

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.

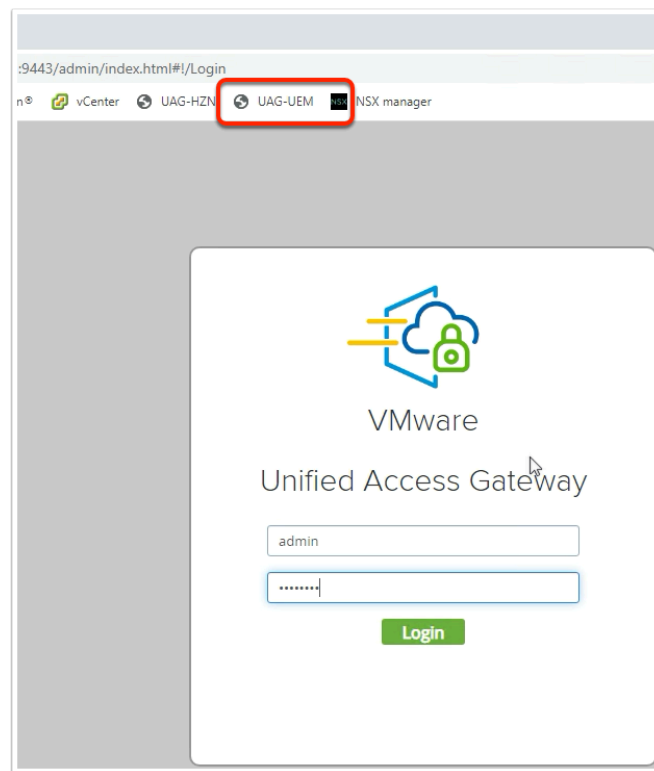
Prerequisites

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

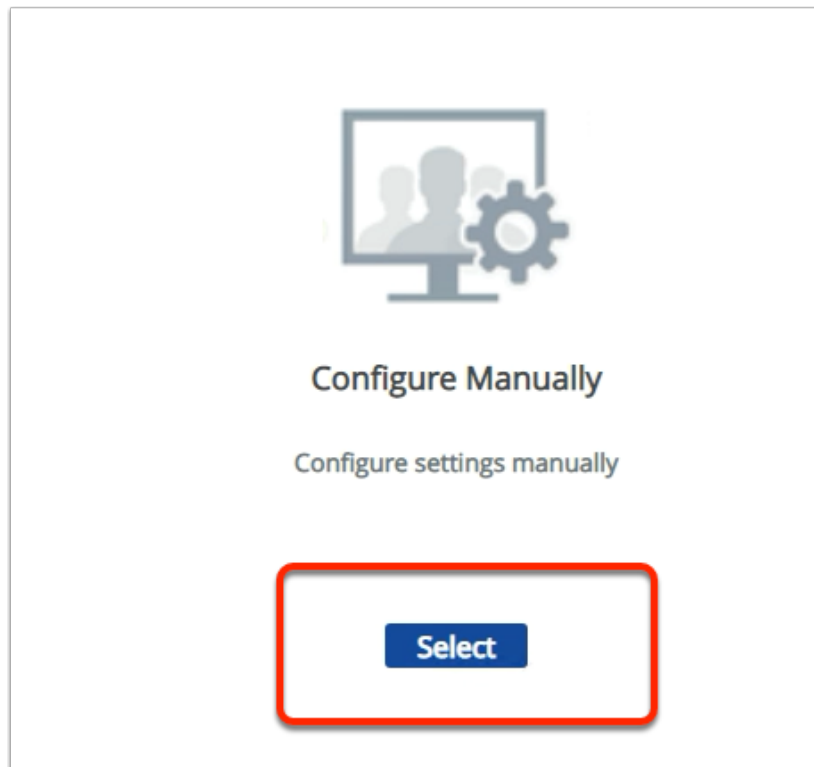
- VMware Unified Access Gateway with VMware Tunnel edge service configured
 - UAG has been deployed. We will configure the Edge service
 - Your UAG is on representative on-premises infrastructure and is UAG-UEM.euc-liveware.com.
 - It is on an NSX-T managed 172.16.20.x subnet. This subnet is representative 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

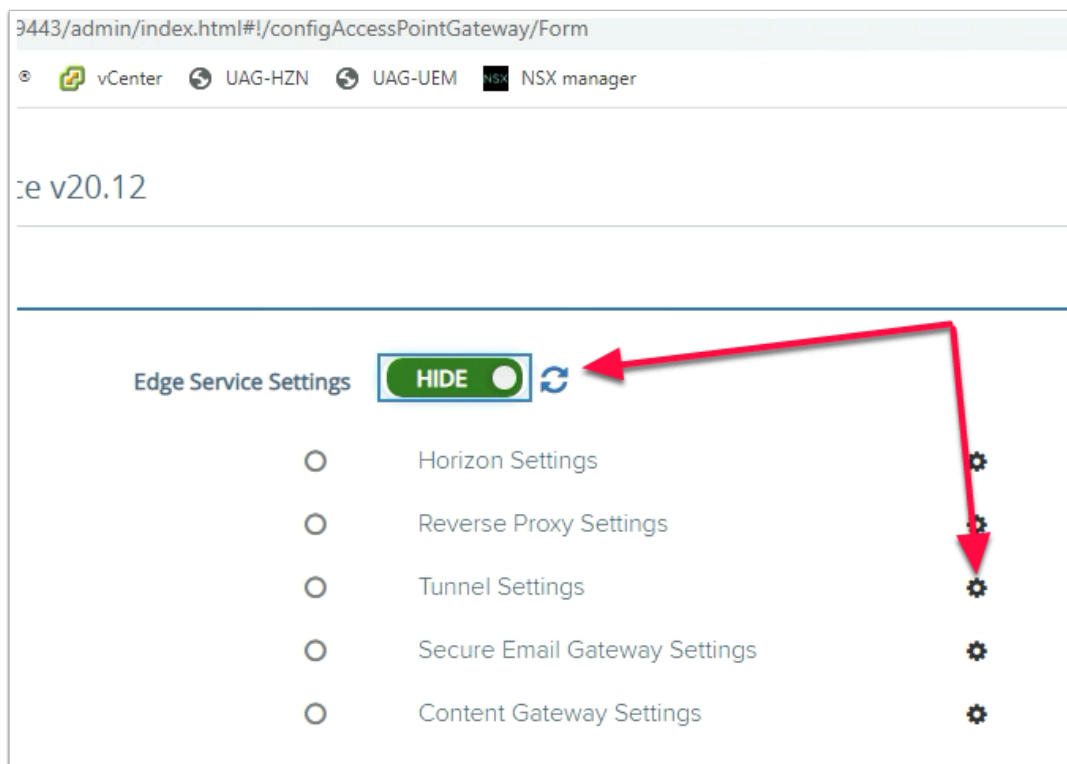


1. On your **ControlCenter** server, open your **Chrome Browser** and select the **UAG-UEM** shortcut.
 - In the **UAG Admin Console** Login
 - Enter **admin** for **username**
 - Enter **VMware1!** for **password**
 - Select **Login**



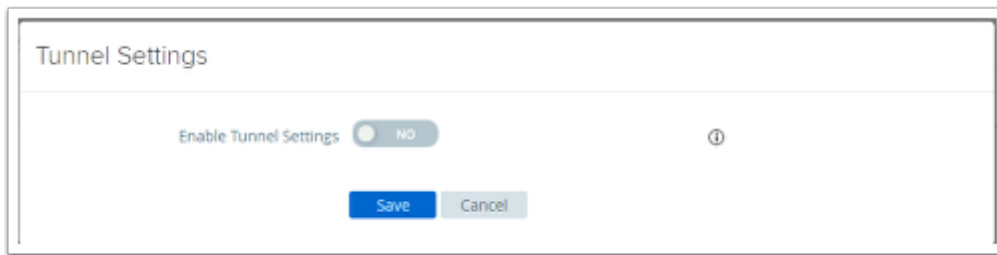
2. Under **Configure Manually**

- Click the **Select** button



3. Next to **Edge Service Settings**

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



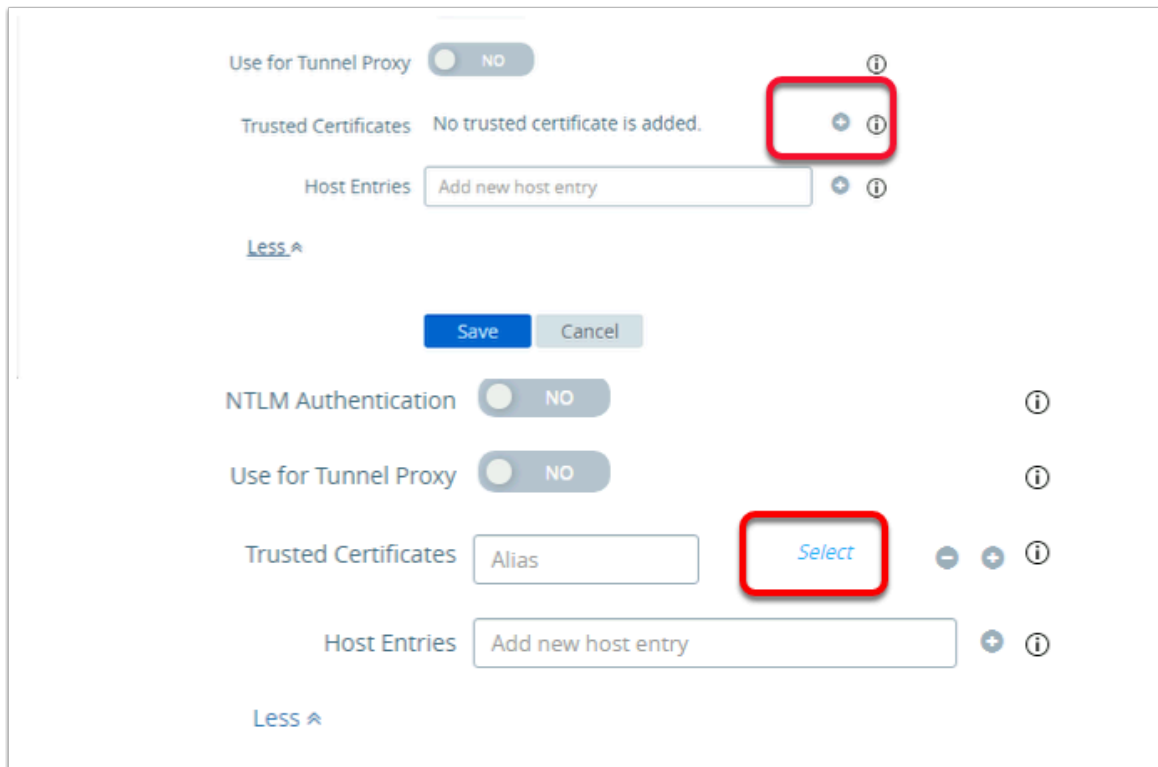
4. In the **Tunnel Settings** window, next to **Enable Tunnel Settings**, change the setting from **NO** to **YES**

 A screenshot of the 'Tunnel Settings' window with the 'Enable or disable Tunnel Settings' toggle switched to 'YES' (green). Below the toggle are five input fields, each with an information icon (i) to its right:

- API Server URL *: https://cn-livefire.awmdm.com
- API Server Username *: grantflenderman@gmail.com
- API Server Password *: (masked with dots)
- Organization Group ID *: grantZTRN444
- Tunnel Server Hostname *: uag-uem.euc-livefire.com

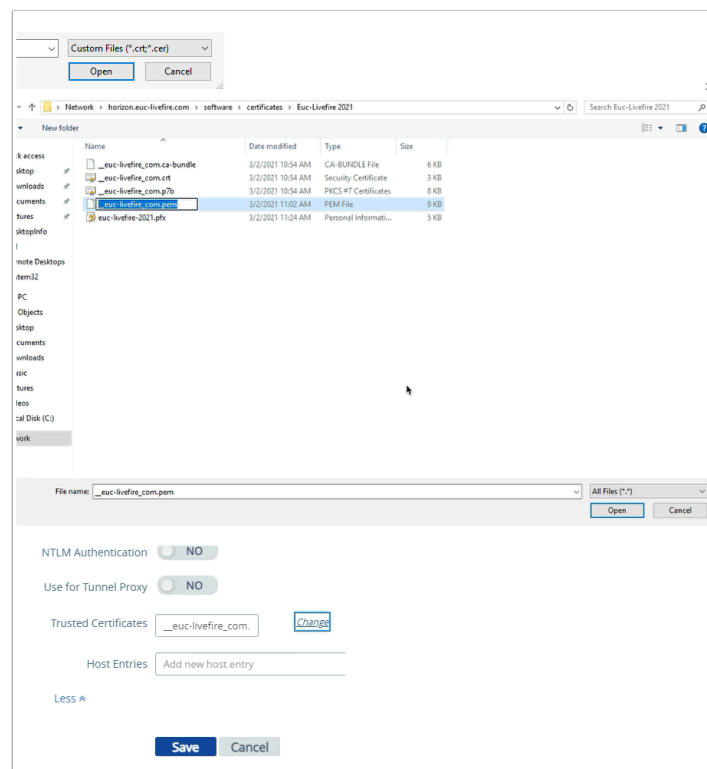
 At the bottom left, there is a 'More' button with a dropdown arrow. A red arrow points to this button. At the bottom right, there are 'Save' and 'Cancel' buttons.

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

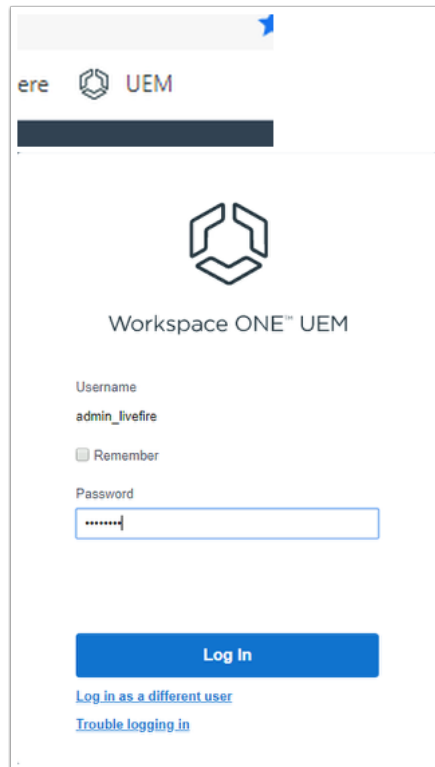
- To the right of **Trusted Certificates**, click the **+** icon
- Click the **Select** button



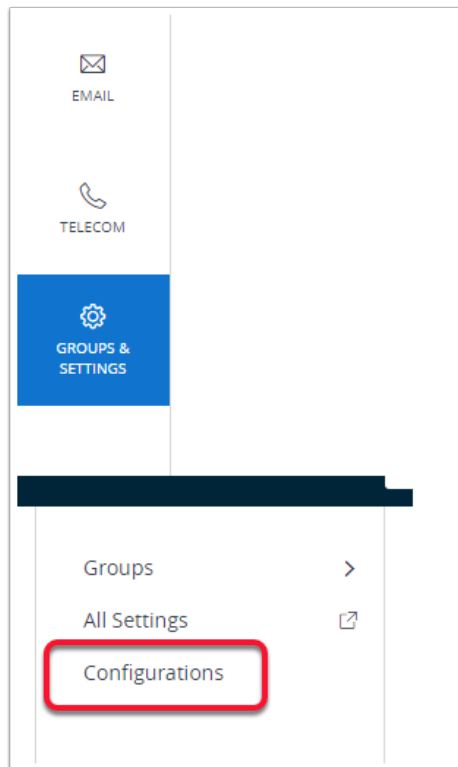
7. In the **address bar**,

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

Part 2: - Configuring the VMware Tunnel Edge Service

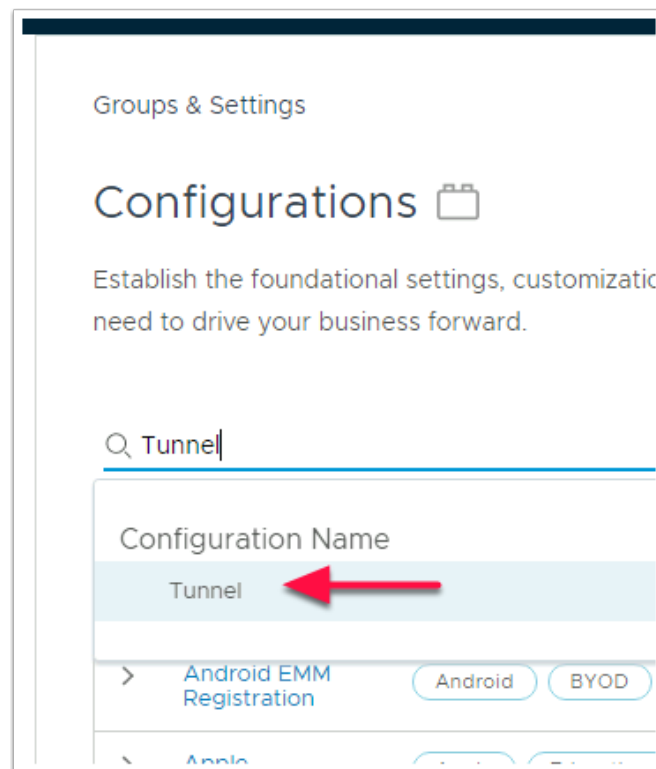


1. On your **ControlCenter** server,
 - Open your **Chrome** browser
 - In the address bar type <https://cn-liveware.awmdm.com> .
 - Under **Username** enter your custom **UEM username**
 - Select **Next**
 - Under **Password** enter **VMware1!** and select **Log In**



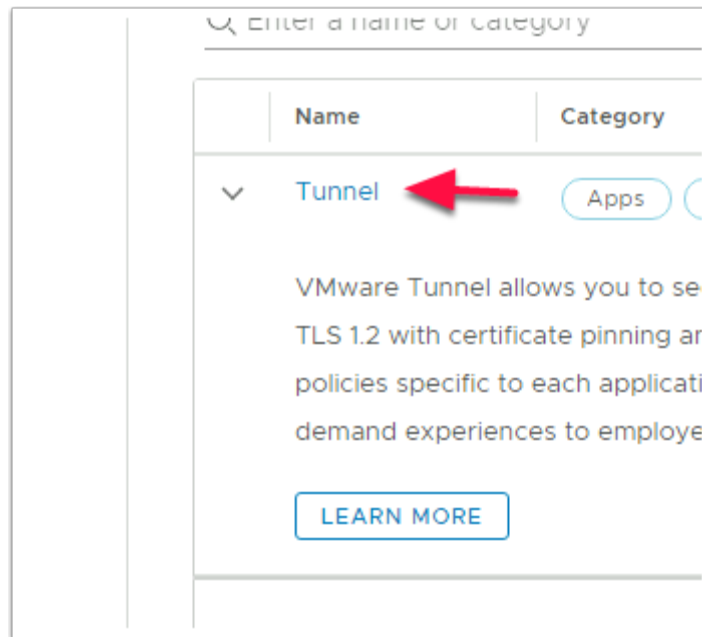
2. In the **Workspace ONE UEM** Console:

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



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

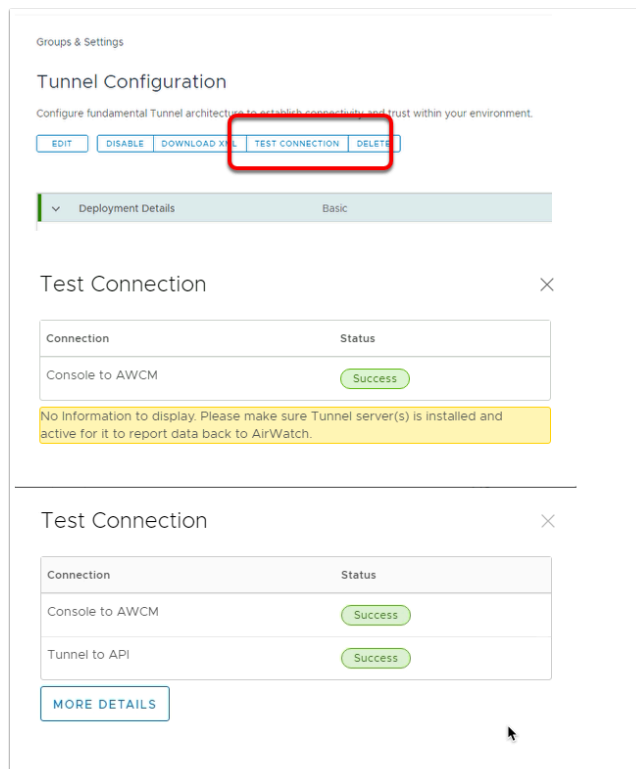
- When **Tunnel** shows under **Configuration Name** select **Tunnel**



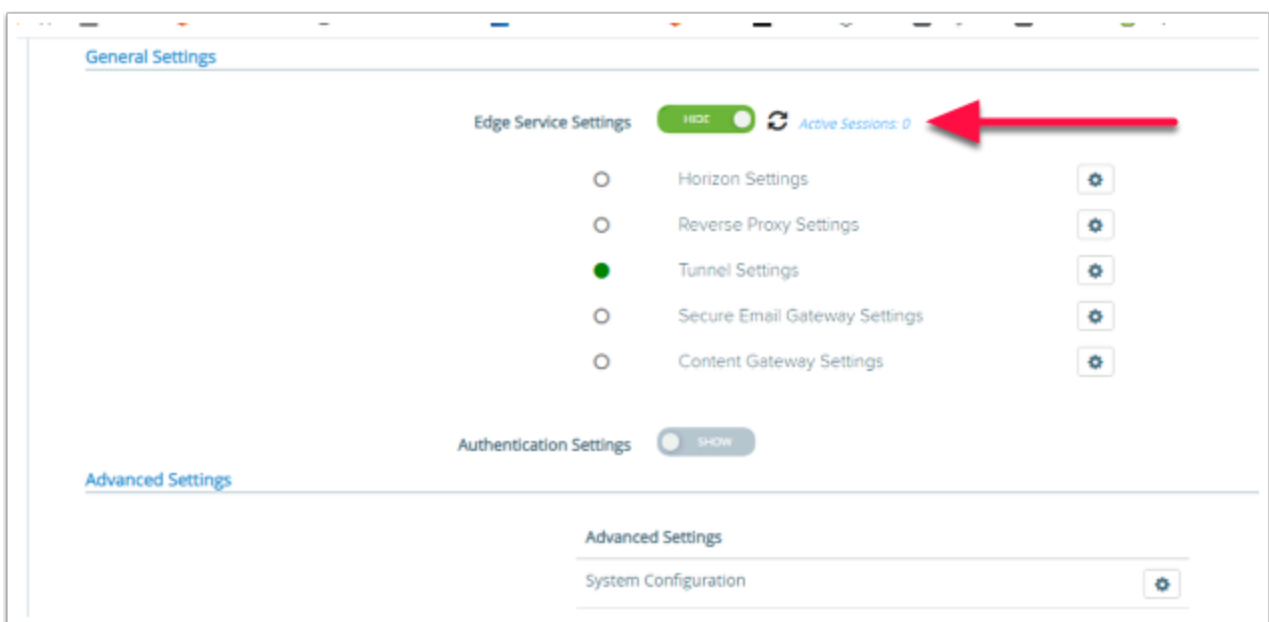
4. Under **Name** select **Tunnel**

The screenshot shows the "New Tunnel Configuration" form. At the top, there is a header "Groups & Settings" and a title "New Tunnel Configuration". Below the title is a subtitle "Configure fundamental Tunnel architecture to establish connectivity and trust within your environment." and two buttons: "SAVE" and "CANCEL". On the right side, there is a link "Download Installer". The form is divided into two tabs: "Deployment Details" and "Basic". The "Basic" tab is selected. Under the "Basic" tab, there are three fields: "Deployment Type" with radio buttons for "Basic" (selected) and "Cascade", "Hostname" with the value "uag-uem.euc-livefire.com", and "Port" with the value "443". Below these fields, there is a table with four rows: "Server Authentication" (AirWatch), "Client Authentication" (AirWatch), "Networking" (Disabled), and "Logging" (Disabled).

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



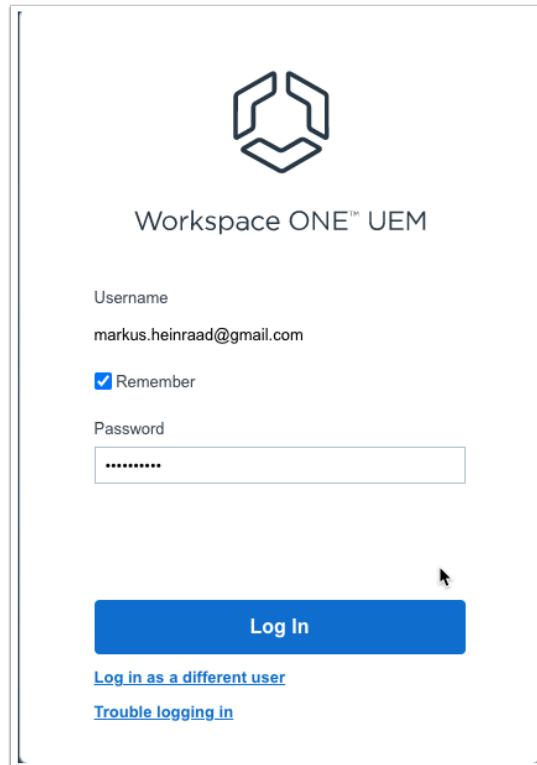
6. In the **Tunnel Configuration** page select **TEST CONNECTION**,
 - You should have two responses
 - **Console to AWCN**
 - **Tunnel to API**
 - **Status** should read **Success** on both, but if you see one, carry on with your labs, it can take a while for this to show



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

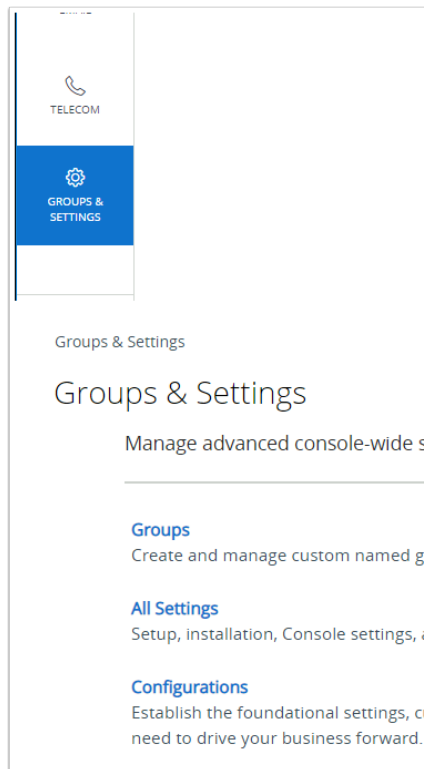
Password

[Log In](#)

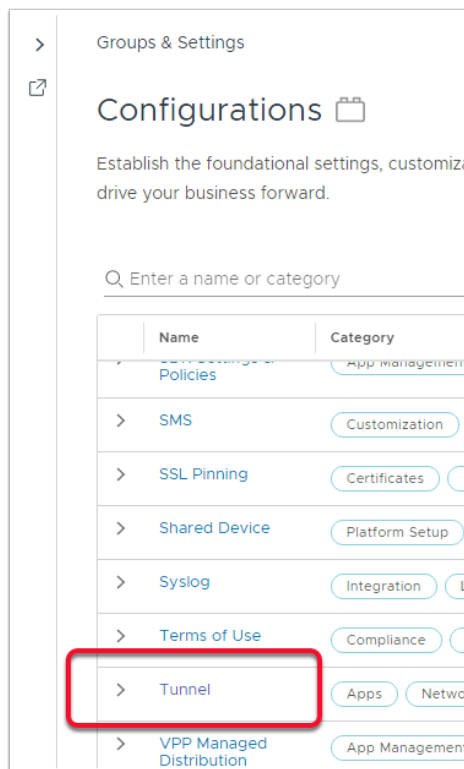
[Log in as a different user](#)

[Trouble logging in](#)

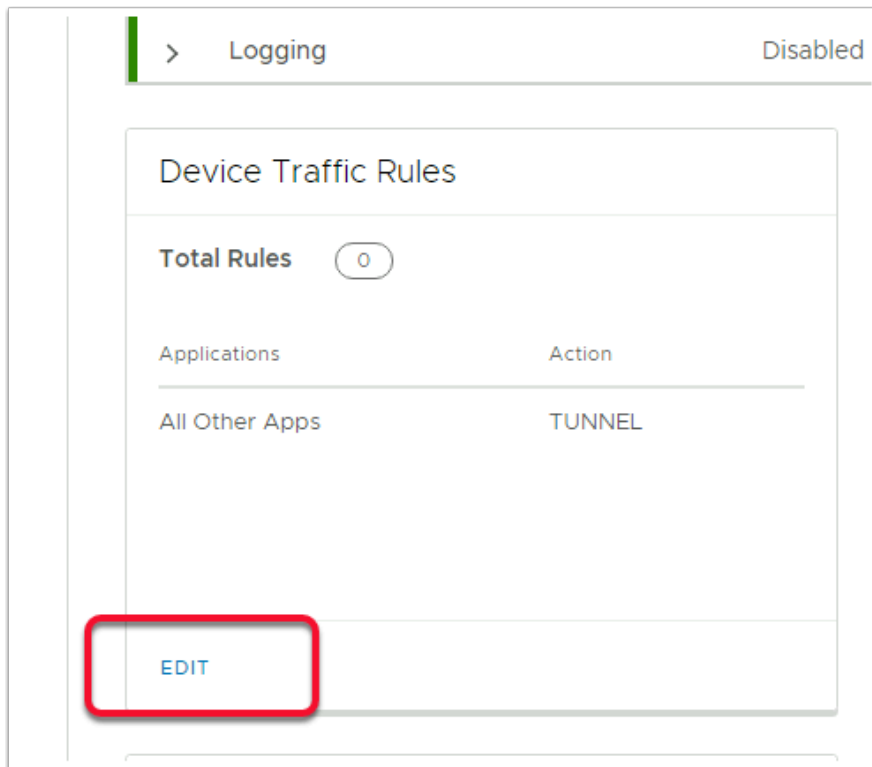
1. If necessary log in to your **Workspace ONE UEM** console
 - Log in using your custom username **custom username** and password **custom password**
 - Select **Log In**



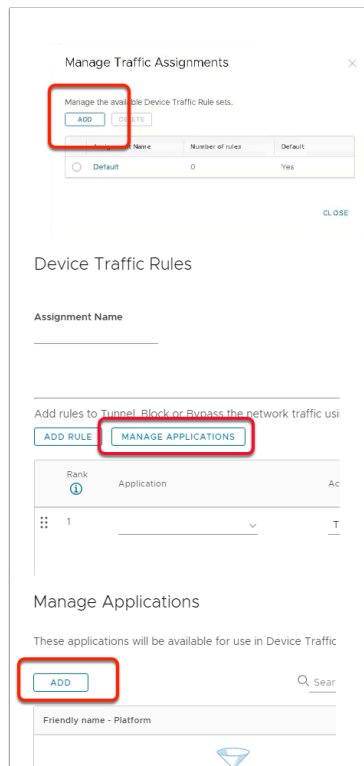
2. In the **UEM Console**,
 - Select **GROUPS & SETTINGS**,
 - Select **Configurations**



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



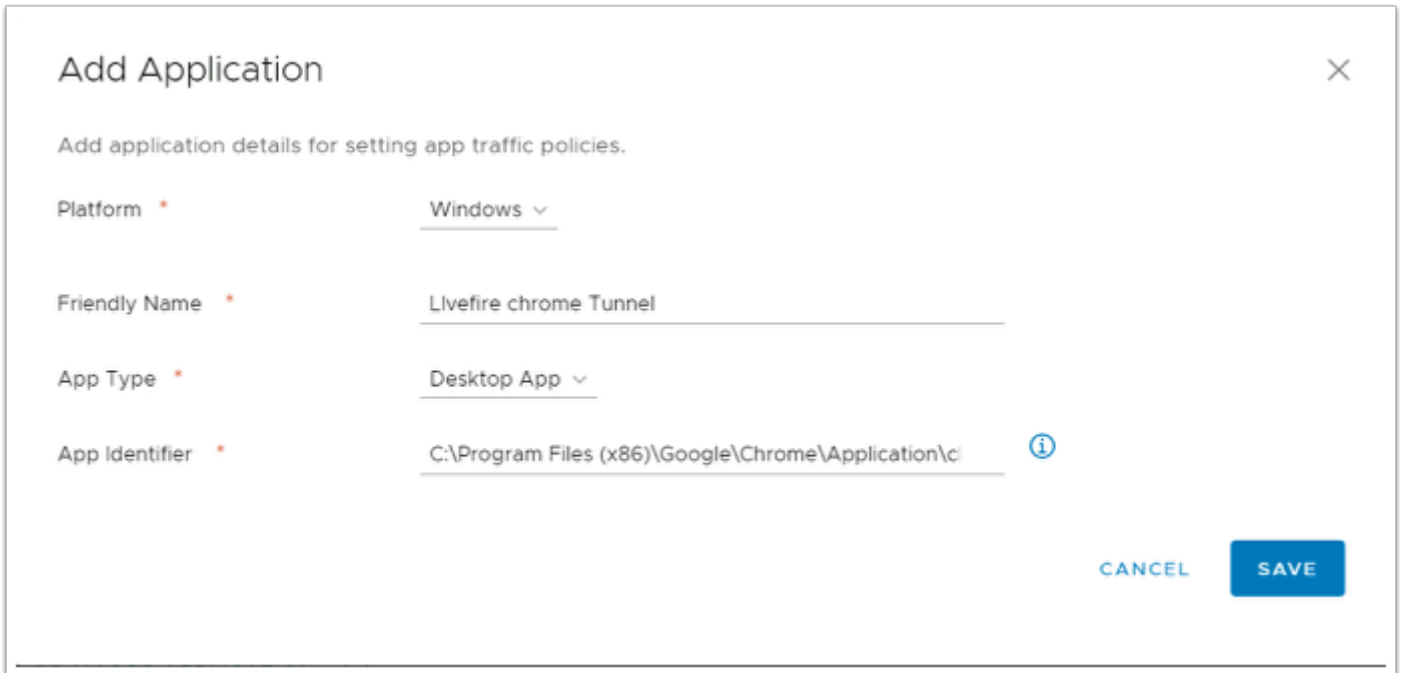
4. In the **Tunnel Configuration** window under **Device Traffic Rules** select **EDIT**



5. Under **Manage Traffic Assignments**

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

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

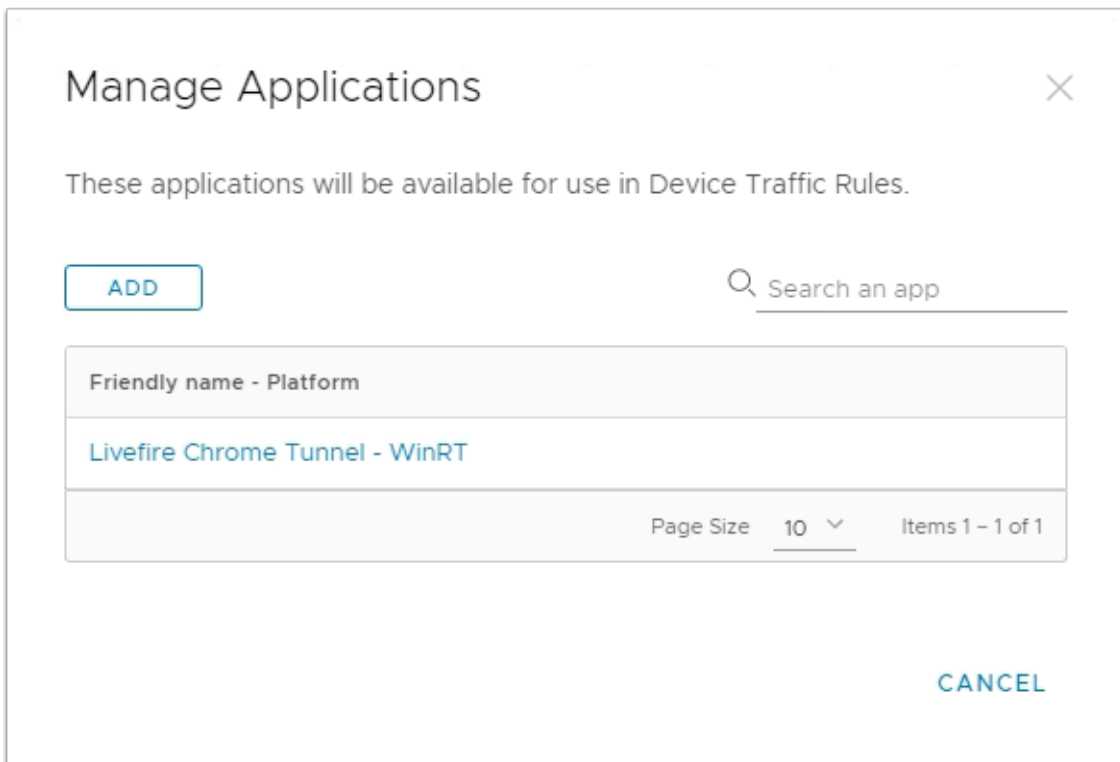


The 'Add Application' dialog box is shown with a close button (X) in the top right corner. Below the title bar, there is a subtitle: 'Add application details for setting app traffic policies.' The form contains four fields, each with a red asterisk indicating it is required:

- Platform ***: A dropdown menu with 'Windows' selected.
- Friendly Name ***: A text input field containing 'Livefire chrome Tunnel'.
- App Type ***: A dropdown menu with 'Desktop App' selected.
- App Identifier ***: A text input field containing 'C:\Program Files (x86)\Google\Chrome\Application\chrome.exe'. To the right of this field is a blue information icon (i).

At the bottom right of the dialog, there are two buttons: 'CANCEL' and 'SAVE'.

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**



The 'Manage Applications' dialog box is shown with a close button (X) in the top right corner. Below the title bar, there is a subtitle: 'These applications will be available for use in Device Traffic Rules.' The dialog contains an 'ADD' button on the left and a search bar on the right with a magnifying glass icon and the text 'Search an app'.

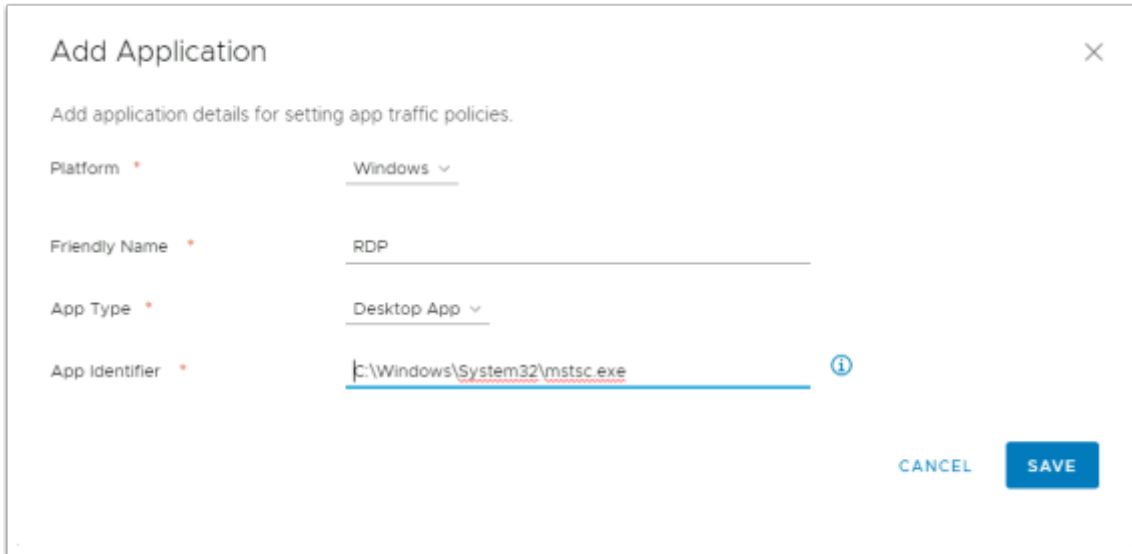
Below the search bar is a table with the following content:

Friendly name - Platform
Livefire Chrome Tunnel - WinRT

At the bottom right of the table, there is a 'Page Size' dropdown menu set to '10' and a text label 'Items 1 - 1 of 1'. At the bottom right of the dialog, there is a 'CANCEL' button.

7. In the **Manage Applications** window

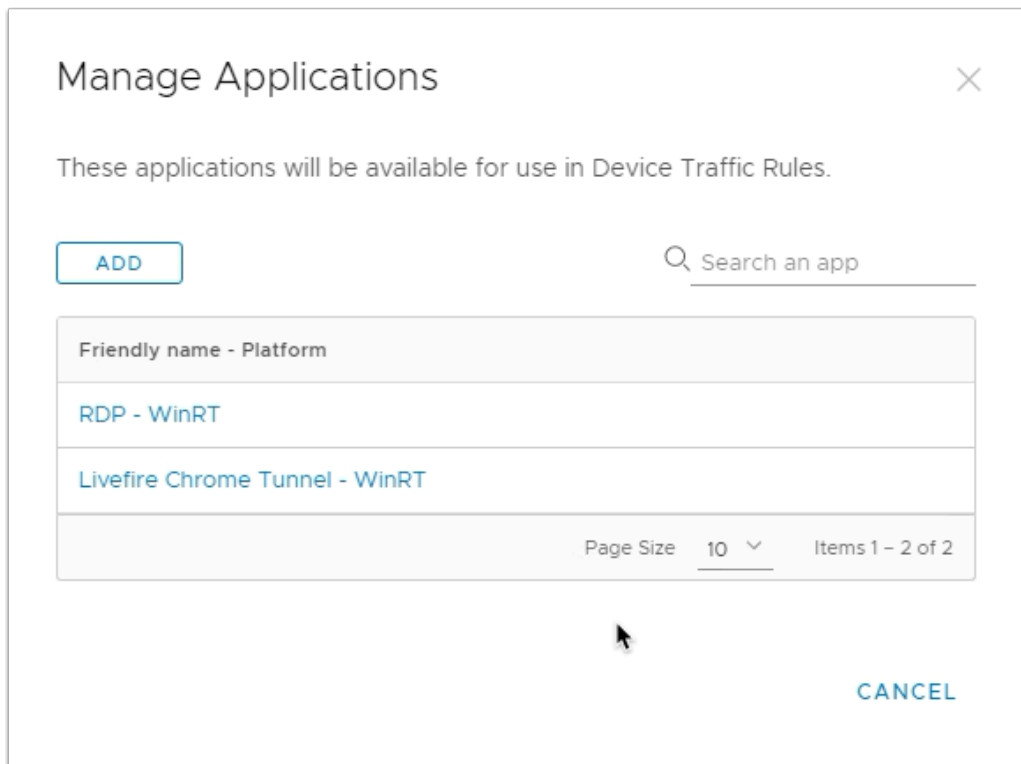
- Select **ADD**



The 'Add Application' dialog box is shown. It has a title bar with a close button (X). Below the title bar, it says 'Add application details for setting app traffic policies.' There are four fields: 'Platform' with a dropdown menu set to 'Windows', 'Friendly Name' with a text input field containing 'RDP', 'App Type' with a dropdown menu set to 'Desktop App', and 'App Identifier' with a text input field containing 'c:\Windows\System32\mstsc.exe'. There is an information icon (i) to the right of the 'App Identifier' field. At the bottom right, there are two buttons: 'CANCEL' and 'SAVE'.

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**



The 'Manage Applications' window is shown. It has a title bar with a close button (X). Below the title bar, it says 'These applications will be available for use in Device Traffic Rules.' There is an 'ADD' button on the left and a search bar on the right with the placeholder text 'Search an app'. Below the search bar, there is a table with two columns: 'Friendly name' and 'Platform'. The table contains two rows: 'RDP - WinRT' and 'Livewire Chrome Tunnel - WinRT'. At the bottom right, there is a 'CANCEL' button. The table has a footer with 'Page Size 10' and 'Items 1 - 2 of 2'.

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 ▾

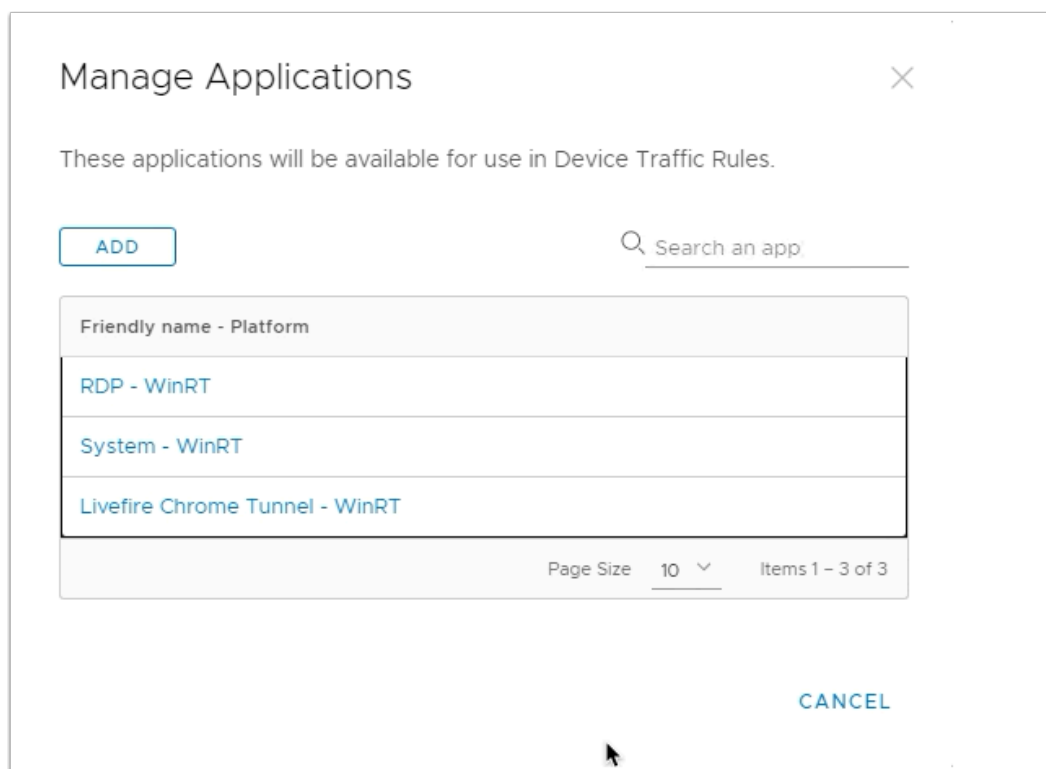
App Identifier * System ⓘ

CANCEL SAVE

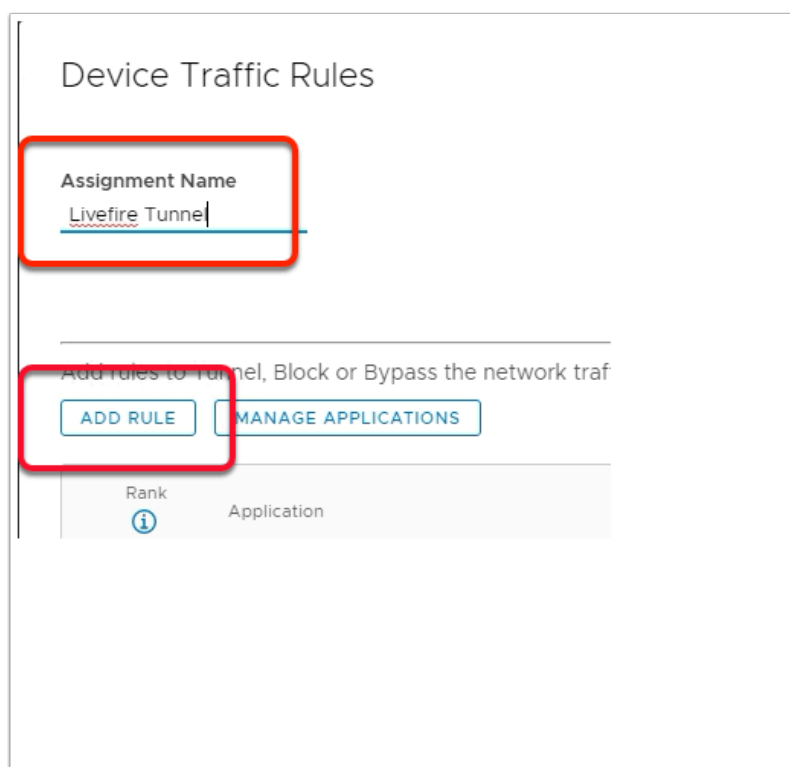
10. We add support for tunneling SMB traffic from system to allow users to map network shares and network printers. This allows end users to connect to file shares and printers that are located behind the corporate firewall. As the SMB protocol built into the Windows Operating system, the App Identifier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

Add rules to Tunnel, Block or Bypass the network traffic

ADD RULE **MANAGE APPLICATIONS**

Rank	Application
1	

Add rules to Tunnel, Block or Bypass the network traffic

ADD RULE **MANAGE APPLICATIONS**

Rank	Application
1	<input type="checkbox"/> Safari - iOS <input type="checkbox"/> Safari - macOS <input type="checkbox"/> Android workspace - Android <input type="checkbox"/> Web - Workspace ONE - And... <input type="checkbox"/> AirWatch Email Client - Andr... <input checked="" type="checkbox"/> System - WinRT <input checked="" type="checkbox"/> Livefire Chrome Tunnel - Win... <input checked="" type="checkbox"/> RDP - WinRT <input type="checkbox"/> Samba Domains - iOS <input type="checkbox"/> All Applications

System - WinRT x

Livefire Chrome Tunnel - WinRT x

RDP - WinRT x

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

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

network traffic. There is also an option available to route network traffic to a custom web proxy

Action	Destination ?
TUNNEL	<input type="text" value="rdsh-01a.euc-livewire.com"/>
BYPASS	*

CANCEL SAVE

Are you sure you want to continue? ×

Publishing Device Traffic Rules will update and republish all Tunnel profiles managed at this Organization Group. Profiles in lower Organization Groups should be manually updated.

CANCEL OK

17. Under **Destination** enter the following:-
- Type: **rdsh-01a.euc-livewire.com**
 - Select **SAVE**
 - In the **Are you sure you want to continue?** window
 - select **OK**

Manage Traffic Assignments ×

Manage the available Device Traffic Rule sets.

ADD DELETE

	Assignment Name	Number of rules	Default
<input type="radio"/>	Default	0	Yes
<input type="radio"/>	Livewire Tunnel	1	No

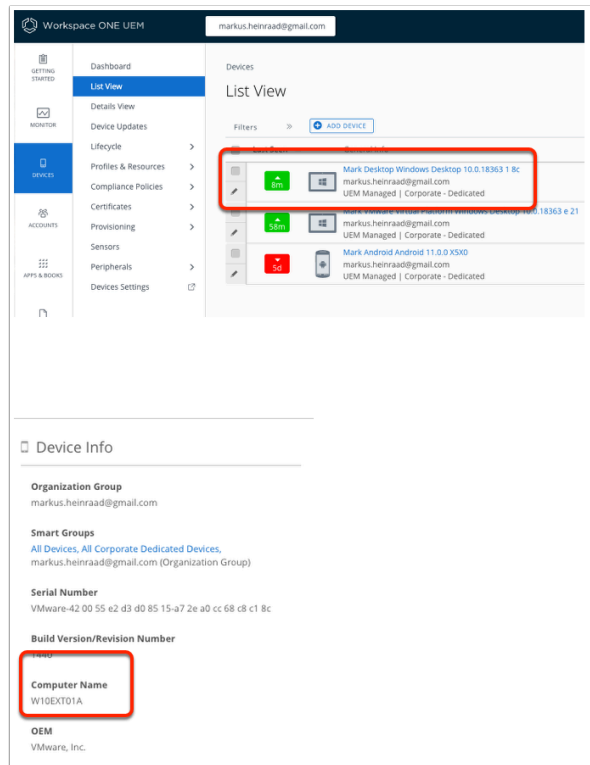
CLOSE

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

- Select **CLOSE**

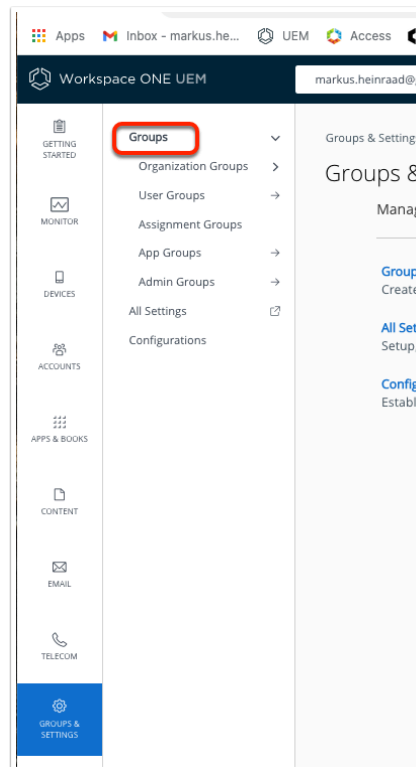
Part 4: Distributing Workspace ONE Tunnel Application, for Windows 10

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



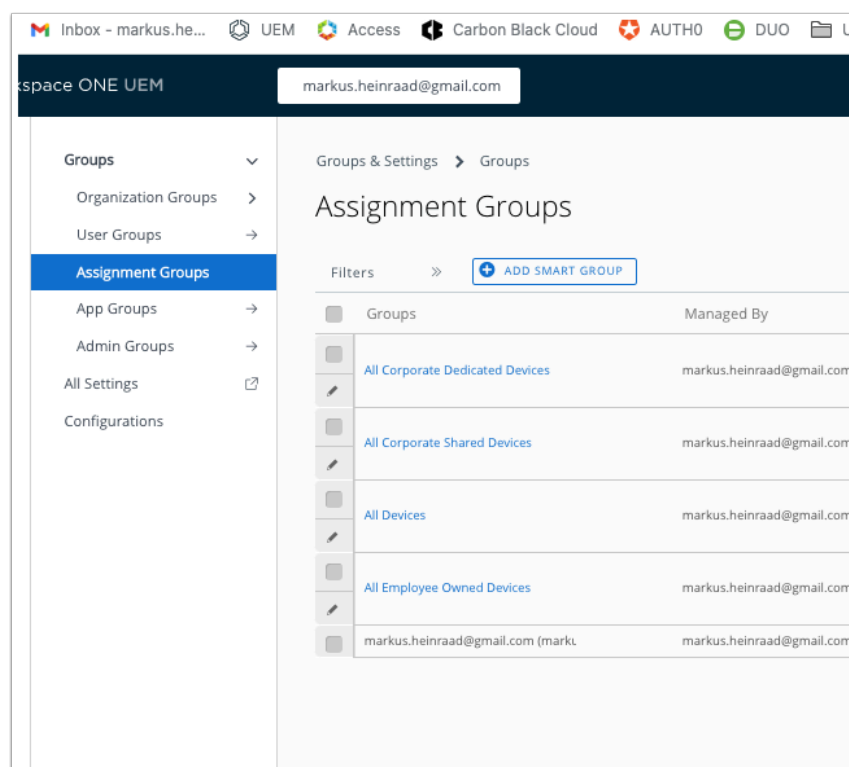
1. On your **ControlCenter** server

- 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**

Create New Smart Group

Name

Managed By markus.heinraad@gmail.com

Choose Type

Organization Group All

☒ markus.heinraad@gmail.com

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

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

Edit Smart Group

Name

Managed By markus.heinraad@gmail.com

Choose Type

Devices 1

Choose Type

Devices 1

ManfredVogal@gmail.com: VMware7.1 2 12W10EXT01A666	<input type="button" value="ADD"/>
ManfredVogal@gmail.com: VMware Virtual Platform e 21W10CLIENT666	
ManfredVogal@gmail.com: VMware7.1 2 12W10EXT01A666	<input type="button" value="ADD"/>
ManfredVogal@gmail.com: VMware7.1 2 9IATTENDEE125	
Mark Android Android 10.0.0 X3X0	

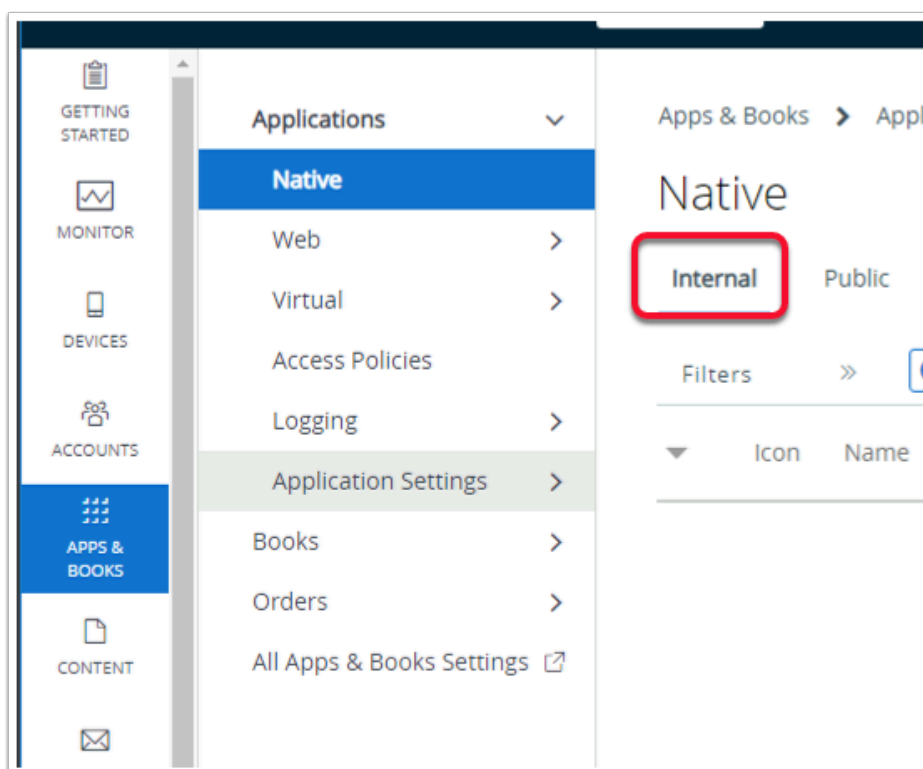
Device Preview

total enrolled device(s)

5. Next to **Choose type**

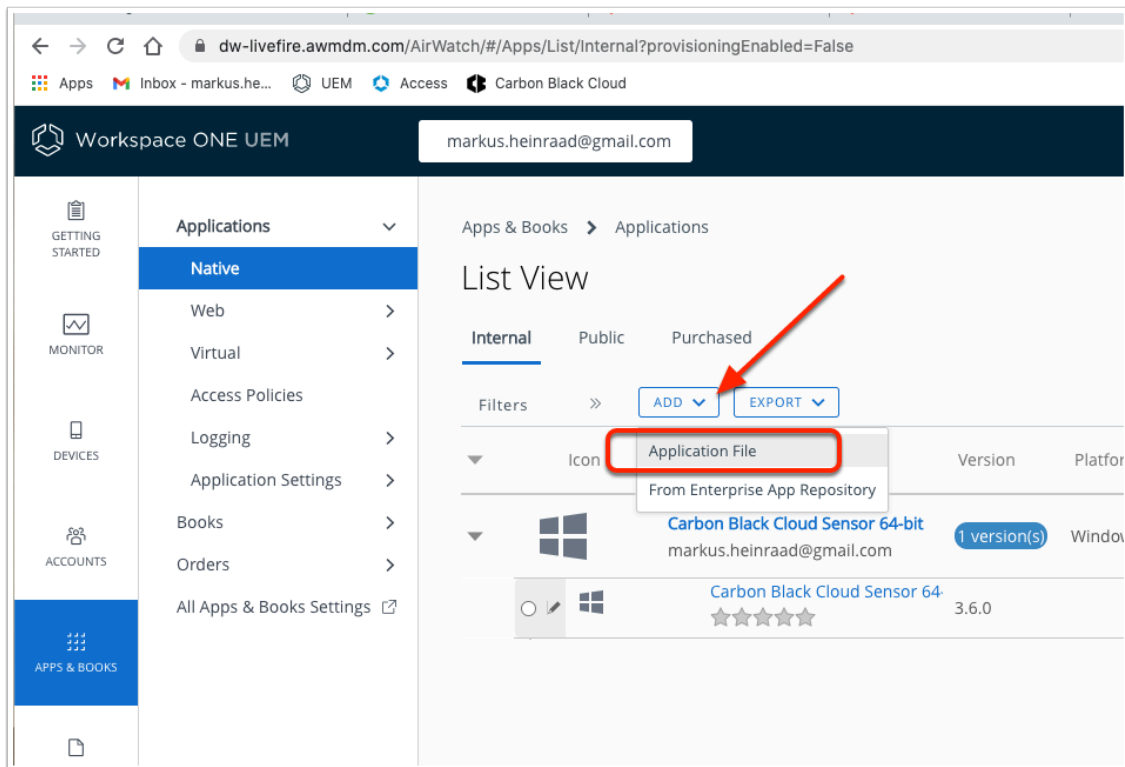
- Select **DEVICES OR USERS**
 - Under **Devices**, in the box , select **your eg Mark Windows Desktop** (for W10EXT01a)
 - (The example in the screenshot is what this test environment looks like, ensure you are select yours)
 - Select **ADD**
- To the right of the window,

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



6. On your ControlCenter server

- If necessary Login <https://cn-livewire.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**

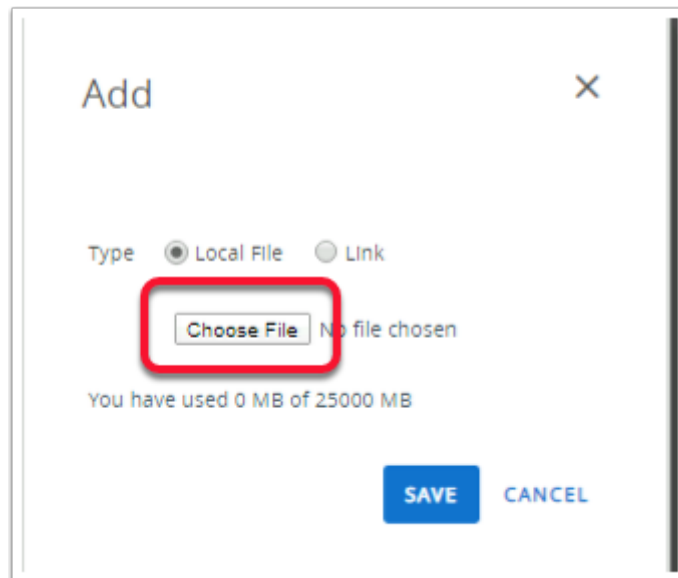
Add Application

Organization Group ID *

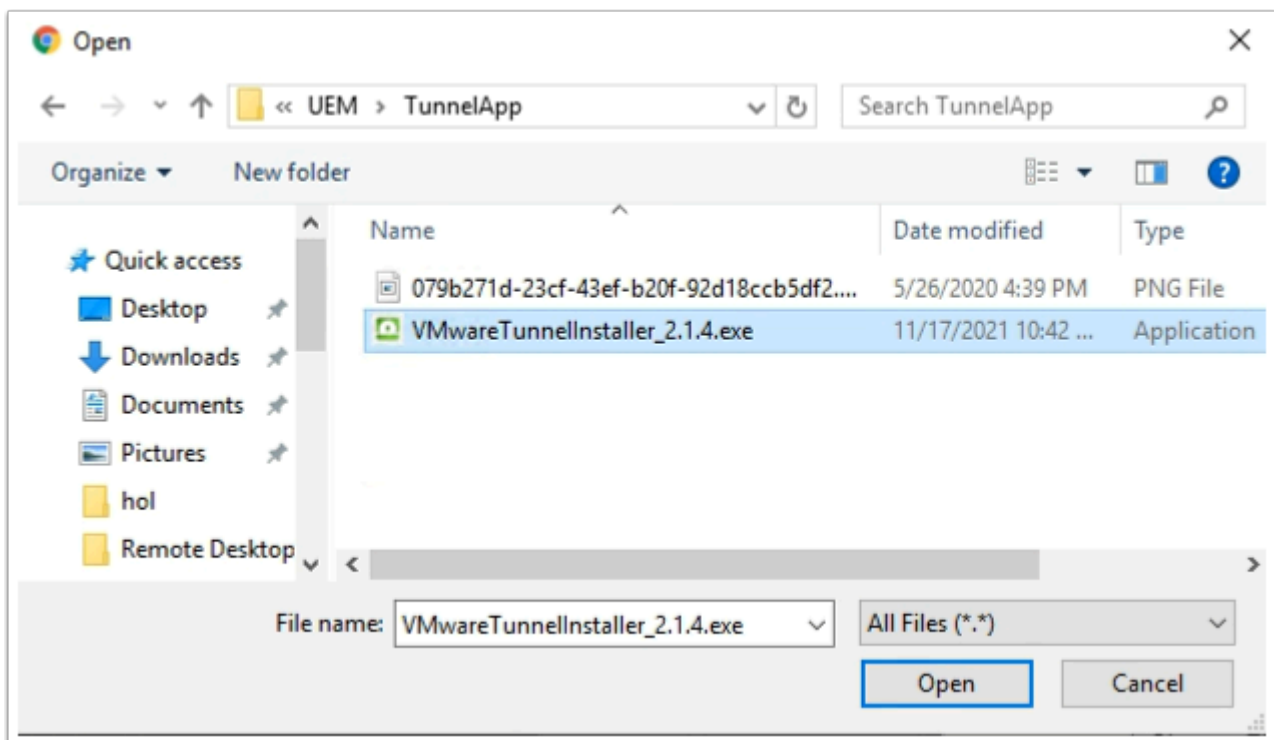
Application File *

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**

The 'Add' window is a modal dialog with a title bar containing the word 'Add' and a close button (X). Inside the window, there is a 'Type' section with two radio buttons: 'Local File' (which is selected) and 'Link'. Below this is a 'Choose File' button followed by the text 'VMwar....1.4.exe'. A status message at the bottom left states 'You have used 48 MB of 20000 MB'. At the bottom right, there are two buttons: 'SAVE' (highlighted in blue) and 'CANCEL'.

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

The 'Add Application' window is a modal dialog with a title bar containing the text 'Add Application'. It contains three main sections: 1) 'Organization Group ID' with a text input field containing 'grantZTRNEL' and a red asterisk indicating a required field. 2) 'Application File' with a text input field containing 'VMwareTunnelInstaller_2.1.4.exe', a red asterisk, and an 'UPLOAD' button to its right. 3) 'Is this a dependency app?' with two radio buttons, 'YES' and 'NO' (which is selected), and an information icon (i) to the right. A 'CONTINUE' button is located at the bottom right of the window.

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

Build Version {be42421d-ec20-4538-aba6-393b04e960e4}

Version 1 . 0 . 0

Supported Processor Architecture 64-bit

Is Beta YES NO

Add Application - VMwareTunnelInstaller_2.1.4.exe
Internal | Managed By: grantZTRNEL | Application ID: {d44afe57-dd74-4f33-b797-48654f3cd9f}

Details Files Deployment Options Images Terms of Use

Upload any scripts to identify the course of actions to be run to uninstall the application.

Custom Script Type *

Uninstall Command * VMwareTunnelInstaller_2.1.4.exe /uninstall /Passive

CAI

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**

Windows logo 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**

When To Call Install Complete

Identify Application By *

DEFINING CRITERIA USING CUSTOM

+ ADD ⓘ

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

Add Criteria

Criteria Type * File exists ⓘ

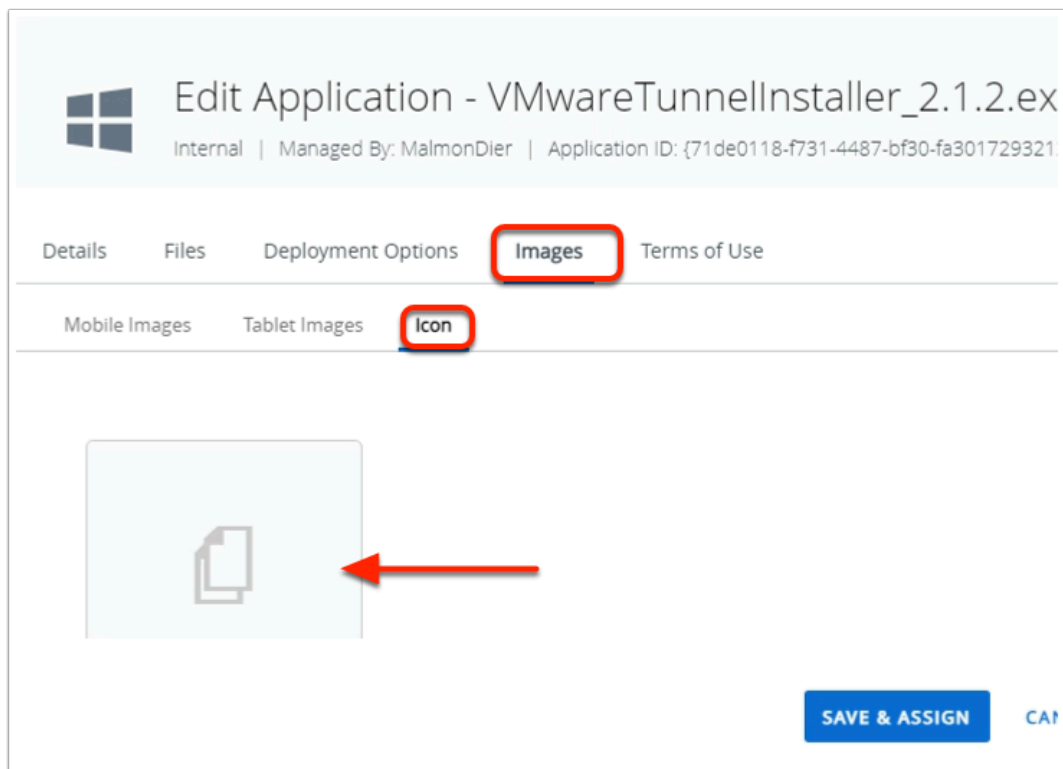
Path * C:\Program Files\VMware\Workspace ONE Tunnel\VMwareTunnel.exe ⓘ

Version * Any

Modified On * 2/02/1999 12:00 AM ⓘ

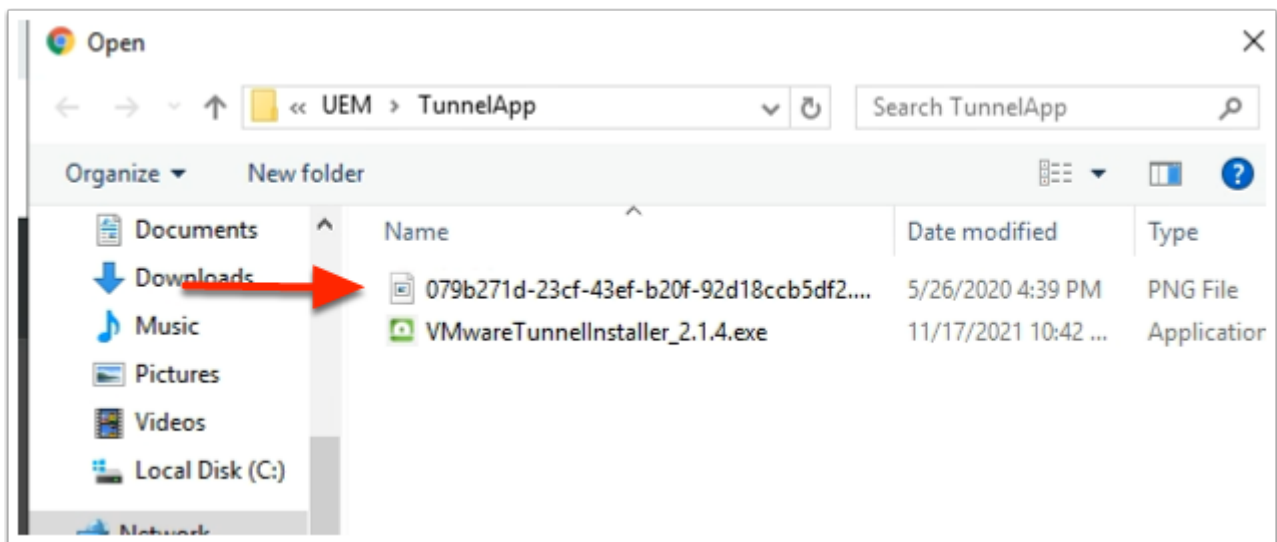
ADD CANCEL

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**.



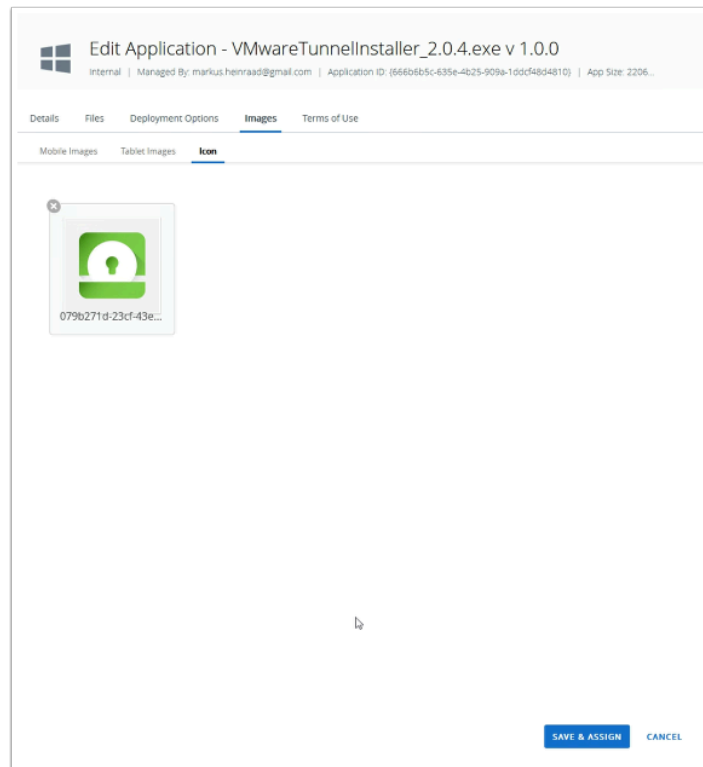
18. In the **Edit Application - VMwareTunnelInstaller_2.1.4.exe** window

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

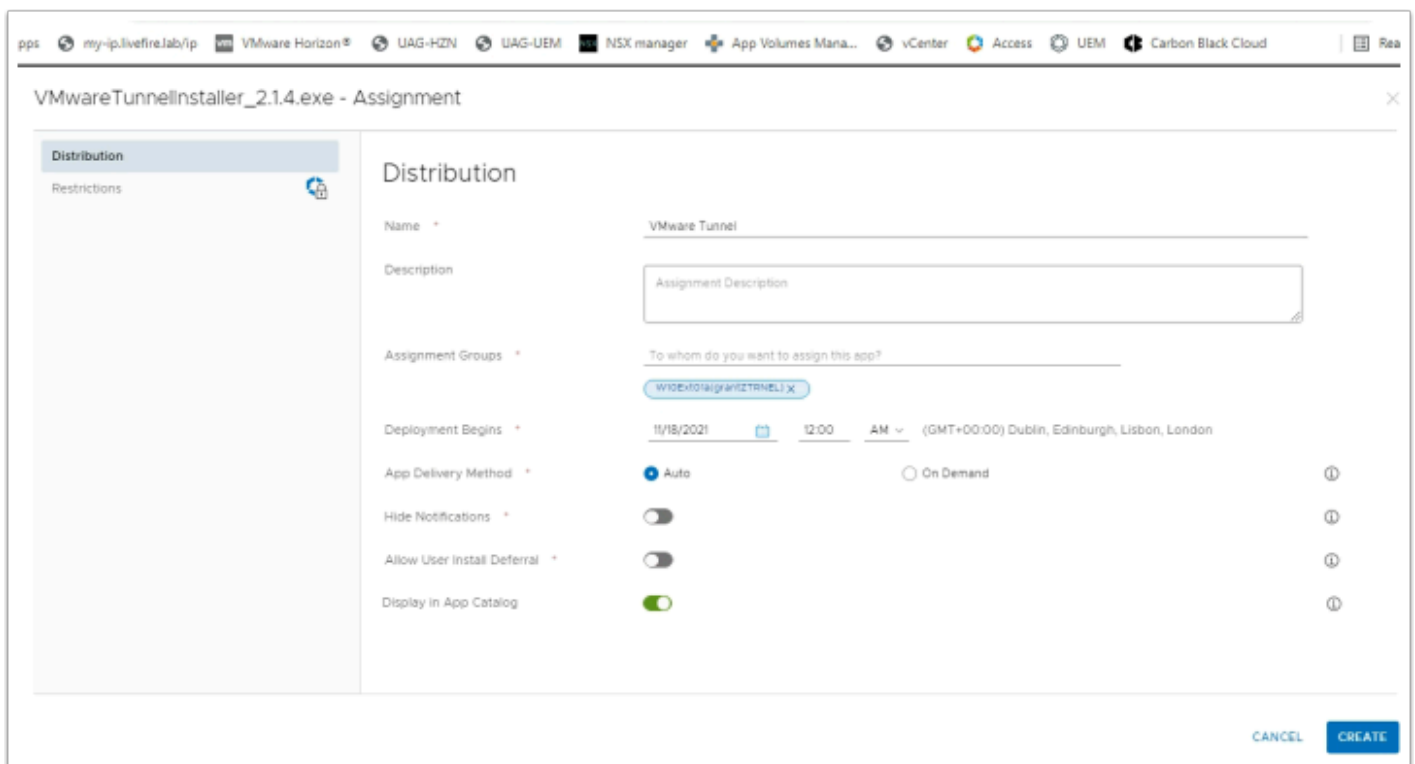


19. In the **Open** window,

- 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**

VMwareTunnellInstaller_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

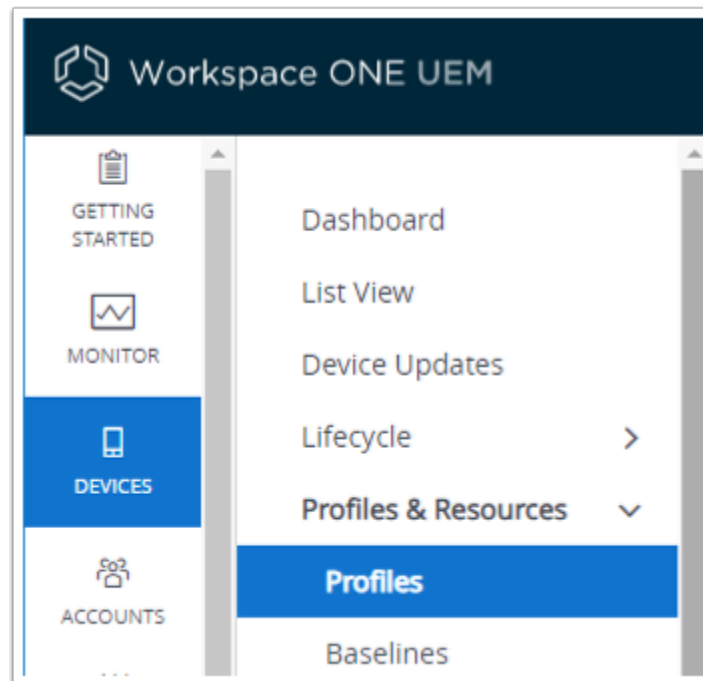
Priority	Assignment Name	Description
0	VMware Tunnel	

VMwareTunnellInstaller_2.1.4.exe - Preview Assigned Devices

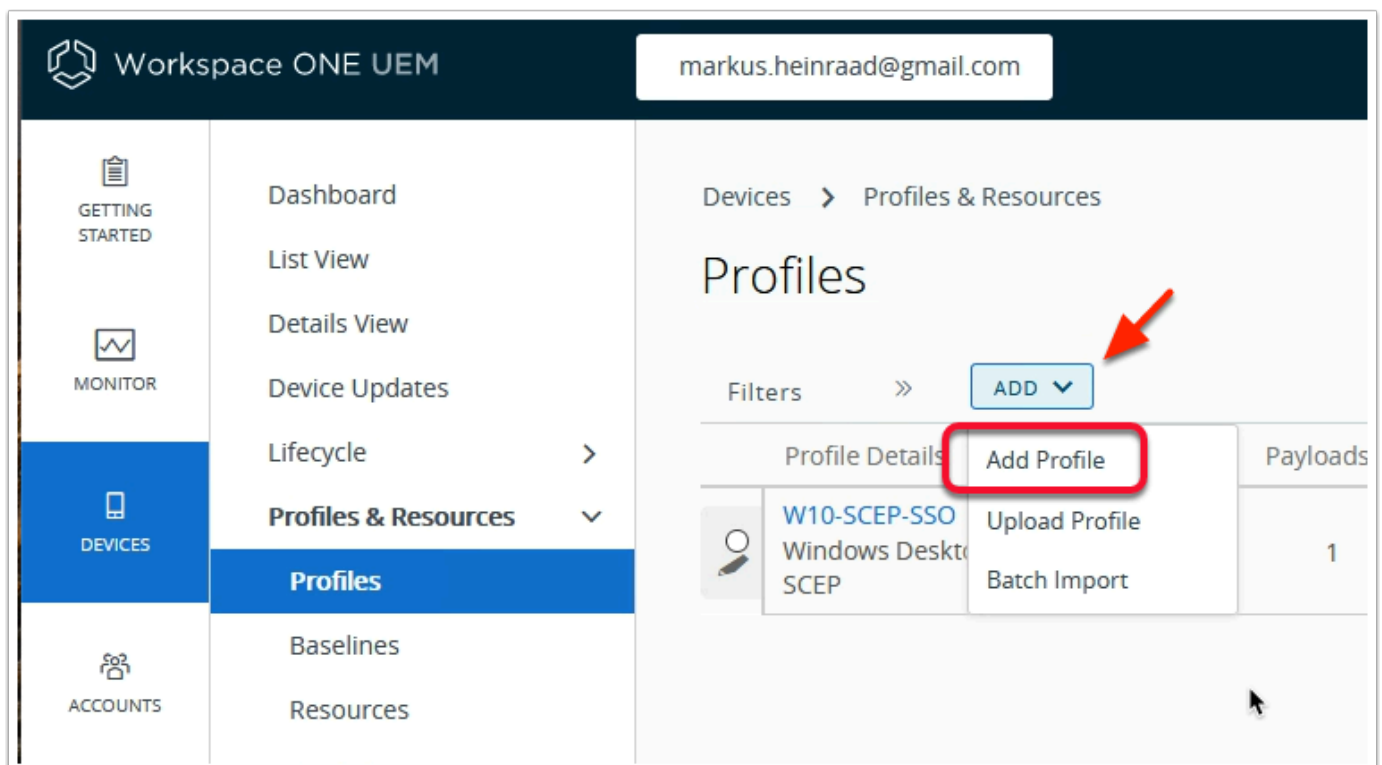
Assignment status	Friendly name	User
Added	Mark VMware7.1 Windows Desktop 10.0.18363.5 e5	Mark

- On the **VMwareTunnellInstaller_2.1.4.exe - Assignment** window
 - Select **SAVE**
 - On the **VMwareTunnellInstaller_2.1.4.exe - Assignment Devices** window
 - Select **PUBLISH**

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

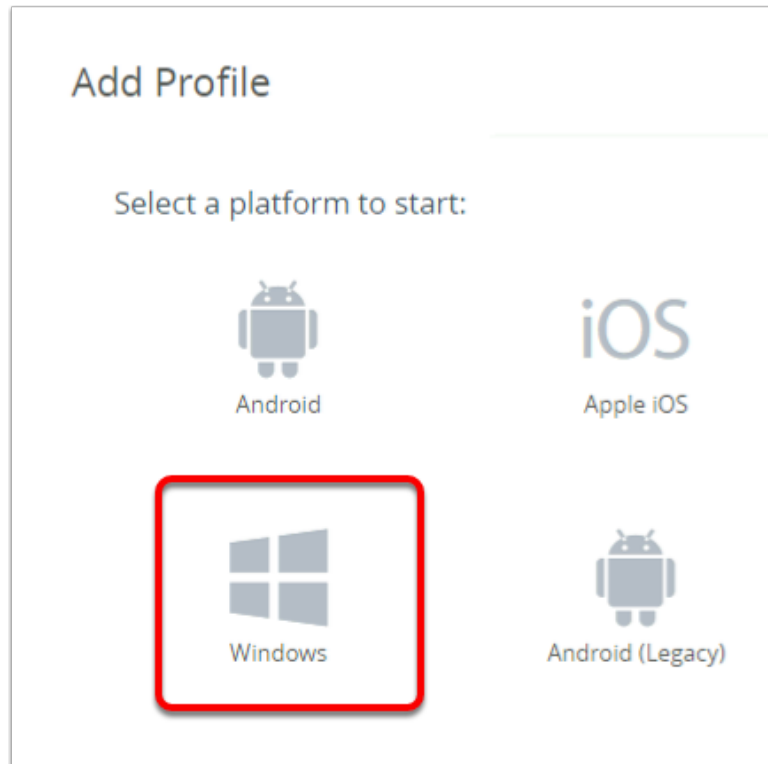


1. In **Workspace ONE UEM** inventory
 - Select **DEVICES** > **Profile & Resources**
 - Select **Profiles**



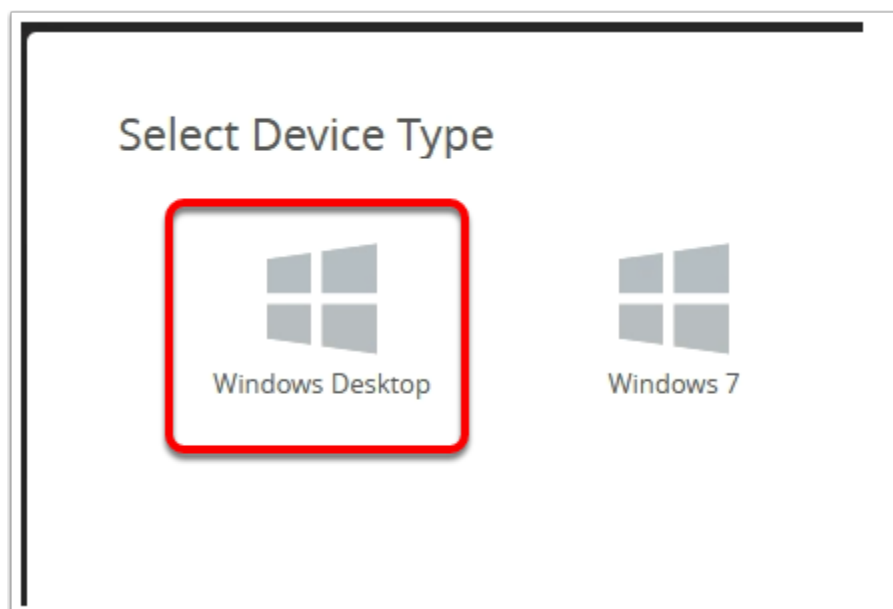
2. Under **Profiles**

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



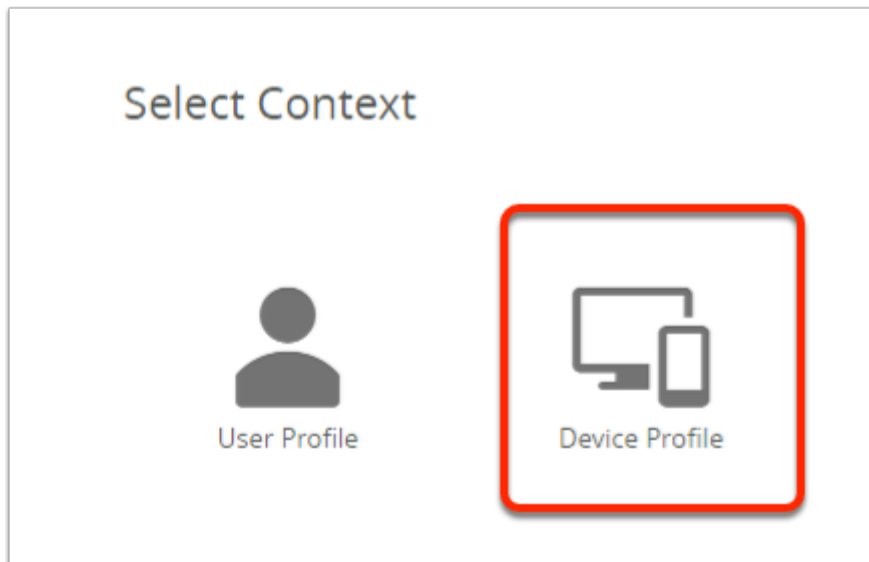
3. In the **Add Profile** window

- Select **Windows**



4. In the **Select Device Type** window

- Select **Windows Desktop**



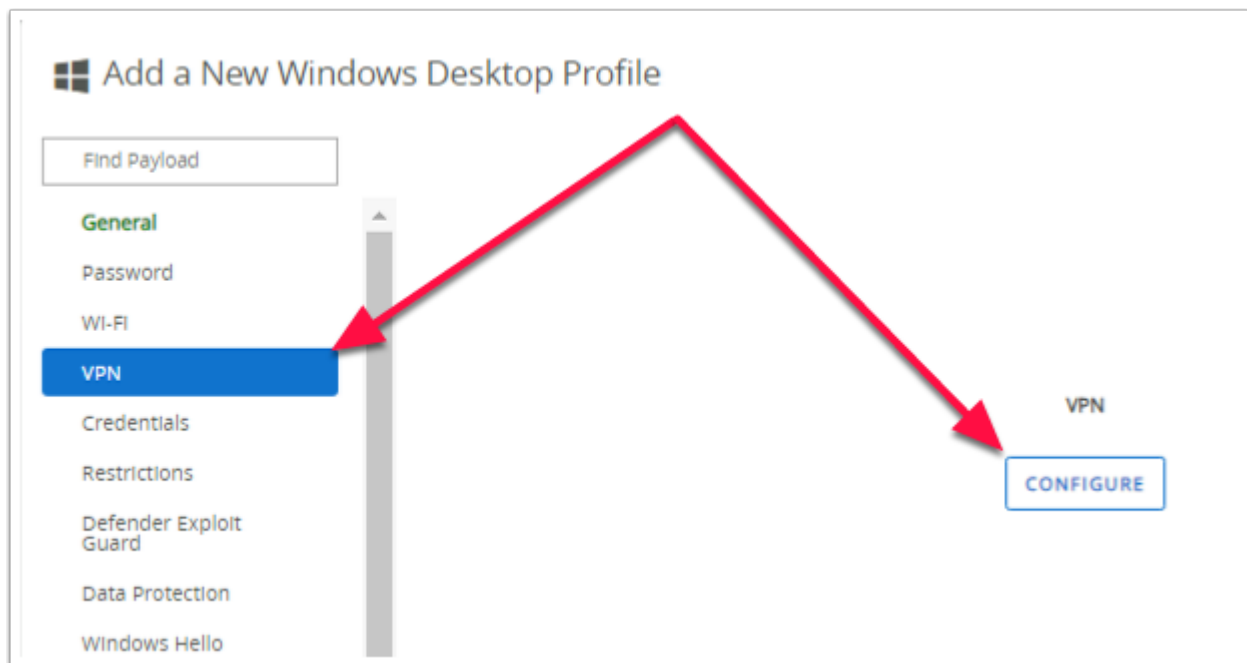
5. In **Select Context** window

- Select **Device Profile**

The image displays the 'Per App VPN' configuration window. On the left, a sidebar lists various settings, with 'VPN' highlighted by a red box. The main area is the 'General' tab. The 'Name' field is set to 'Per App VPN'. The 'Smart Groups' field shows a selected group 'markus.heinraad@gmail.com (markus.heinraad@gmail.com)' with a red box around the selection area. Other fields include 'Version' (1), 'Description', 'Deployment' (Managed), 'Assignment Type' (Auto), 'Allow Removal' (Always), 'Managed By' (markus.heinraad@gmail.com), 'Exclusions' (NO), 'Additional Assignment Criteria' (unchecked), 'Removal Date' (M/D/YYYY), and 'Track Profile Status during OOB Provisioning' (unchecked).

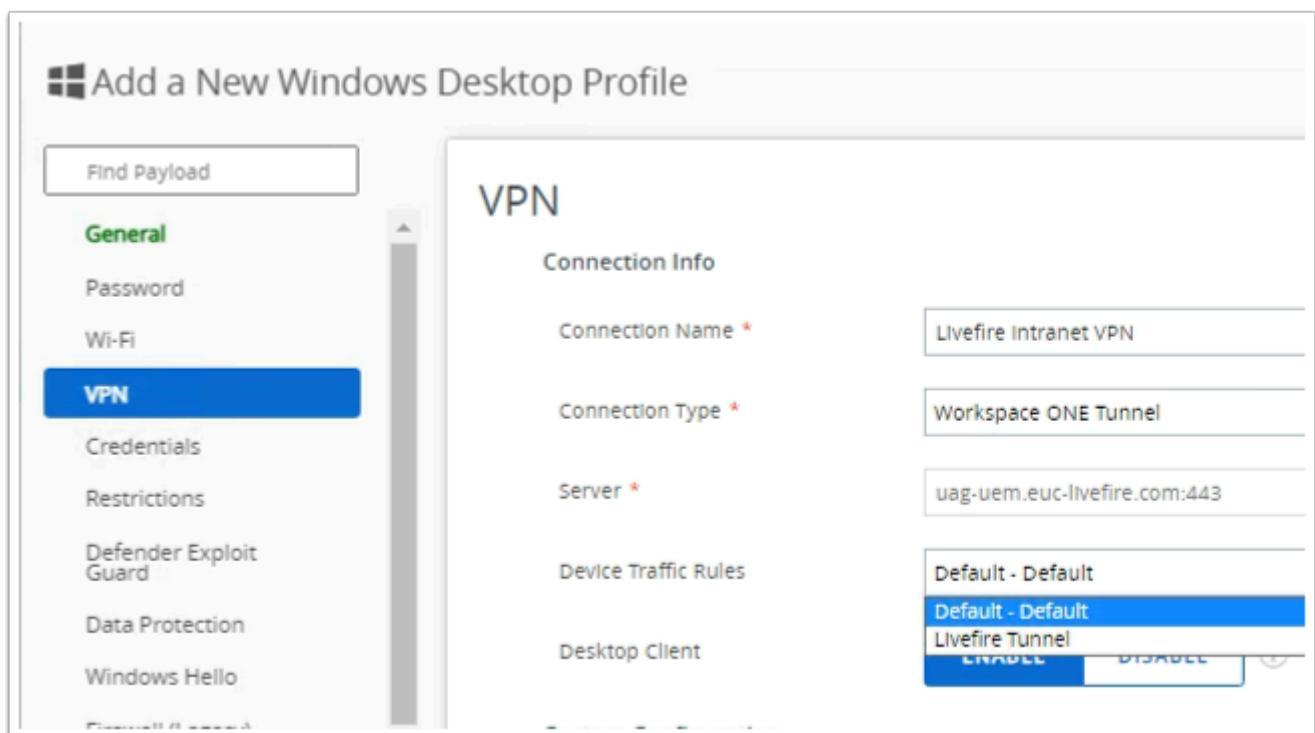
6. In the **Add Profile** window,

- 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-liv...</ServerCertSN>
</CustomConfiguration>
```

Trusted Network Detection

DNS Resolution via Tunnel Gateway

Domain ⓘ

euc-liv...

+ ADD NEW DOMAIN

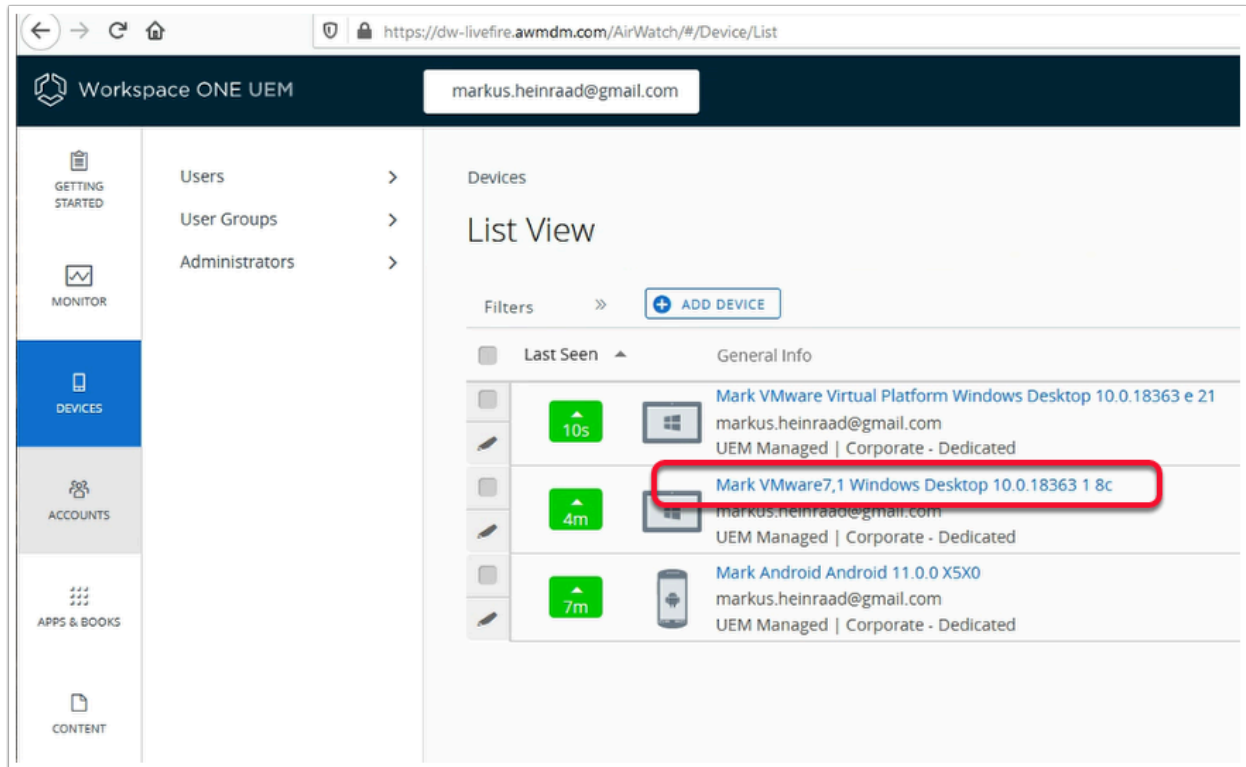
SAVE AND PUBLISH CANCEL

PUBLISH CANCEL

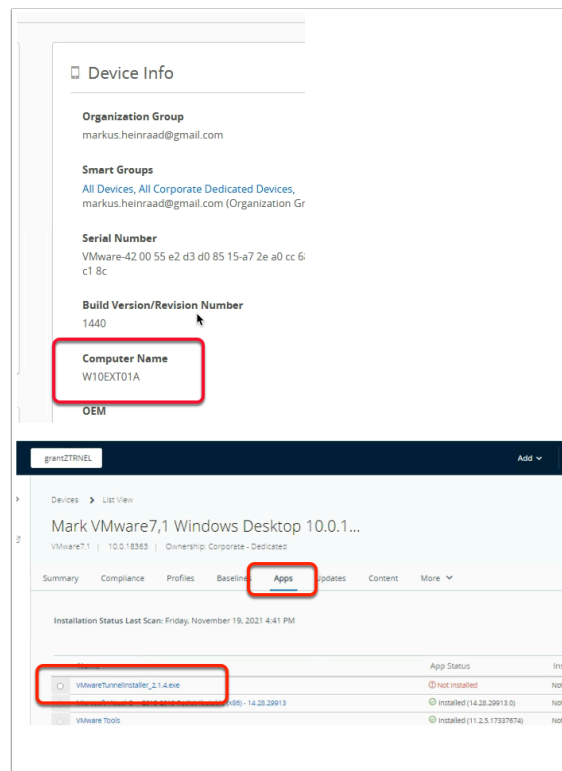
9. In the **VPN** window, next to:

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

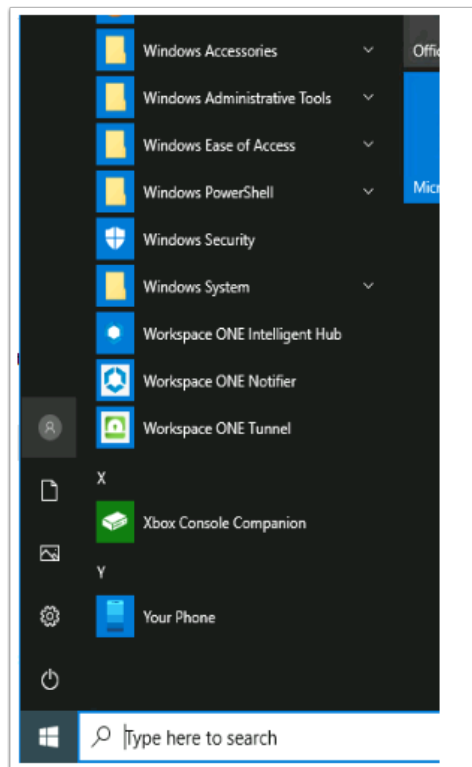
Part 6: Testing Per APP VPN Tunneling with Windows 10



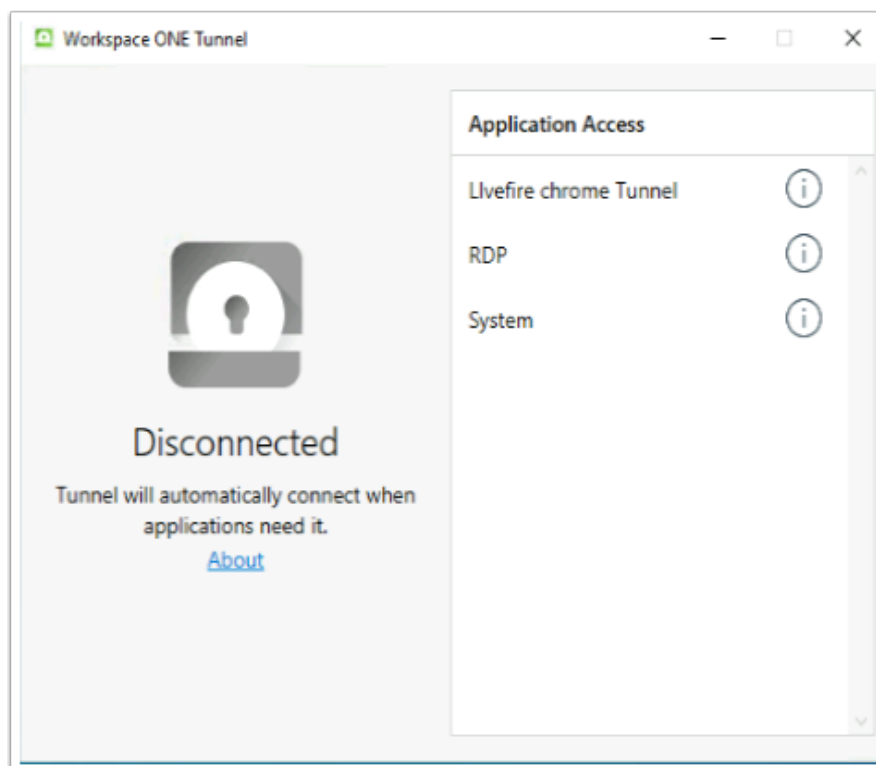
1. In the **Workspace ONE UEM** console
 - Select **DEVICES > List View**
 - Under **List View**,
 - Select Your. **Windows Desktop 10.0.1863 (W10EXT01a enrolled device)**



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**

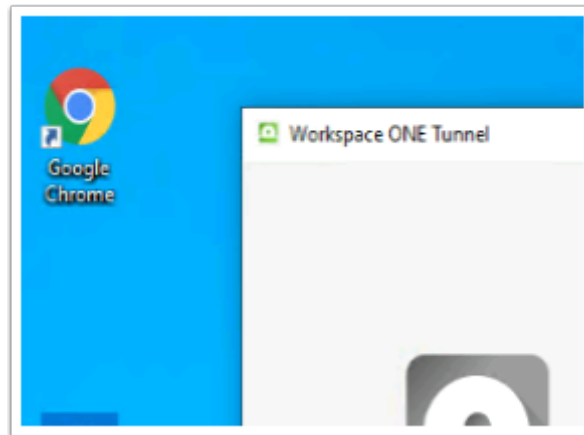


3. Switch to your **W10EXT01a** virtual machine.
 - Select the **Start Menu** and scroll down to **Workspace ONE Tunnel** under **Recently added**
 - **Note**

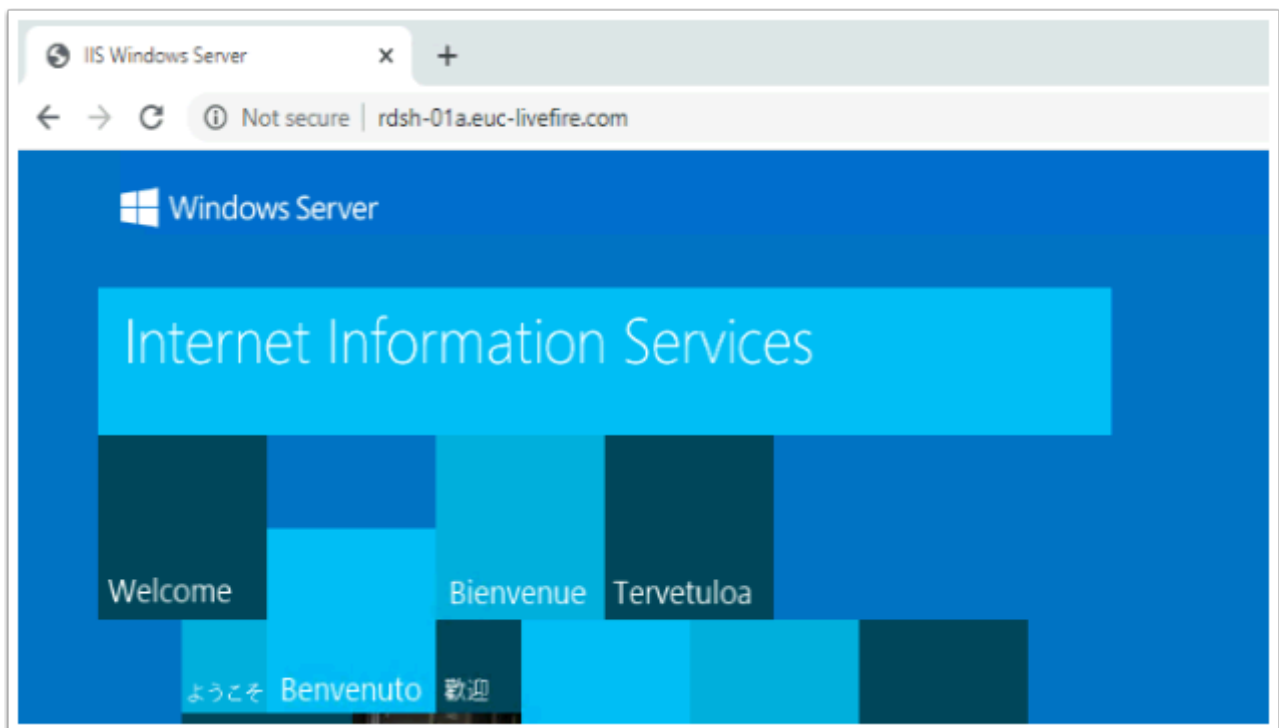


4. In the **Workspace ONE Tunnel** application notice your **Application Access** configurations

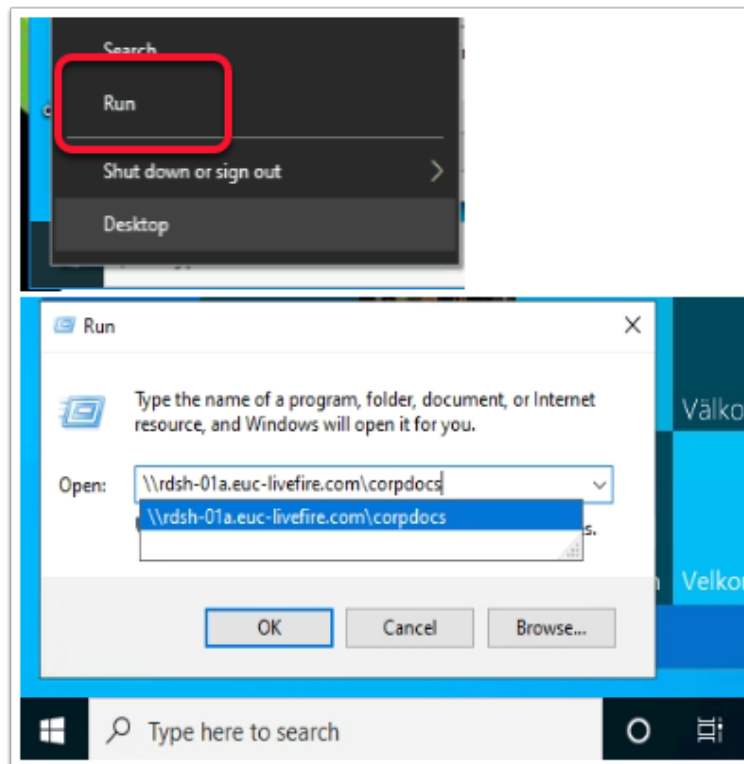
- We will now proceed with a test



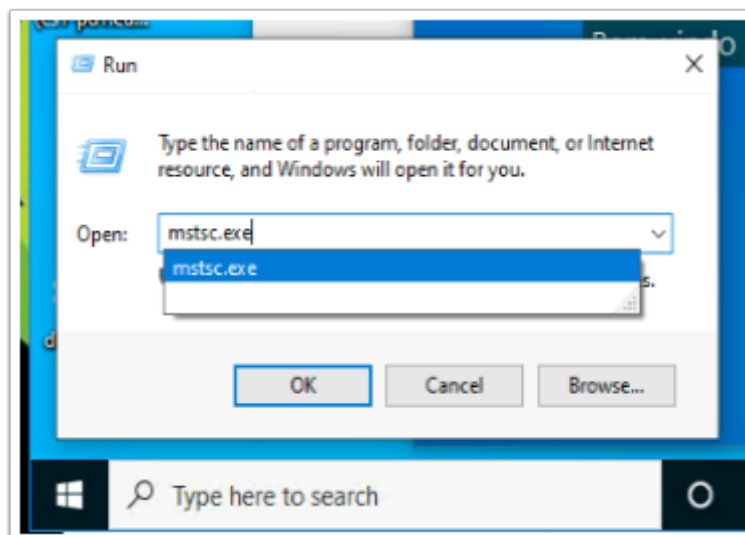
5. From the **w10EXT01a** Desktop launch the **Google Chrome** browser



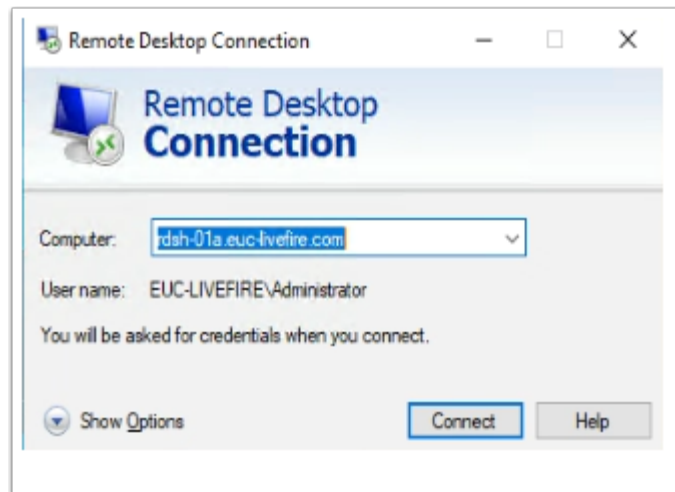
6. In the **Google Chrome Address** bar.
- Enter <http://rdsh-01a.euc-livewire.com> and select **Enter**
 - You should now see the default IIS web services web page



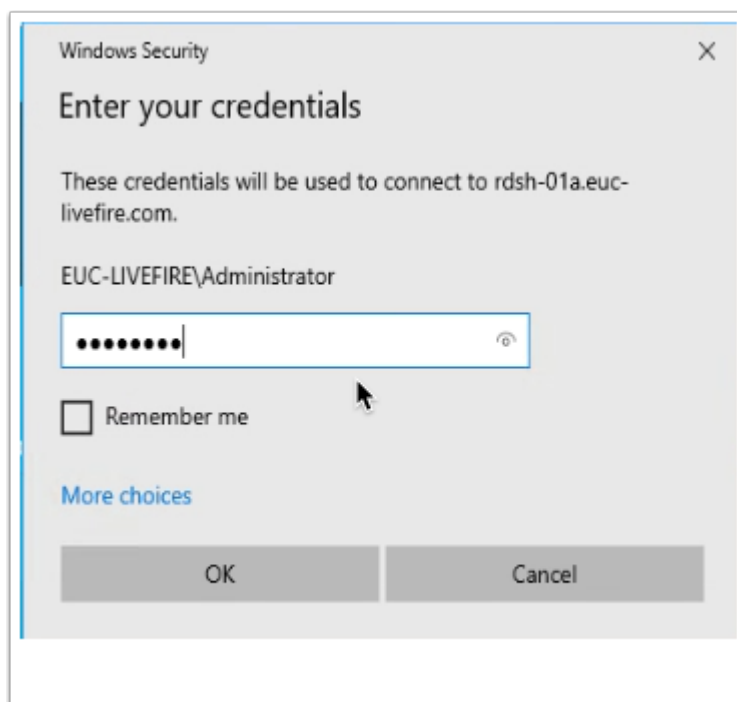
7. On the W10Ext01a Desktop
 - Select the **Start** button, right-click, select **Run**,
 - Next to **Open:** type **\\rdsh-01a.euc-livefire.com\corpdocs**
 - Select **OK**
 - Notice that you are now leveraging the SMB based functionality in **VMware Workspace ONE Tunnel**. This too might considered in-secure, this has now been secured using **VMware Workspace ONE Tunnel**



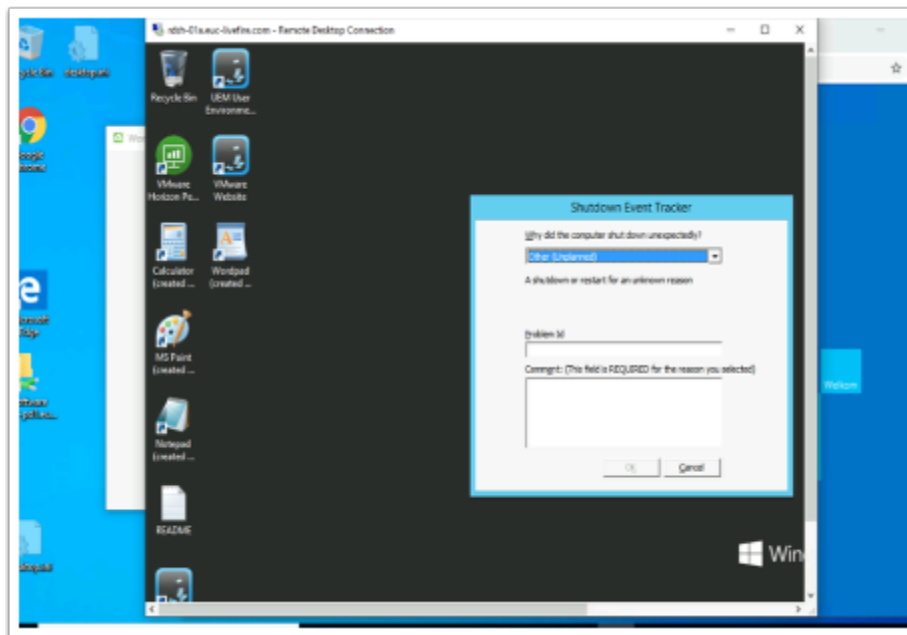
8. In the **Run** window next to **Open:** delete the text from **step 7**, type **mstsc.exe** and select **OK**



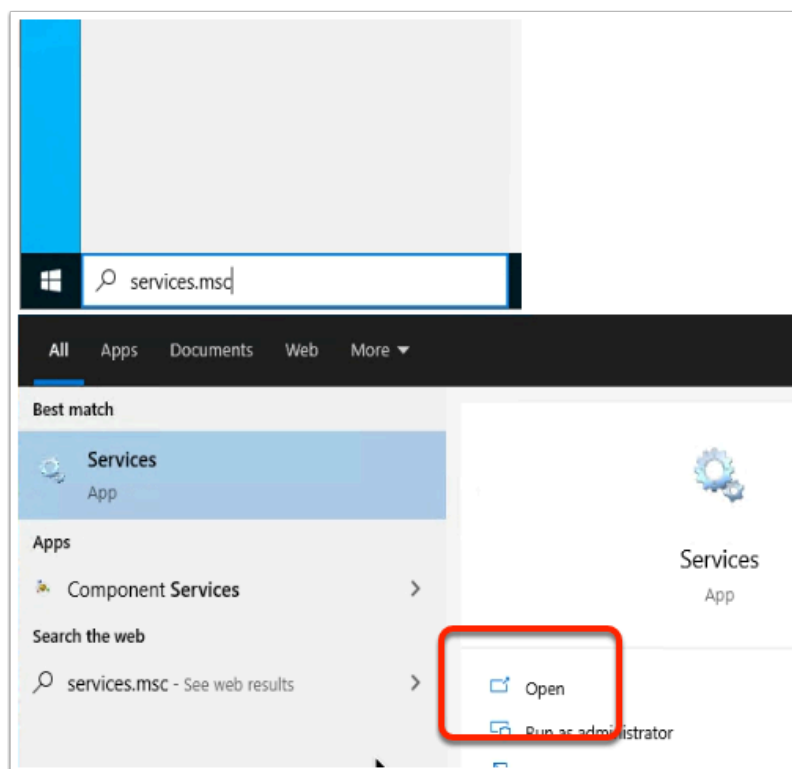
9. In the **Remote Desktop Connection** window, next to
- **Computer:** type **rdsh-01a.euc-livfire.com**
 - **User name:** type **EUC-livfire\administrator**
 - Select **Connect**



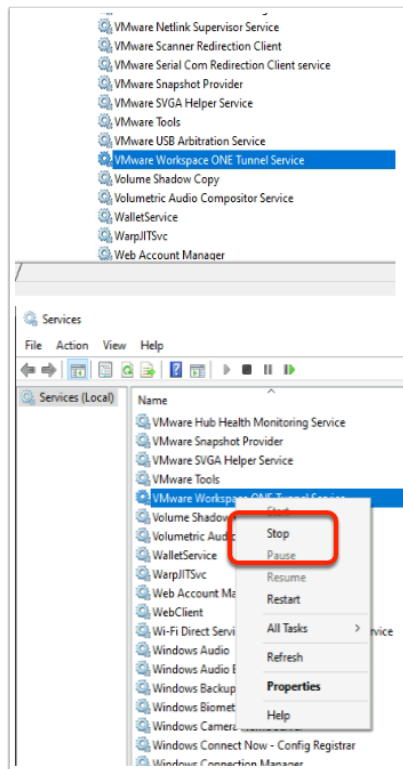
10. In the **Enter your credentials** enter **VMware1!** as the password
- Select **OK**



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

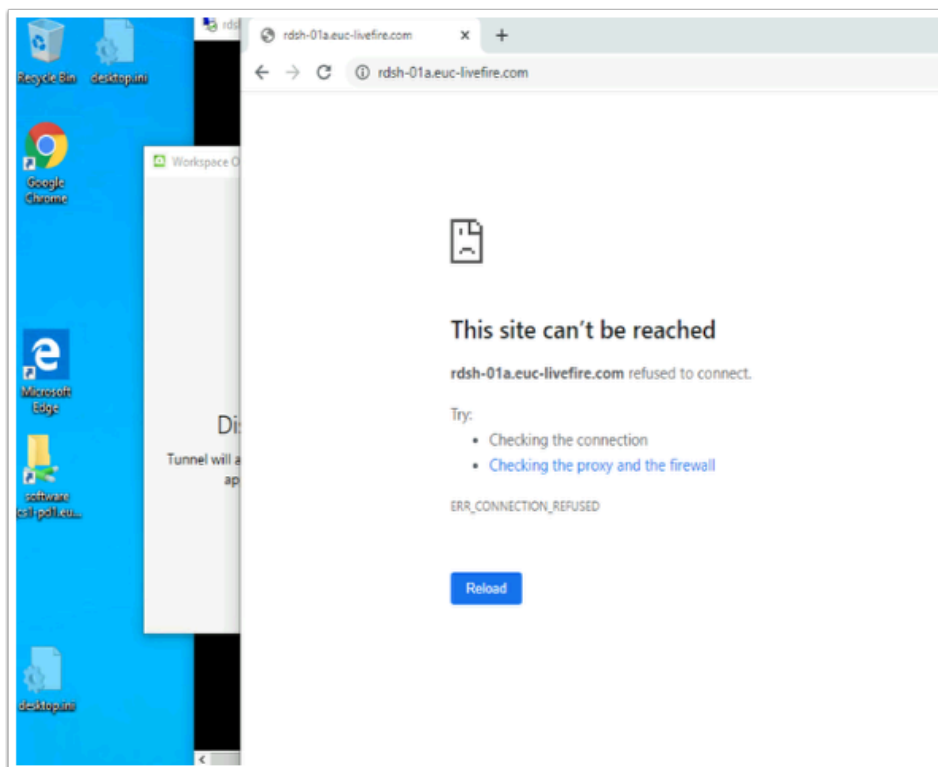


12. On your **W10EXT01a** Desktop,
- In the **Type here to Search** area enter **services.msc**
 - Under the **Services** shortcut, select **Open**
 - Select **Yes**



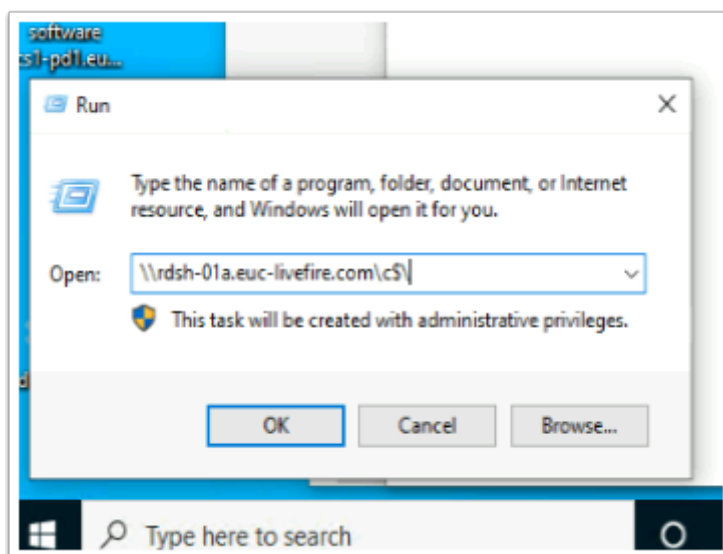
13. In the **Services MMC**

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

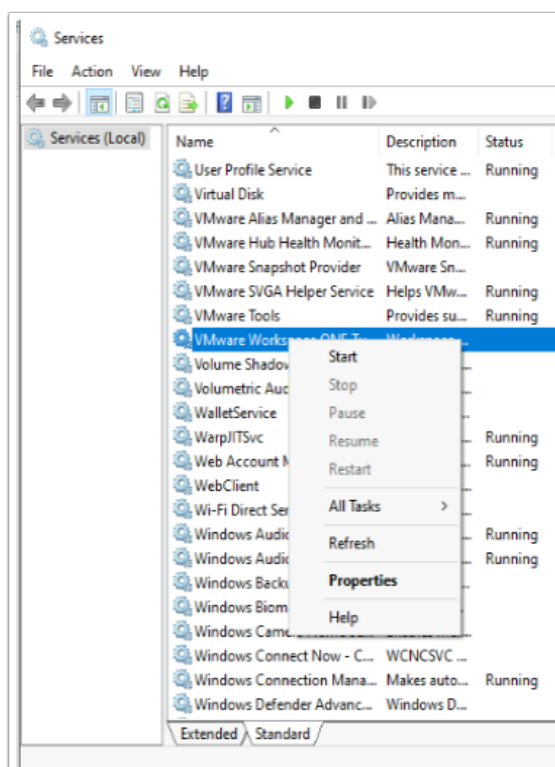


14. Notice your RDP connection just got disconnected!

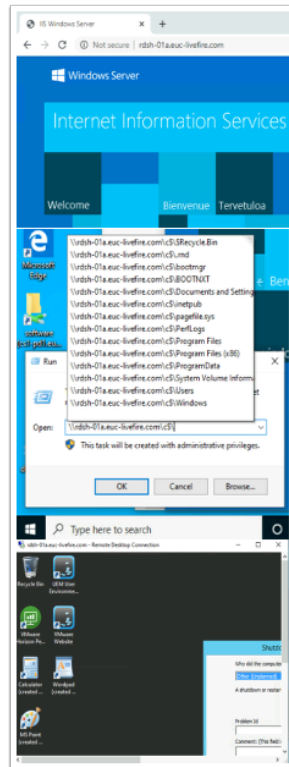
- **Refresh** your **Chrome browser** and notice you are unable to reach your website on the **RDSH-01a.euc-livewire.com** server.



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>