application** window,
- Select **CONTINUE**



13. In the **Edit Application - VMwareTunnelInstaller_2.1.4.exe** window
 - In the **Details** tab
 - Next to **Supported Architecture**, change it from **32-bit** to **64-bit**
 - Select the **Files** tab
 - Scroll down to **Uninstall Command *** ,
 - **Copy** and **paste** the following box to the right of **Uninstall Command ***
 - **VMwareTunnelInstaller_2.1.4.exe /uninstall /Passive**

Edit Application - VMwareTunnelInstaller_2.1.2.exe..
 Internal | Managed By: MalmonDier | Application ID: {71de0118-f731-4487-bf30-fa3017293212} |

Details Files **Deployment Options** Images Terms of Use

Install Context **DEVICE** USER ⓘ

Install Command * VMwareTunnelInstaller_2.1.2.exe /Install /F ⓘ

Admin Privileges **YES** NO ⓘ

Device Restart User-engaged restart ⓘ

Number of days after 7 ⓘ

SAVE & ASSIGN CANCEL

14. Select the **Deployment Options** Tab.

- **Scroll down** to find the **How To Install** section.
- Next to **Install Command ***, enter the following
 - **VMwareTunnelInstaller_2.1.4.exe /Install /Passive**
- Ensure **Admin Privileges** is set to **YES**.
- Next to **Device Restart** , from the dropdown, select **User Engaged Restart**.

Details Files **Deployment Options** Images Terms of Use

Retry Interval * 5 ⓘ

Install Timeout * 60 ⓘ

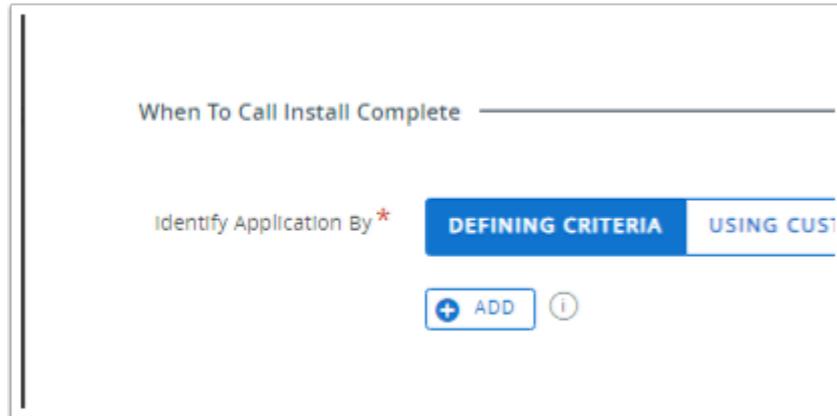
Installer Reboot Exit Code 3010 ⓘ

Installer Success Exit Code 0 ⓘ

15. In the **Deployment Options** Tab.

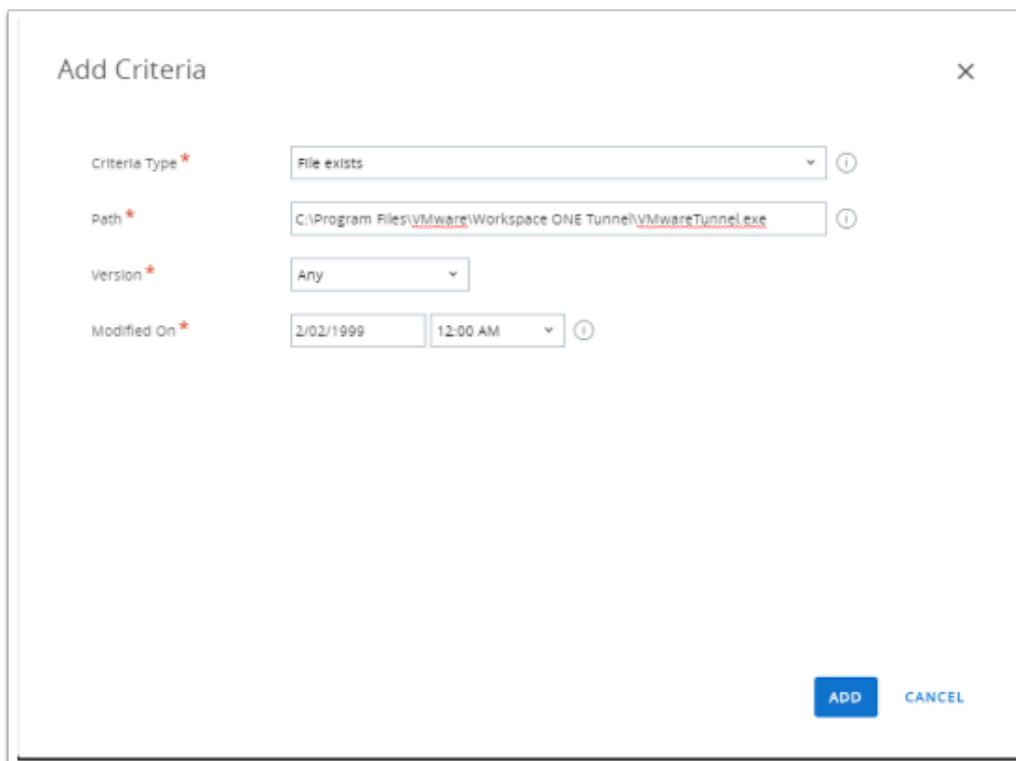
- **Scroll** down to **and next to**
 - **Installer Reboot Exit Code**, enter **3010**

- **Installer Success Exit Code**, enter **0**



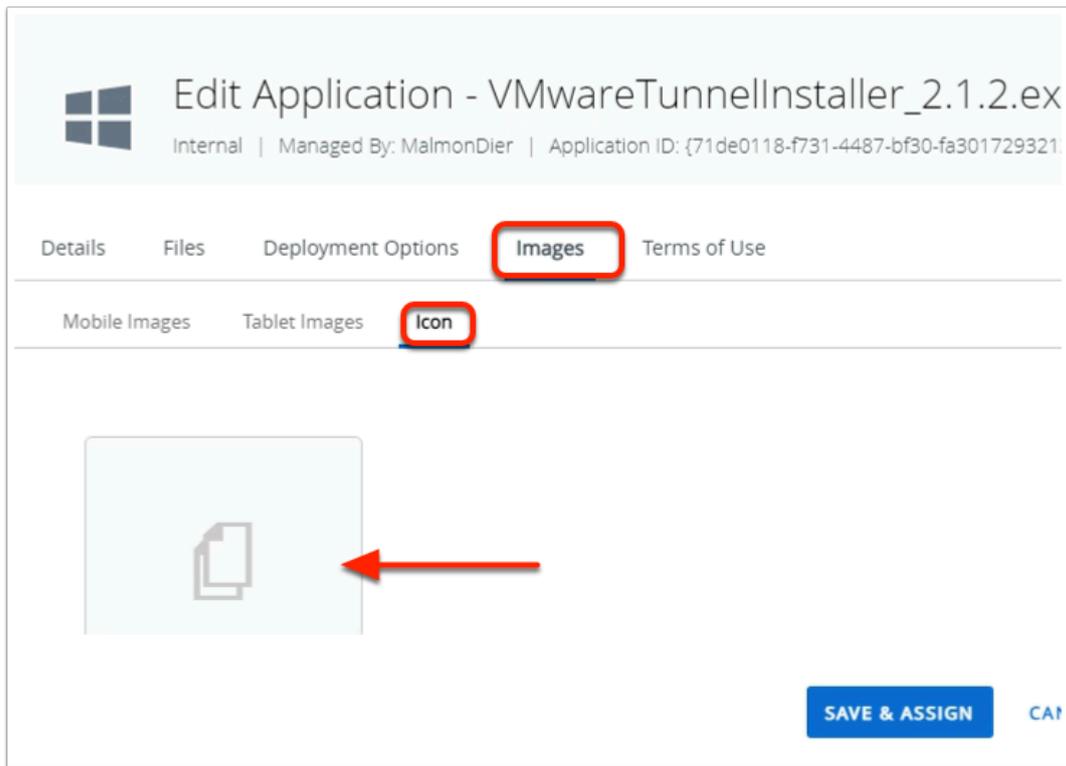
16. In the **Deployment Options** Tab.

- Scroll further down
 - In the **When to Call Install Complete** section, under **DEFINING CRITERIA**
- Select **+ ADD**



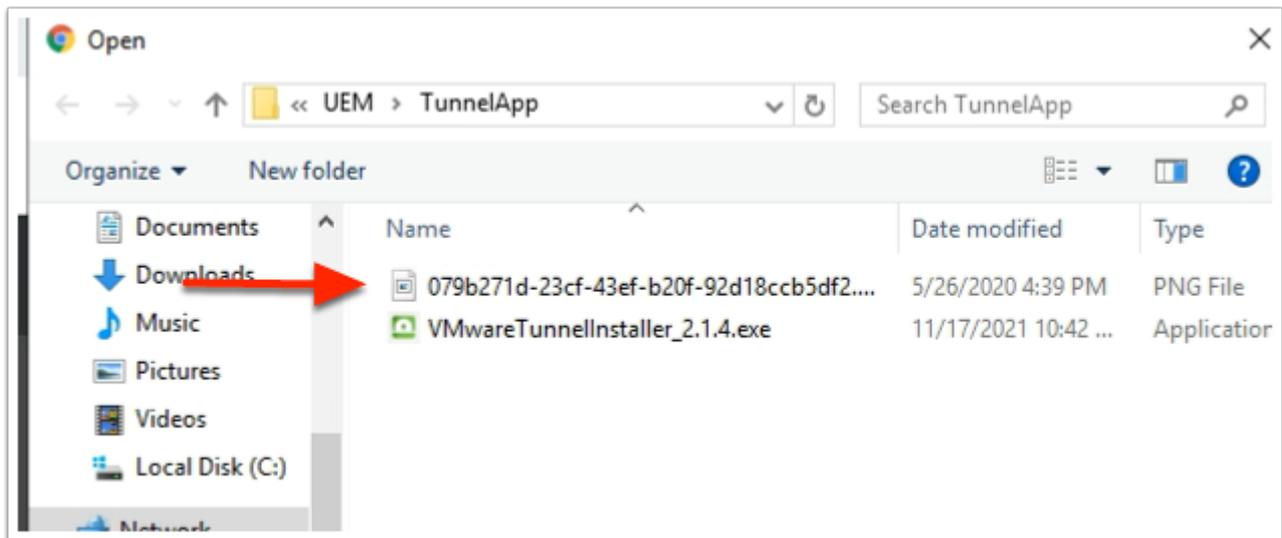
17. In the **Add Criteria** window

- Next to **Criteria Type** select **File Exists**
- Next to **Path**, enter **C:\Program Files\VMware\Workspace ONE Tunnel\VMwareTunnel.exe**
- Select **ADD**.



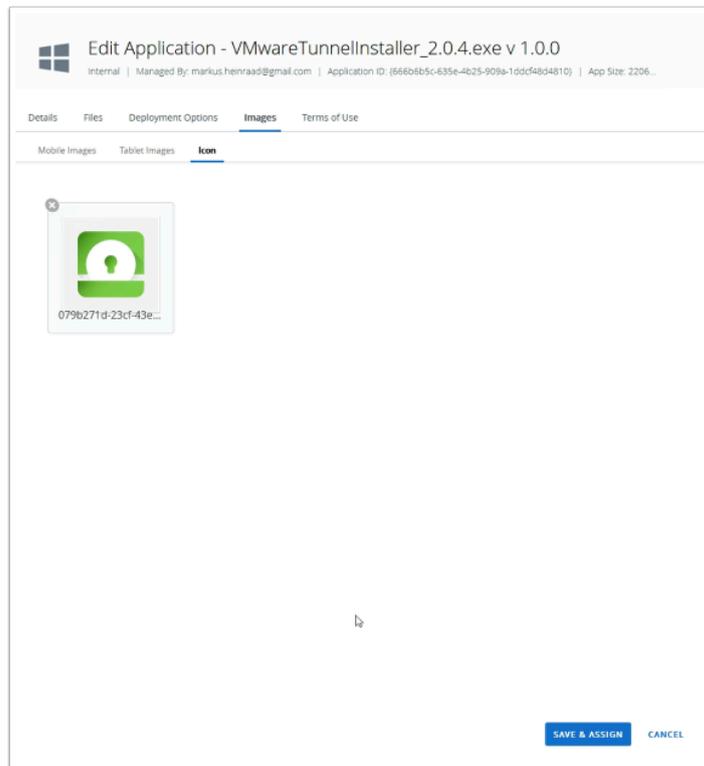
18. In the **Edit Application - VMwareTunnelInstaller_2.1.4.exe** window

- Select **Images** tab
- Select the **Icon** tab
- Select **Click or drag files here** area



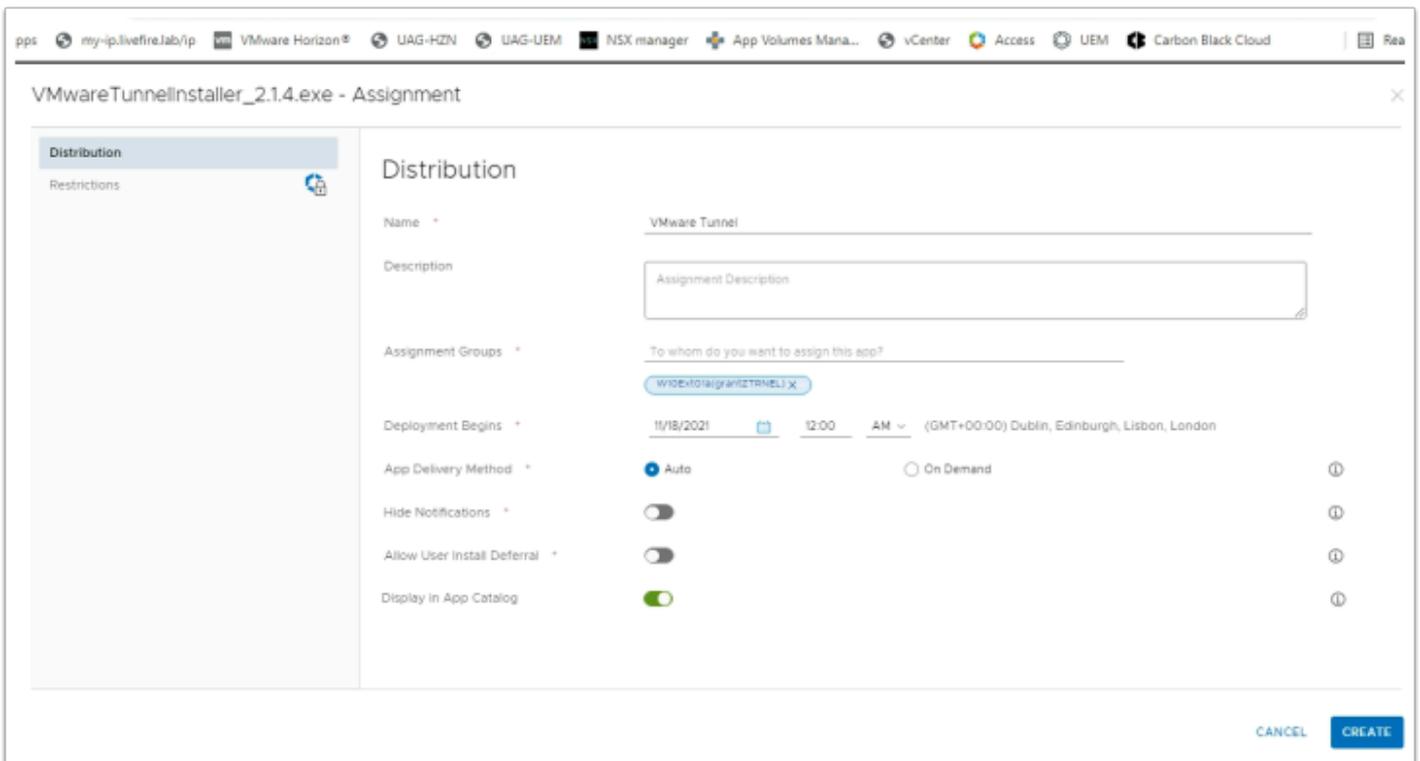
19. In the **Open** window,

- Select the **xxxxx.png** file
- Select **Open**



20. In the **Edit Application** window

- Select **SAVE & ASSIGN**



21. In the **VMwareTunnelInstaller_2.1.4.exe - Assignment** window

- Under **Distribution** enter and configure the following next to
 - **Name:** **VMware Tunnel**

- **Assignment Groups** : select **W10EXT01a**
- **Deployment begins** : **Enter a time 1 day, yesterday of your time.**
- **App Delivery Method** : Select the **Auto radio button**
- Select **CREATE**

VMwareTunnelInstaller_2.1.4.exe - Assignment

Details
 App Version : 1.0.0.0 UEM Version : 1.0.0.0 Platform : Windows Desktop Status : ✔ Active

Assignments Exclusions

Devices will receive application based on the configurations below. Devices with multiple assignments will receive assignment to edit. Adding a new assignment will create a new rule at the bottom of the list.

ADD ASSIGNMENT

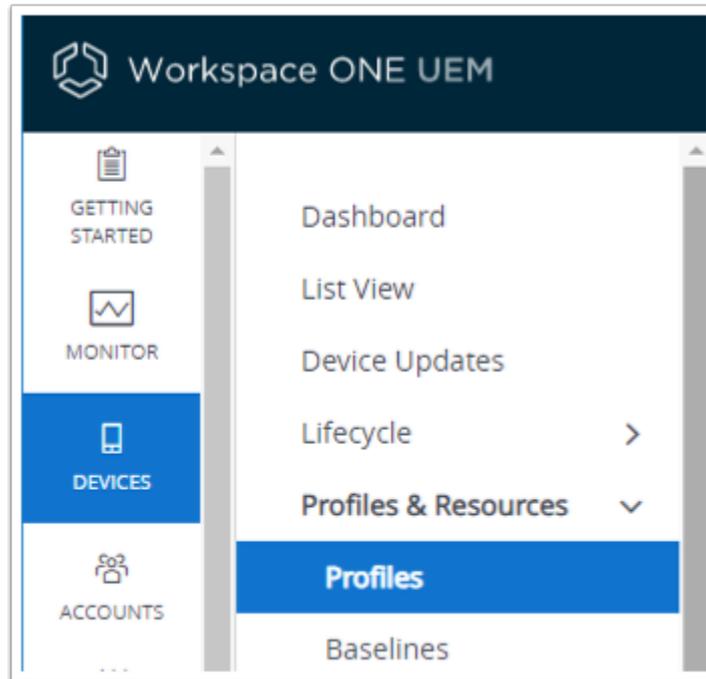
Priority	Assignment Name	Description
⋮ 0 ▾	VMware Tunnel	

VMwareTunnelInstaller_2.1.4.exe - Preview Assigned Devices

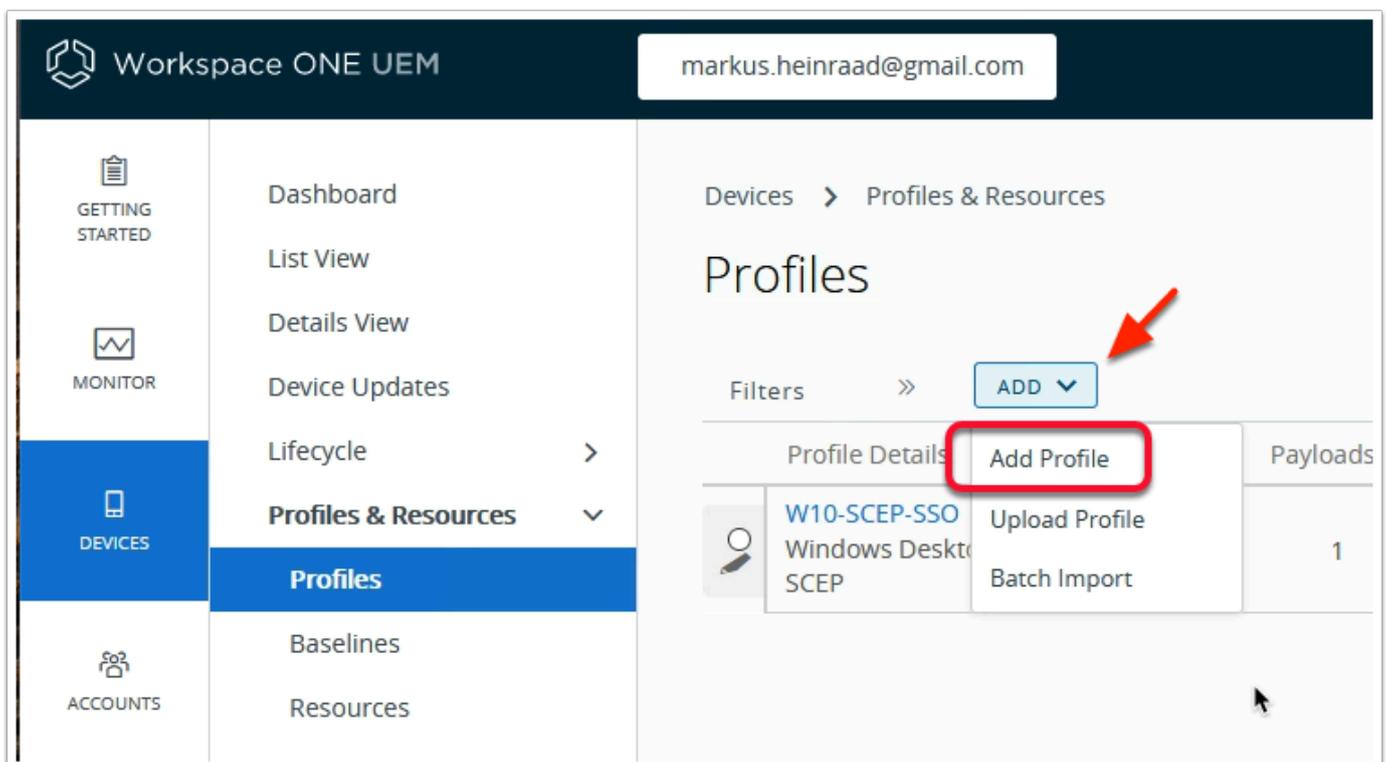
Assignment status	Friendly name	User
Added	Mark VMware7.1 Windows Desktop 10.0.18363 5 e5	Mark

22. On the **VMwareTunnelInstaller_2.1.4.exe - Assignment** window
 - Select **SAVE**
 - On the **VMwareTunnelInstaller_2.1.4.exe - Assignment Devices** window
 - Select **PUBLISH**

Part 5: Creating Per-App VPN Profile for Windows 10

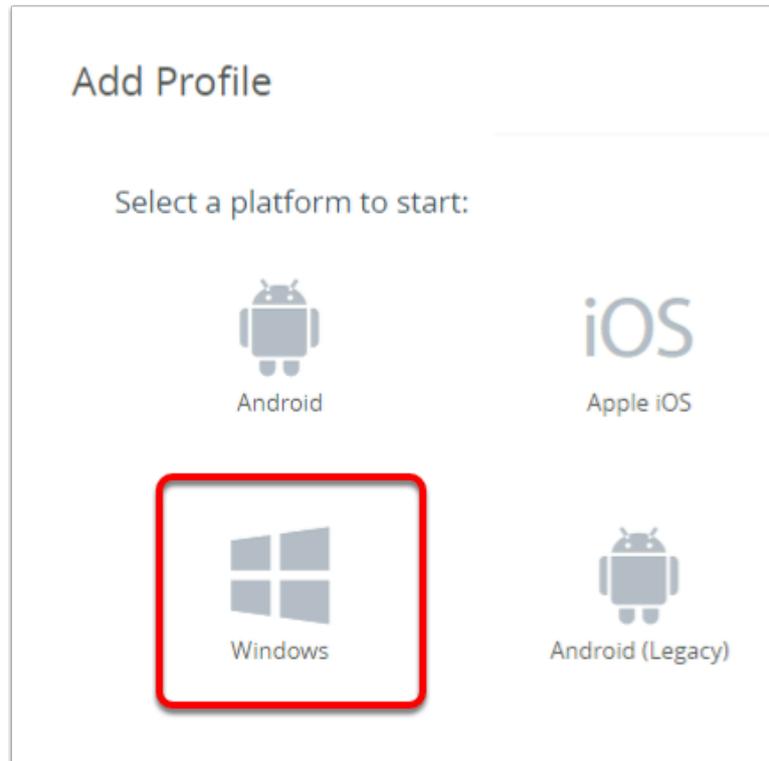


1. In **Workspace ONE UEM** inventory
 - Select **DEVICES** > **Profile & Resources**
 - Select **Profiles**



2. Under **Profiles**

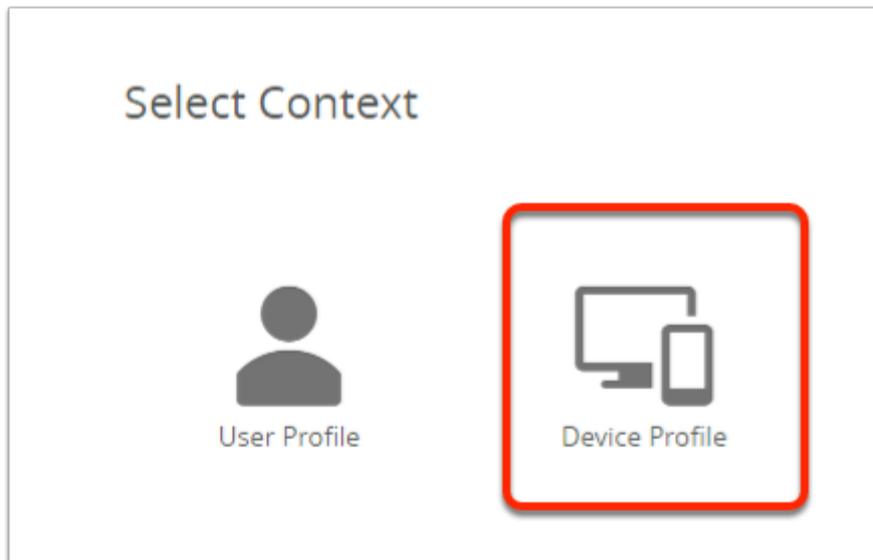
- Select **ADD**
- Select **Add Profile**



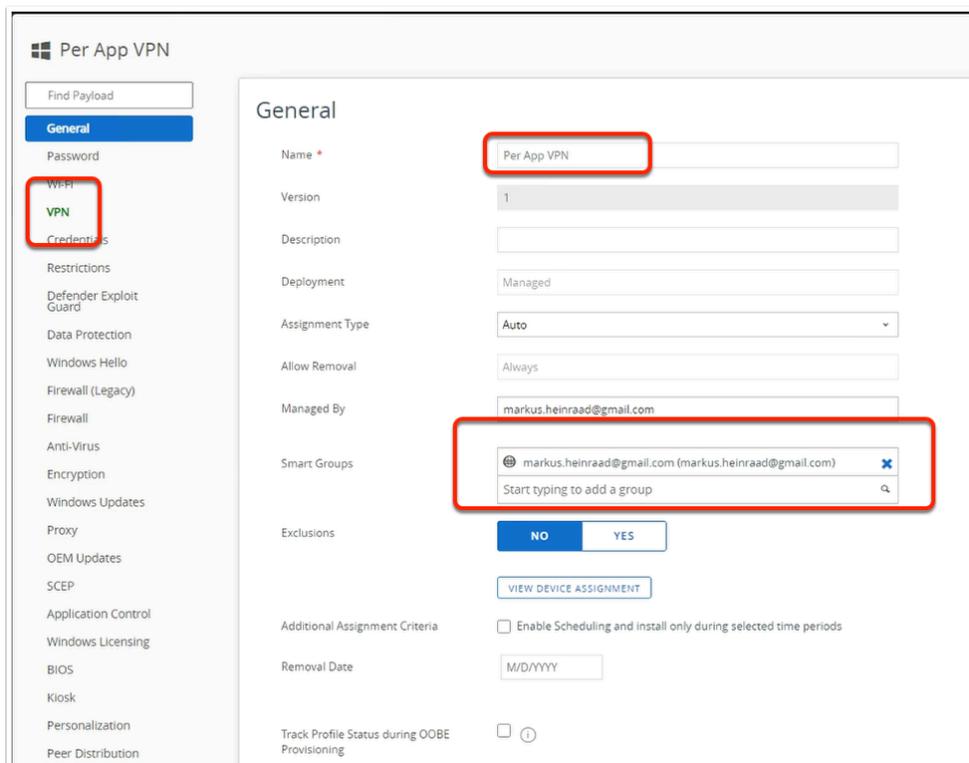
3. In the **Add Profile** window
- Select **Windows**



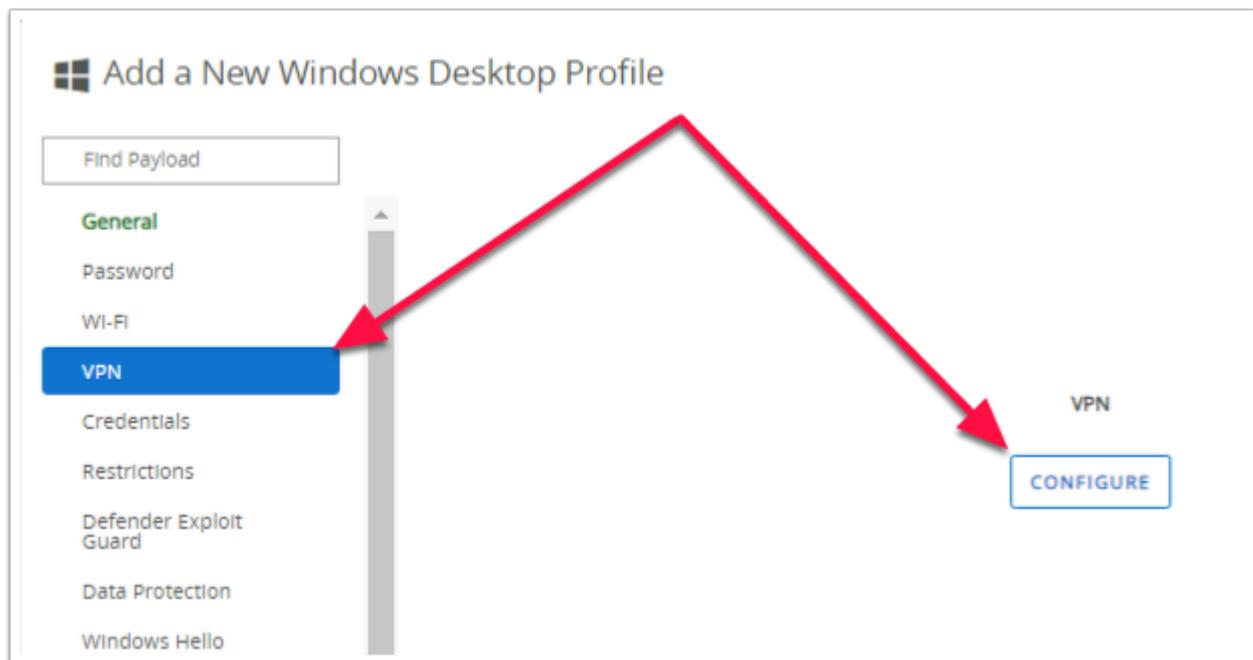
4. In the **Select Device Type** window
- Select **Windows Desktop**



5. In **Select Context** window
- Select **Device Profile**

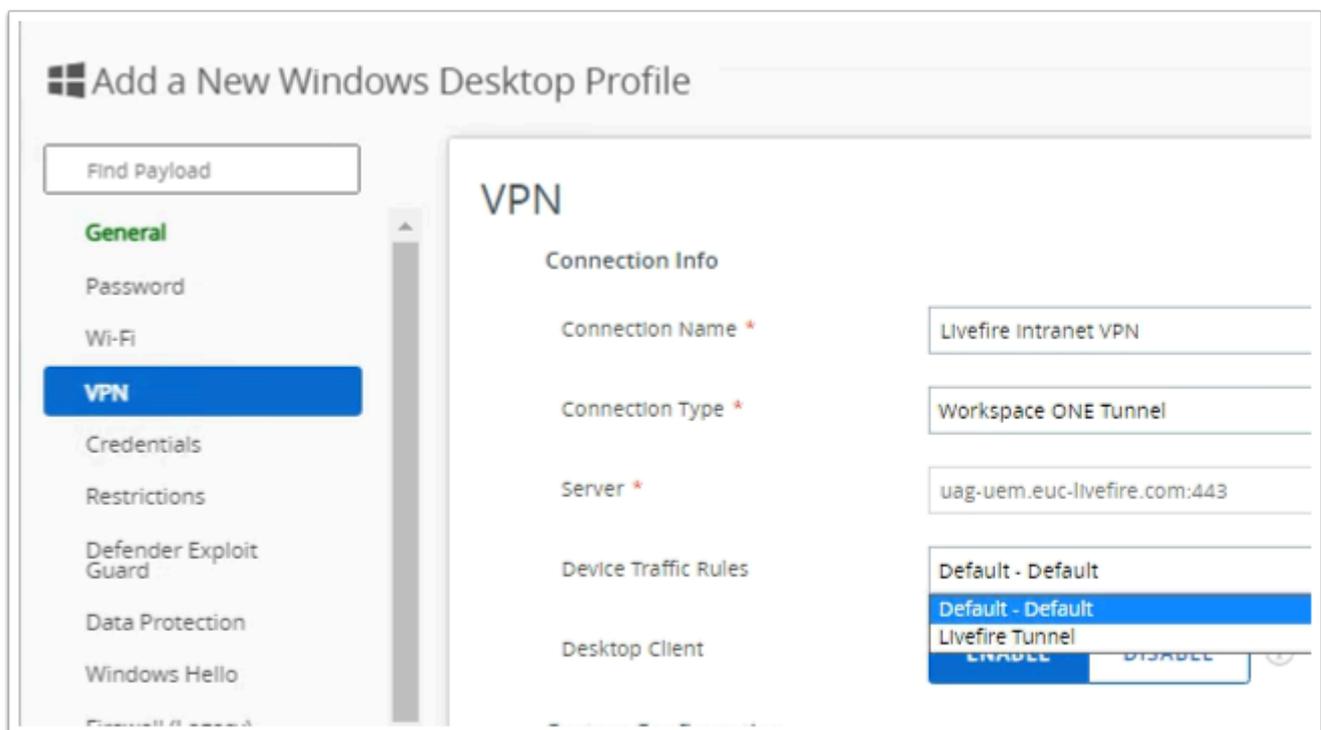


6. In the **Add Profile** window,
- Under **General**, configure the following next to:
 - **Name *** type **Per APP VPN**
 - **Smart Groups** select **your Custom org**



7. In the **Add Profile** window inventory ,

- Select **VPN** ,
- Select **CONFIGURE**



8. In the **VPN** window, configure the following next to:-

- **Connection Name *** type, **Livefire Intranet vPN**
- **Connection Type *** select , **Workspace ONE Tunnel**
- **Device Traffic Rule Sets :** **Livefire Tunnel**
- **Server *** (should already be configured)

- **Desktop Client**, ensure **ENABLE** is selected

Custom Configuration

Custom Configuration XML

```
<CustomConfiguration>
<ServerCertSN>*.euc-livefire.com</ServerCertSN>
</CustomConfiguration>
```

Trusted Network Detection

DNS Resolution via Tunnel Gateway

Domain ⓘ

euc-livefire.com

+ ADD NEW DOMAIN

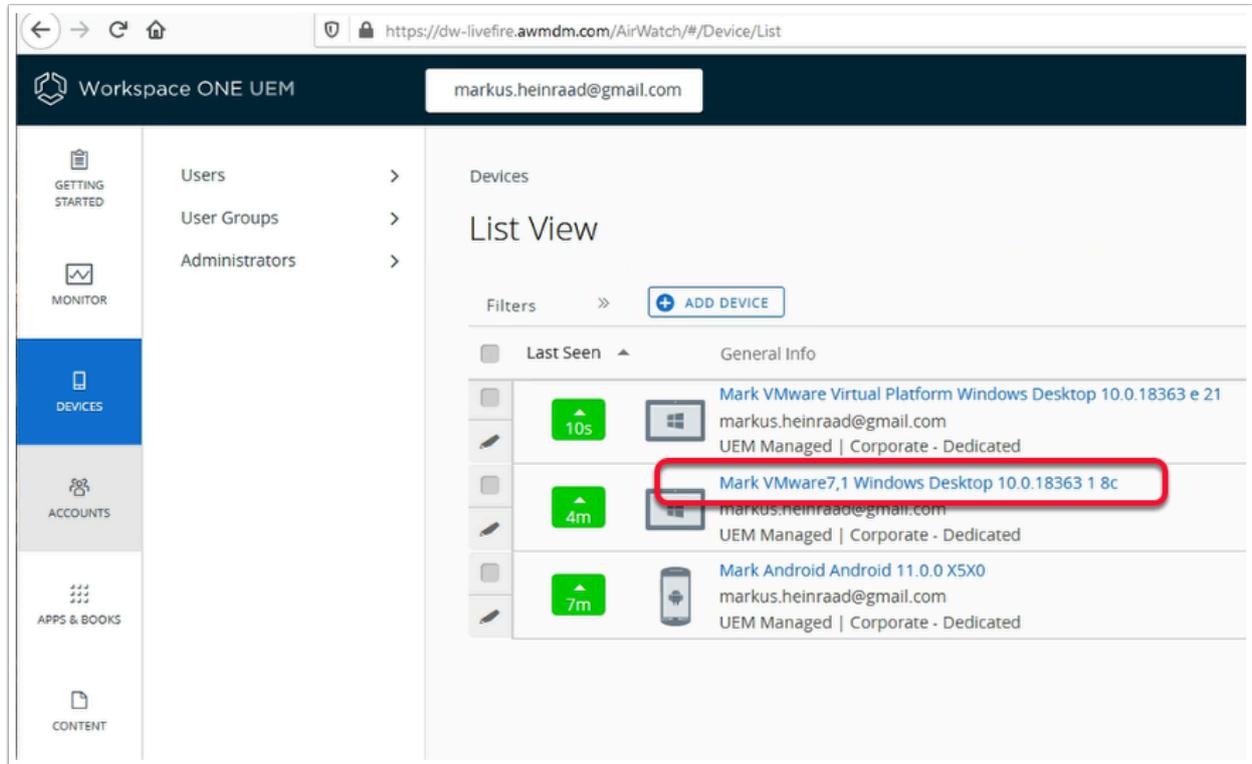
SAVE AND PUBLISH CANCEL

PUBLISH CANCEL

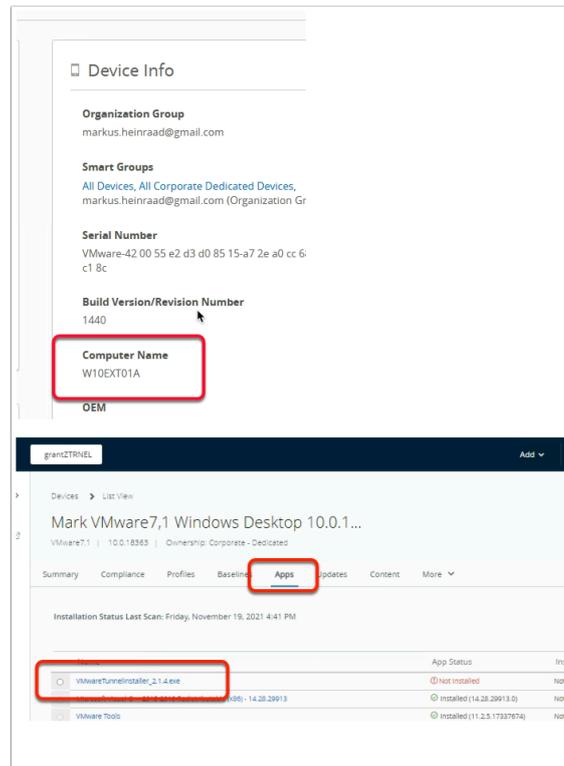
9. In the **VPN** window, next to:

- **Custom Configuration XML**, enter the following
 - **<CustomConfiguration> <ServerCertSN>*.euc-livefire.com</ServerCertSN></CustomConfiguration>**
- Under **Domain**,
 - Select **+ ADD NEW DOMAIN** , enter **euc-livefire.com**
- Select **SAVE AND PUBLISH**
- Select **PUBLISH**

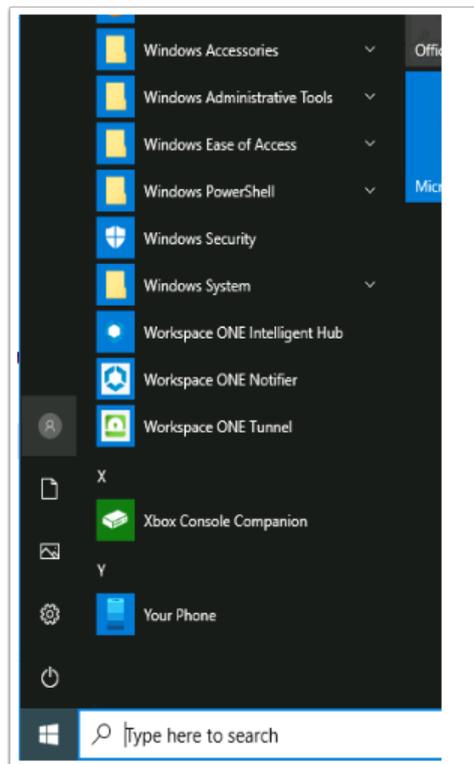
Part 6: Testing Per APP VPN Tunneling with Windows 10



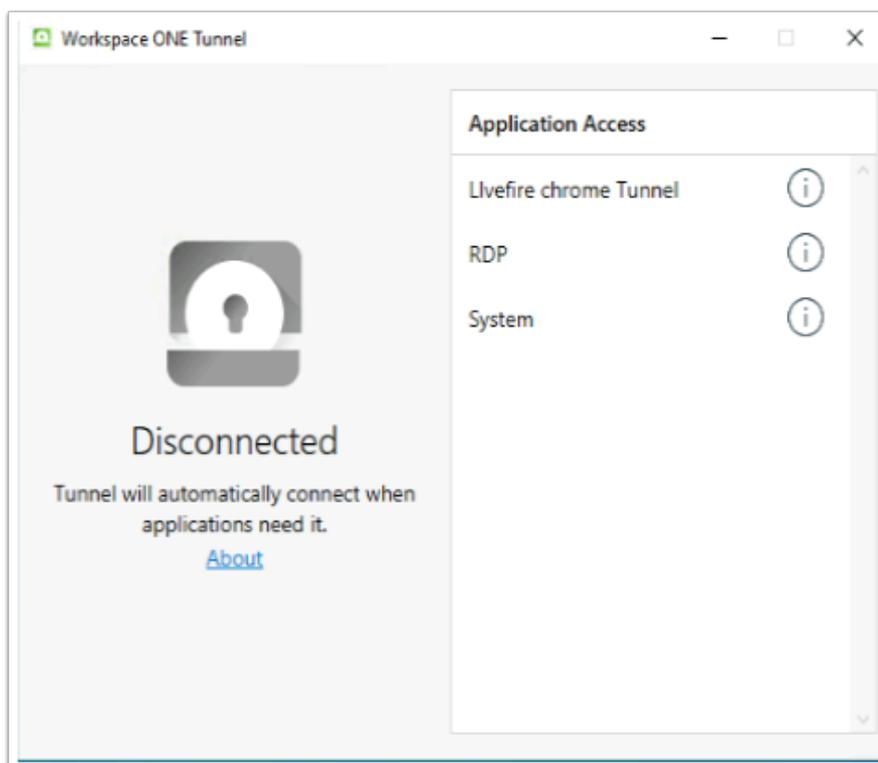
1. In the **Workspace ONE UEM** console
 - Select **DEVICES > List View**
 - Under **List View**,
 - Select Your **Windows Desktop 10.0.1863 (W10EXT01a enrolled device)**



2. In the **Mark VMware7,1. Windows Desktop 10.0.1863** window,
 - To the right under **Device Info**, ensure you are looking at **W10EXT01A**, (if not select the other windows 10 profile)
 - Select **Apps**
 - Notice the VMware Workspace ONE Tunnel **App Status is Installed**
 - **If it is not installed**
 - Select the **radio button** next to **VMwareTunnelInstaller_2.1.4.exe**
 - Select **INSTALL**

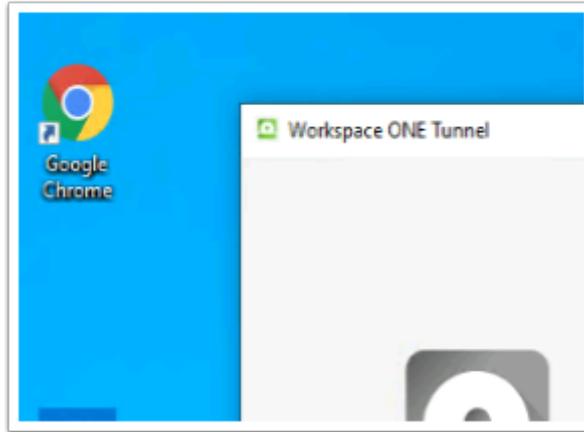


3. Switch to your **W10EXT01a** virtual machine.
 - Select the **Start Menu** and scroll down to **Workspace ONE Tunnel** under **Recently added**
 - **Note**

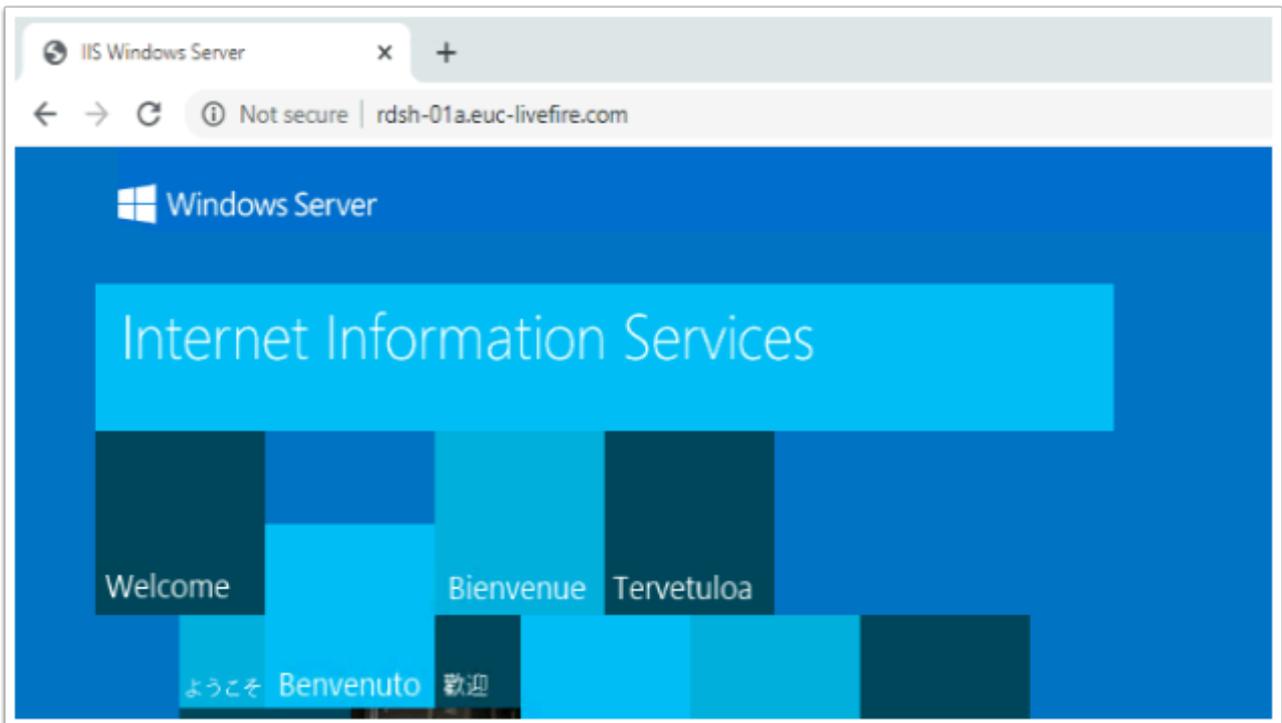


4. In the **Workspace ONE Tunnel** application notice your **Application Access** configurations

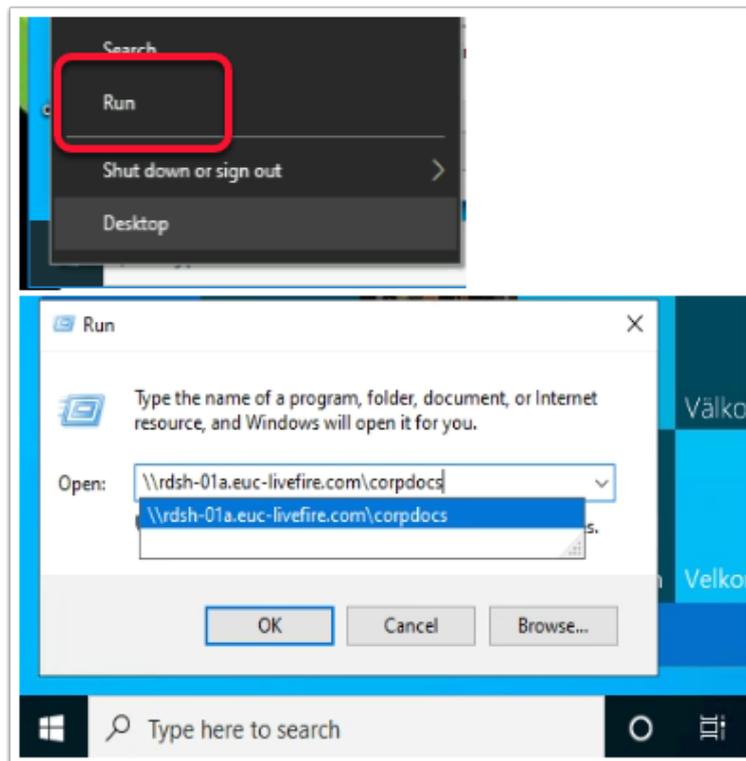
- We will now proceed with a test



5. From the **w10EXT01a** Desktop launch the **Google Chrome** browser

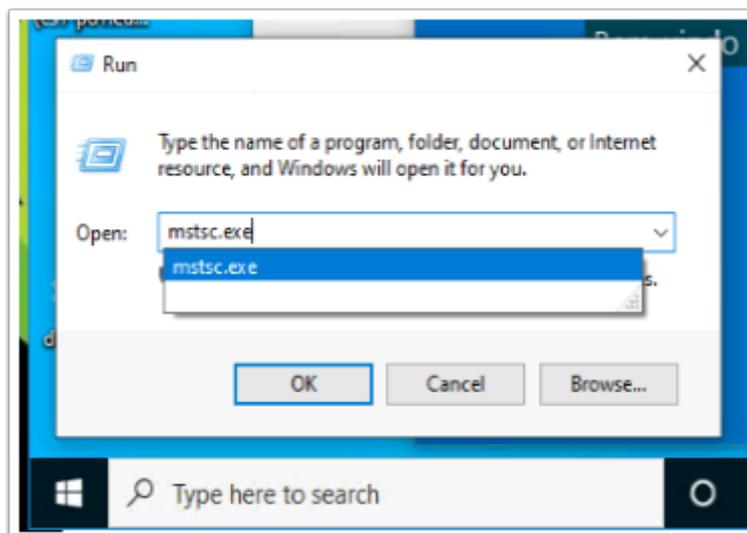


6. In the **Google Chrome Address** bar.
 - Enter <http://rdsh-01a.euc-livefire.com> and select **Enter**
 - You should now see the default IIS web services web page



7. On the W10Ext01a Desktop

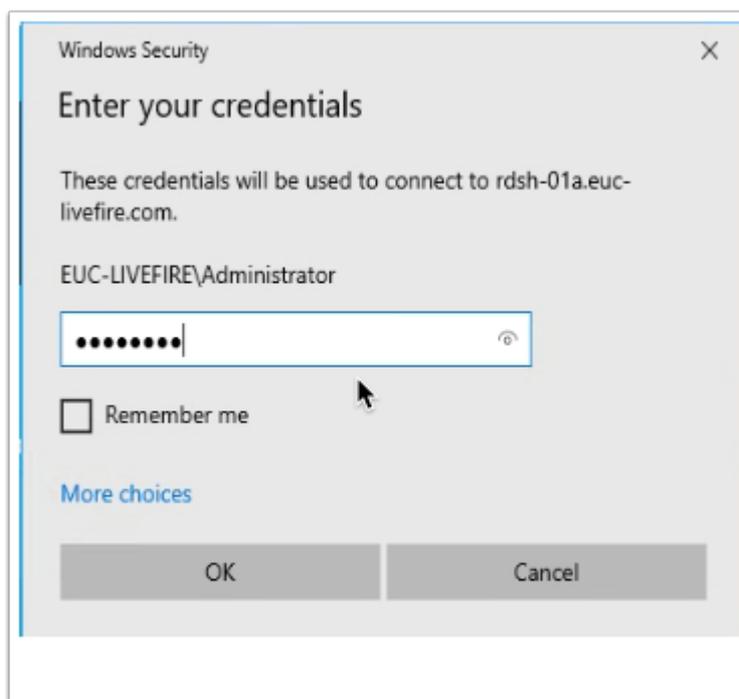
- Select the **Start** button, right-click, select **Run**,
- Next to **Open:** type **\\rdsh-01a.euc-livefire.com\corpdocs**
- Select **OK**
- Notice that you are now leveraging the SMB based functionality in **VMware Workspace ONE Tunnel**. This too might considered in-secure, this has now been secured using **VMware Workspace ONE Tunnel**



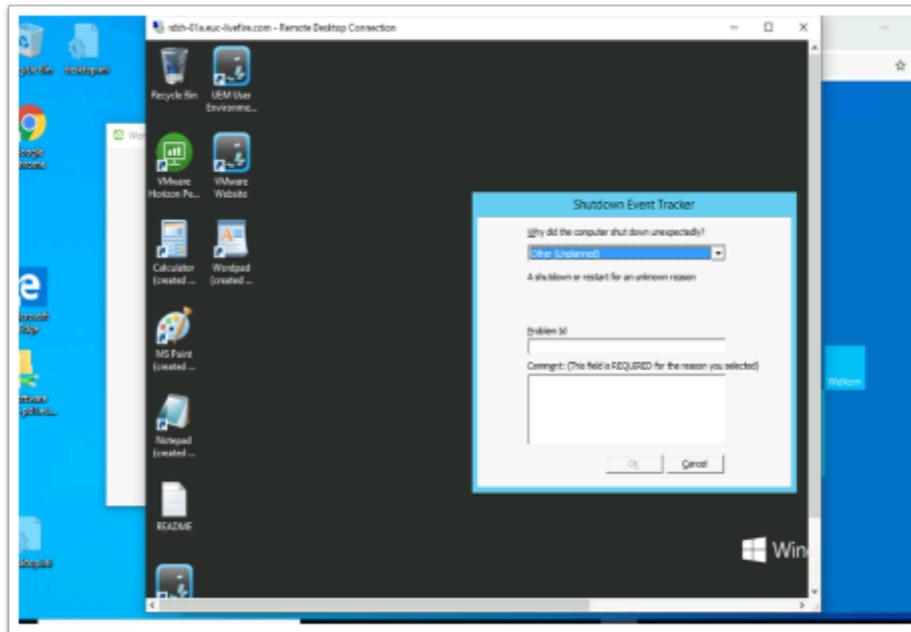
8. In the **Run** window next to **Open:** delete the text from **step 7**, type **mstsc.exe** and select **OK**



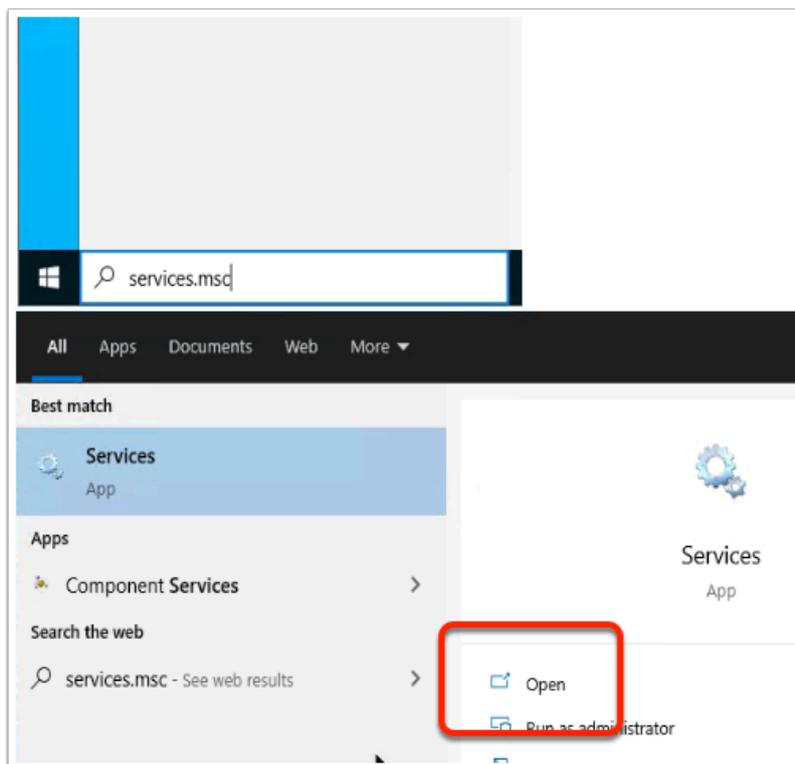
9. In the **Remote Desktop Connection** window, next to
- **Computer:** type **rdsh-01a.euc-livefire.com**
 - **User name:** type **EUC-livefire\administrator**
 - Select **Connect**



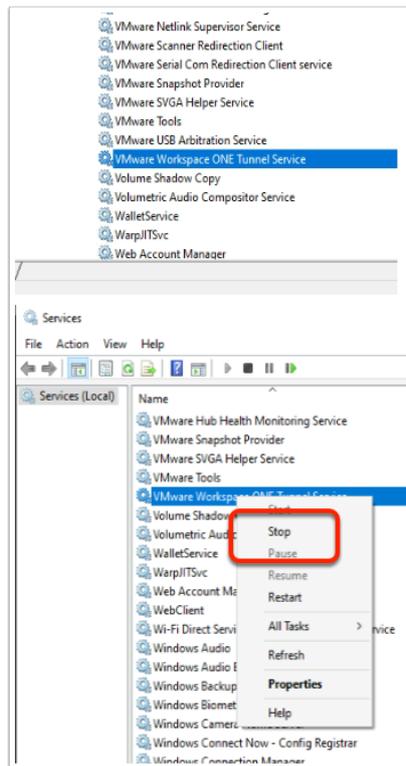
10. In the **Enter your credentials** enter **VMware1!** as the password
- Select **OK**



11. Notice you have now have a secure tunnel with RDP.

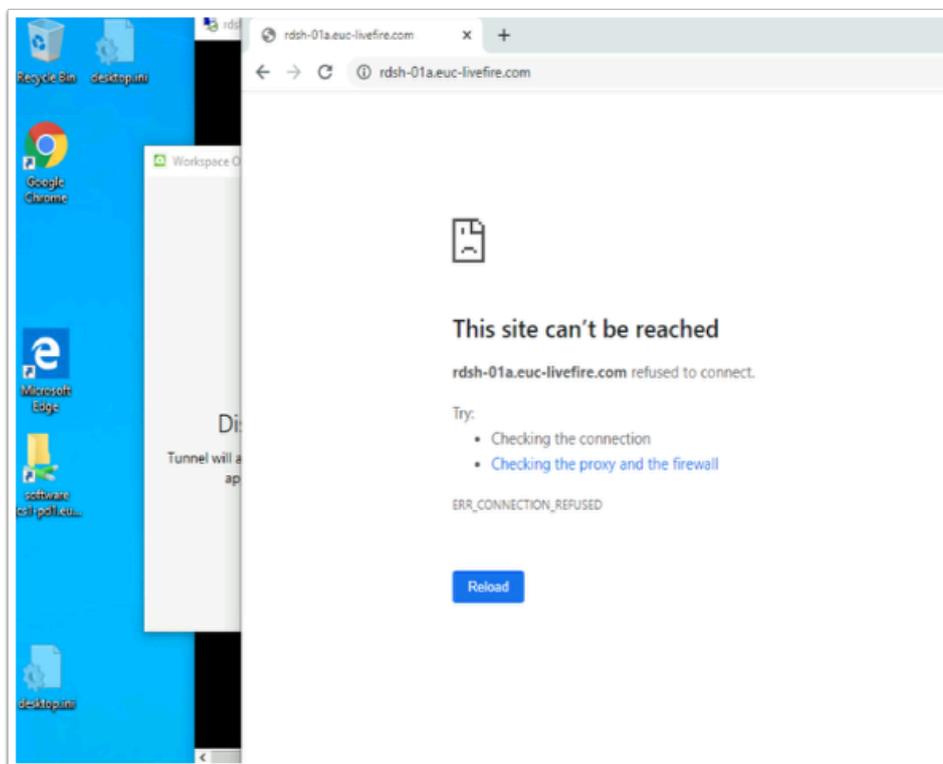


12. On your **W10EXT01a** Desktop,
- In the **Type here to Search** area enter **services.msc**
 - Under the **Services** shortcut, select **Open**
 - Select **Yes**



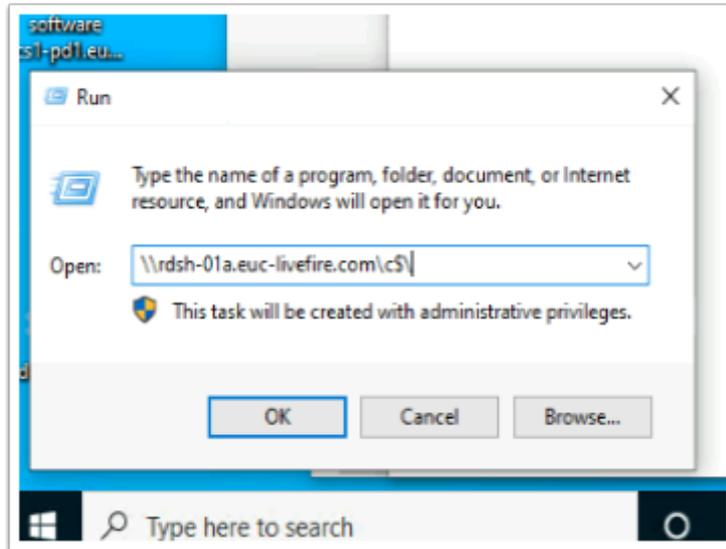
13. In the **Services MMC**

1. **Scroll** down until you find the **VMware Workspace ONE Tunnel Service** ,
2. **select > right click** and select **Stop**

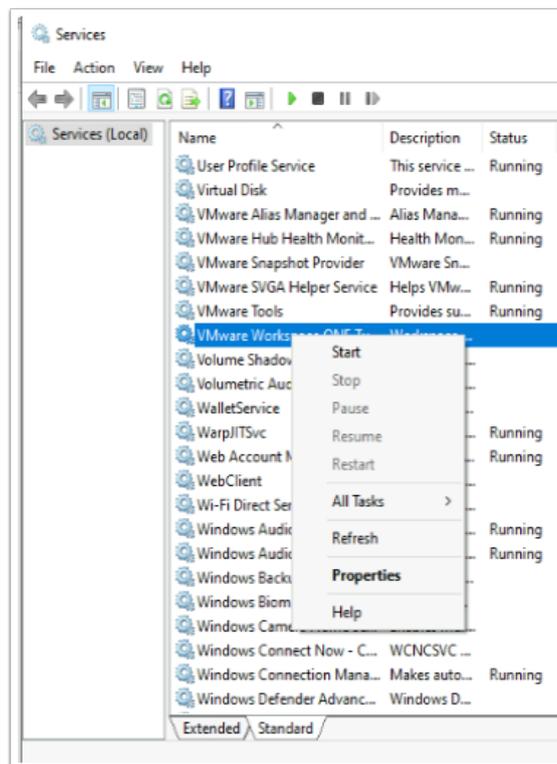


14. Notice your RDP connection just got disconnected!

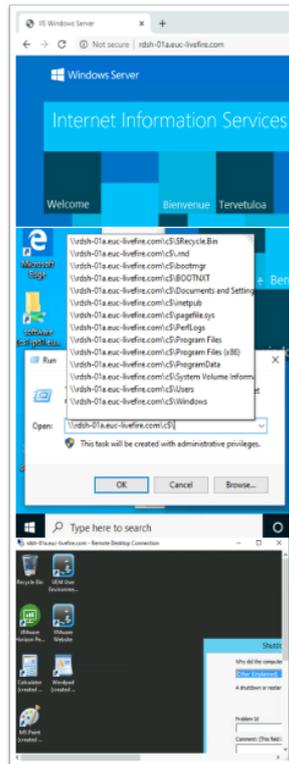
- **Refresh** your **Chrome browser** and notice you are unable to reach your website on the **RDSH-01a.euc-livewire.com** server.



15. In the **Run** window, next to **Open:** type **\\rdsh-01a.euc-livewire.com\c\$**
 - Notice SMB is no longer working to the RDSH-01a server



16. Switch back to **Services** and select **Start** against the **VMware Workspace ONE Tunnel service**



17. On the **W10EXT01a** desktop, perform the following
- **Refresh** your chrome browser
 - **Retest** SMB to RDSH-01a.euc-livewire.com
 - **Retest** RDP to RDSH-01a.euc-livewire.com

This Concludes this section in our Series of labs Securing the Transport as one of the pillars in Zero-Trust with Windows 10

Acknowledgements

We would like to thank the VMware Tech Marketing Team for the use of their guidance in the creation this content

We would like to thank Mark Benson from the EUC CTO Office for his support and content

If you were interested in learning how to secure other Platforms using the VMware Workspace ONE Tunnel, visit the following VMware TechZone page for further step-by-step Guidance

<https://techzone.vmware.com/deploying-vmware-workspace-one-tunnel-vmware-workspace-one-operational-tutorial#1214601>

About the author Reinhart Nel

<https://www.livewire.solutions/meet-the-team/reinhartnel/>

For any questions related to this session, email Reinhart at RACE-Livewire-EUC@vmware.com>