## 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.euclivefire.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

9443/admin/index.html#!/Login
18 🕜 vCenter 📀 UAG-HZN 📀 UAG-UEM 🏧 NSX manager
<u></u>
VMware
N
Unified Access Gateway
admin
Login

- 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

Tunnel Settings		
Enable Tunnel Settings	● N0	0
I	Save Cancel	

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

Tunnel Settings		
Enable or disable Tunnel Settings		(i)
API Server URL *	https://cn-livefire.awmdm.com	Ū
API Server Username *	grantflenderman@gmail.com	(i)
API Server Password *		(i)
Organization Group ID *	grantZTRN444	(i)
Tunnel Server Hostname *	uag-uem.euc-livefire.com	0
<u>More</u> .≽		
	Save Cancel	

- 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**

Use for Tunnel Proxy	NO	0	
Trusted Certificates No	trusted certificate is added.	• (1)	
Host Entries Ad	dd new host entry	• •	
Less A			
	Save Cancel		
NTLM Authentication	NO NO		(j)
Use for Tunnel Proxy	O NO		(j)
Trusted Certificates	Alias	Select	•••
Host Entries	Add new host entry		•
Less *			

- 6. Find the **Trusted Certificates**, section
  - To the right of **Trusted Certificates**, click the **+ icon**
  - Click the **Select** button

Open       Cancel         • New folder       Search functionation on the set of set of sector functionation of set of set of sector functionation of set of se	<ul> <li>Custom Files (</li> </ul>	*.crt;*.cer) ~							
Hende hoteneous-buffer.com ; sehare ; eterficite : 5 for Under 201 v ()     Iso in the inconcerbuffer.com ; iso inco	Open	Cancel .:!							;
Nor folder     Nore for for concerning 12/2021 1054 AM     C-0.007(Centificate 3.00     Center of the for concerning 12/2021 1054 AM     Secure (Centificate 3.00     Center of the for concerning 12/2021 1054 AM     Port of the for concerning 12/2021 1054		n.euc-livefire.com > software >	certificates > Euc-Li	ivefire 2021			~ Ö	Search Euc-Livefire	2021 ,0
Keess Akeps are circled agene abaution are circled agene a	<ul> <li>New folder</li> </ul>							811	• 💷 🔞
Firename_excluding.com.pem     All Fliet (*)     Cancel       NTLM Authentication     NO       Use for Tunnel Proxy     NO       Trusted Certificates     _euc-livefire_com.       Host Entries     Add new host entry       Less A	k accest stop website stop website turners l website turners k connects l website k connects l website k connects l website k connects l website k connects l website k connects l website k connects l website k connects l website k connects l website k connects l k con	n ne s-bundle dire_com of dire_com p0 direcomp00	Date modified 12/2021 1054 AM 12/2021 1054 AM 12/2021 1054 AM 12/2021 11054 AM 12/2021 11024 AM	Type CA-BURDLEFile Security Certificate PIX5 97 Certificates PIX5 97 Certificates PIX5 97 Presental Information	Size	6 KB 3 KB 8 KB 9 KB 5 KB			
Intrinsie     Less A	Cite and and the second second							All Elles (* *)	
View Line	File name:euc-live	ire_com.pem					Ý	All Files (*.*)	~ ~
	NTLM Authentica Use for Tunnel Pr Trusted Certifica Host Ent Less A	tion NO oxy NO ates _euc-livefire_con ries Add new host ent	n. <u>Char</u> try	155				Upen	Cancel

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 <u>euc-livefire\_com.pem</u> file and select Open
- At the bottom of the Tunnel Settings window select Save

## Part 2: - Configuring the VMware Tunnel Edge Service

	*
ere	🕲 UEM
	Workspace ONE <sup>™</sup> UEM
	Username
	admin_livefire
	Remember
	Password
	Log In
	Log in as a different user
	Trouble logging in

- 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

EMAIL			
TELECOM			
GROUPS & SETTINGS			
Groups		>	
All Setting	gs	Ø	
Configura	itions		

- 2. In the **Workspace ONE UEM** Console:
  - Select Groups & Settings.
  - Select Configurations.

Groups & Settings	
Configuration	ns 🗂
Establish the foundation need to drive your busin	nal settings, customizatic ness forward.
Q Tunnel	
Configuration Nam	e
Tunnel	_
> Android EMM	Android BYOD
Registration	

3. Under Configurations, in the Enter a name or category type Tunnel
When Tunnel shows under Configuration Name select Tunnel

<ul> <li>Tunnel</li> <li>Apps</li> <li>VMware Tunnel allows you to TLS 1.2 with certificate pinning policies specific to each appli demand experiences to empli</li> </ul>		Name	Category
VMware Tunnel allows you to TLS 1.2 with certificate pinnin policies specific to each appli demand experiences to empl	~	Tunnel	Apps
TLS 1.2 with certificate pinning policies specific to each appli demand experiences to empl		VMware Tuni	nel allows you to
policies specific to each appli demand experiences to empl		TLS 1.2 with c	ertificate pinning
demand experiences to empl		policies speci	fic to each appli
		demand expe	eriences to empl
		LEARN MOR	8E

#### 4. Under Name select Tunnel

oups & Settings		
ew Tunnel Configuratior	1	
nfigure fundamental Tunnel architecture to e	stablish connectivity and trust within your environment.	
SAVE CANCEL		Download Installer
<ul> <li>Deployment Details</li> </ul>	Basic	
Deployment Type	💽 Basic 🔘 Cascade  🚯	
Hostname *	uag-uem.euc-livefire.com	
Port *	443	
> Server Authentication	AirWatch	
> Client Authentication	AirWatch	
> Networking	Disabled	
> 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

anner configuration		
EDIT DISABLE DOWNLOAD XI L	To exhibit consectivity and rust within your environment.	
✓ Deployment Details	Basic	
Test Connection	×	
Connection	Status	
Console to AWCM	Current	
	Success	
No Information to display. Please r active for it to report data back to	make sure Tunnel server(s) is installed and AirWatch.	
No Information to display Please active for it to report data back to Test Connection	make sure Tunnel server(s) is installed and AirWatch.	
No information to display. Please i active for it to report data back to Test Connection	success make sure Tunnel server(s) is installed and AirWatch.	
No Information to display Please active for it to report data back to Test Connection Connection	Success  make sure Tunnel server(s) is installed and AirWatch.  Status  Status  Success	

- 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

	-	• • • • • •	
General Settings			
	Edge Service Settings	HIDE 🔍 🌫 Active Sessions: 0	
	0	Horizon Settings	٥
	0	Reverse Proxy Settings	٥
	•	Tunnel Settings	•
	0	Secure Email Gateway Settings	٥
	0	Content Gateway Settings	٥
	Authentication Settings	SHOW	
Advanced Settings			
	Advance	d Settings	
	System	Configuration	٥

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 <sup>™</sup> UE	M
Username	
markus.heinraad@gmail.com	
✓ Remember	
Password	
••••••	
	ħ
Log In	
Log in as a different user	

- 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

>		Group	s & Settings	
2		Cor	nfigurations	; 🗂
		drive y	ion the foundationals	d.
		Q Er	ter a name or catego	bry
		,	Name Policies	Category
		>	SMS	Customization
		>	SSL Pinning	Certificates
		>	Shared Device	Platform Setup
		>	Syslog	Integration
	_	>	Terms of Use	Compliance
		>	Tunnel	Apps Netwo
		>	VPP Managed Distribution	App Management

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

Total Rules	
Applications All Other Apps	TUNNEL

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

ſ	Manage the	avail ole Device Tr	gnments affic Rule sets.	×
ų	-	Name	Number of rules	Default
	O Defa	iuit	0	Yes
				CLOSE
De	vice Tr	affic Rule	es	
Assi Ado	rules to T	me unnel Block o MANAGE AP	r Bypass the pet	work traffic usi
	Rank	Application		Ac
	1		~	Ţ
Ma	inage A	Applicatic	ins	
The	se applicat	ions will be av	ailable for use in	Device Traffic
4	DD	]		Q_Sear
Fri	endly name	- Platform		
			-	

- 5. Under Manage Traffic Assignments
  - Select ADD
  - Select MANAGE APPLICATIONS

#### • In Manage Applications window

Select ADD

Add Application				×
Add application details for setting	g app traffic policies.			
Platform *	Windows ~			
Friendly Name *	Livefire chrome Tunnel	-		
Арр Туре *	Desktop App $ \smallsetminus $			
App Identifier	C:\Program Files (x86)\Google\Chrome\Application\cl	(i)		
				_
			CANCEL	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**

Manage Applicatio	ons
These applications will be av	ailable for use in Device Traffic Rules.
ADD	Q Search an app
Friendly name - Platform	
Livefire Chrome Tunnel - Wir	IRT
	Page Size 10 V Items 1 – 1 of 1
	CANCEL
	CANCEL

- 7. In the Manage Applications window
  - Select ADD

Add application details fo	r setting app traffic policies.		
Platform *	Windows ~		
Friendly Name *	RDP		
Арр Туре 🔹	Desktop App $\vee$		
App Identifier *	C:\Windows\ <u>System32\mstsc.exe</u>	<u>(</u> )	

- 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**

Manage Applicatio	ons >
These applications will be ava	ailable for use in Device Traffic Rules.
ADD	Q Search an app
Friendly name - Platform	
RDP - WinRT	
Livefire Chrome Tunnel - Win	RT
	Page Size 10 V Items 1 – 2 of 2
	•
	CANCEL

- 9. In the **Manage Applications** window
  - Select ADD

Add Application				×
Add application details fo	r setting app traffic policies.			
Platform *	Windows ~			
Friendly Name *	System			
App Type *	Desktop App $ \smallsetminus $			
App Identifier *	System	1		
			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**

Manage Applications	$\times$
These applications will be available for	or use in Device Traffic Rules.
ADD	Q_Search an app
Friendly name - Platform	
RDP - WinRT	
System - WinRT	
Livefire Chrome Tunnel - WinRT	
	Page Size 10 V Items 1 – 3 of 3
	CANCEL
	<b>b</b>

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

Device Traffic Rules
Assignment Name Livefire Tunne
Add rules to runnel, Block or Bypass the network traf
Rank () Application

- 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

Action	Destination ()	
TUNNEL	<u>httsh-Ola.euc-livefire.com</u>	×
BYPASS	× *	
CANCEL	SAVE	
re you sure you wa	ant to continue? $\times$	
ublishing Device Traffic Rules	will update and republish all Tunnel profiles	

- 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

Manage Traffic As	ssignments		×
Manage the available Device	e Traffic Rule sets.		
Assignment Name	Number of rules	Default	
O Default	0	Yes	
O Livefire Tunnel	1	No	
			CLOSE

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

🕲 Works	pace ONE UEM	markus.heinraad@gmail.com
GETTING STARTED	Dashboard List View	<sup>Devices</sup> List View
MONITOR	Details View Device Updates	Filters » C ADD DEVICE
DEVICES	Lifecycle > Profiles & Resources > Compliance Policies > Certrificates > Provisioning > Sensors	Montheling     Montheling
###5 & BOOKS	Peripherals > Devices Settings	
Devic	e Info tion Group einraad⊛gmail.com	
Smart Gr All Device markus.h	oups s, All Corporate Dedicated Dev einraad@gmail.com (Organizat	ices, Jon Group)
Serial Nu VMware-4	<b>mber</b> 12 00 55 e2 d3 d0 85 15-a7 2e a	10 cc 68 c8 c1 8c
Build Ver 1440 Compute W10EXTO OEM VMware, I	sion/Revision Number r Name IA	

- 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

Apps	M Inbox - markus.he	🕼 UE	M 🗘 Access 📢
🖏 Works	pace ONE UEM		markus.heinraad@g
GETTING STARTED	Groups	~	Groups & Settings
MONITOR	User Groups Assignment Groups	→	Groups & Manag
DEVICES	App Groups Admin Groups	$\rightarrow$ $\rightarrow$	Group: Create
8 ACCOUNTS	All Settings Configurations	2	<b>All Sett</b> Setup,
APPS & BOOKS			<b>Config</b> Establi
CONTENT			
EMAIL			
TELECOM			
GROUPS & SETTINGS			

- 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 No	ew Smart Group		
Name	W10EXT01a	]	
	Managed By markus.heinraad@gmail.com	-	
Choose Type	CRITERIA DEVICES OR USERS		
<ul> <li>Organizat</li> </ul>	lon Group Al		
🗹 markus.	heinraad@gmail.com		

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

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

	W10EXT01a
	Managed By markus.heinraad@gmail.com
Choose Type	CRITERIA DEVICES OR USERS
Devices (	1 1
hoose Type	CRITERIA DEVICES OR USERS
Devices (i	
ManfredVoga	Il@gmail.com VMware7,1 2 12W10EXT01A666 ADD
ManfredVogal@ 21W10CLIENT	/gmail.com VMware Virtual Platform e
ManfredVogal@	9gmail.com VMware7,1 2 12W10EXT01A666
ManfredVogal@	Igmail.com VMware7,1 b 9fATTENDEE125 ADD
Mark Android Ar	ndroid 10.0.0 X3X0
Device Previ	

#### 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**

← → C iii Apps M	hbox - markus.he	- n.com// O Ac	irWatch/#/Apps/List/Internal?provisioningEnabled=False		,
🖏 Works	pace ONE UEM		markus.heinraad@gmail.com		
GETTING STARTED	Applications Native	~	Apps & Books > Applications		
MONITOR	Web Virtual	> >	Internal Public Purchased		
DEVICES	Access Policies Logging Application Settings	> >	Filters >> ADD >> EXPORT >> Icon Application File From Enterprise App Repository	Version	Platfor
ියි ACCOUNTS	Books Orders	> >	Carbon Black Cloud Sensor 64-bit markus.heinraad@gmail.com	1 version(s)	Windo
iii APPS & BOOKS	All Apps & Books Setting	s 🛛	Carbon Black Cloud Sensor 64	3.6.0	
D					

- 7. Under Internal
  - Select the dropdown next to ADD
  - Select Application File

Add Application		
Organization Group ID *	markus.heinraad@gmail.com	
Application File *		UPLOAD

- 8. In the Add Application window,
  - Select UPLOAD



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

Open			×
← → • ↑ [	« UEM	> TunnelApp v 전 Search TunnelApp	م
Organize 🔻 🛛 N	lew folder		- 🔳 🕐
- Ouiskasses	^	Name Date modified	Туре
		© 079b271d-23cf-43ef-b20f-92d18ccb5df2 5/26/2020 4:39 PM	A PNG File
Desktop	*	VMwareTunnelInstaller_2.1.4.exe 11/17/2021 10:42	Application
Downloads	*		
Documents	*		
Pictures	*		
hol			
Remote Des	ktop 🗸 🤞		>
	File nan	ne: VMwareTunnelInstaller_2.1.4.exe VMwareTunnelInstaller_2.1.4.exe VMwareTunnelInstaller_2.1.4.exe VMwareTunnelInstaller_2.1.4.exe	~
		Open	Cancel

- 10. In the File upload window
  - Browse to \\horizon.euc-livefire.com\software\UEM\TunnelApp
  - Select the VMwareTunnelInstaller\_2.1.4.exe APP
  - At the bottom of the window select **Open**

Add	×
Type <ul> <li>Local File Link</li> <li>Choose File VMwar1.4.exe</li> </ul>	
You have used 48 MB of 20000 MB	
SAVE	CANCEL

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

Add Application		
Organization Group ID *	grantZTRNEL	
Application File *	VMwareTunnelInstaller_2.1.4.exe	UPLOAD
ls this a dependency app?	YES NO ()	
		CONTINUE

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

Build Version	{be42421d-ec20-4538-aba6-393b04e960e4}
Version	1.0.0
Supported Process Architecture	or 64-bit 🔹 🕕
ls Beta	YES NO ()
Details Files Deploy	lication - VMwareTunnelInstaller_2.1.4.e ged By: grantZTRNEL   Application ID: (d44afe57-dd74-4f33-b797-48654f3cd ment Options Images Terms of Use
Upload any scripts to i Custom Script Type*	Jentify the course of actions to be run to uninstall the application.
Uninstall Command *	VMwareTunnelInstaller_2.1.4.exe /uninstall /Passive
	SAVE & ASSIGN CA

- 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 Unistall 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 (i)
Install Command * VMwareTunnelInstaller_2.1.2.exe /Install /F 🛨 (i)
Admin Privileges YES
Device Restart User-engaged restart
Number of days after 7 (i)
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**.

etails	Files Dep	oyment Options Images Terms of Use	
	Retry Interval *	5	(i)
	install Timeout *	60	(i)
	Installer Reboot Exi Code	3010	Ō
	Installer Success Ex Code	0	(i)

- 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

Add Criteria			×
Criteria Type *	File exists	• (i)	
Path *	C:\Program Riles\ <u>\Mwarg</u> \Workspace ONE Tunnel\ <u>\MwargTunnel.exg</u>	0	
Version *	Any *		
Modified On *	2/02/1999 12:00 AM × ①		

#### 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.

Edit Application - VMwareTunnelInstaller_2.1.2.ex Internal   Managed By: MalmonDier   Application ID: {71de0118-f731-4487-bf30-fa301729321
Details Files Deployment Options Images Terms of Use
Mobile Images Tablet Images
SAVE & ASSIGN CAP

#### 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

Distribution		Distribution		
Restrictions	<b>C</b> a	Distribution		
		Name *	VMware Tunnel	
		Description	Assignment Description	1
				10
		Assignment Groups	To whom do you want to assign this app?	
			WIDENTONI (WARTZTRINEL) X	
		Deployment Begins +	11/18/2021 📋 12:00 AM (GMT+00:00) Dublin, Edinburgh, Lisbon, London	
		App Delivery Method	Auto     On Demand	©
		Hide Notifications *	3	Ð
		Allow User Install Deferral +	3	٢
		Display in App Catalog		©

- 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

App V	ls /ersion : 1.0.0	0.0 UEM Version : 1.0.0.0 Platform : Window	s Desktop 🛛 Status : 🎯 Active
Assign	iments Exc	clusions	
Devices	will receive app nent to edit. Ad	plication based on the configurations below. Device ding a new assignment will create a new rule at the	s with multiple assignments will re bottom of the list.
i signi	nene to cont. Ho		bottom of the list.
ADD	ASSIGNMENT		
		-	
	Priority	Assignment Name	Description
:	0 ~	VMware Tunnel	
Mware	eTunnelInstal	ller_2.1.4.exe - Preview Assigned Devices	
	t status	Priendly Name	User
Assignment			

- 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

😥 Workspace ONE UEM			markus.heinraad@gmail.com
GETTING STARTED	Dashboard List View Details View Device Updates		Devices > Profiles & Resources Profiles Filters > ADD ~
_	Lifecycle	>	Profile Details Add Profile Payloads
	Profiles & Resources	~	W10-SCEP-SSO Upload Profile
	Profiles		SCEP Batch Import
ŝ	Baselines		
ACCOUNTS	Resources		•

#### 2. Under Profiles

- Select ADD
- Select Add Profile

Add Profile	
Select a platform to st	art:
Android	iOS Apple iOS
Windows	Android (Legacy)

- 3. In the Add Profile window
  - Select Windows

Se	lect Device Typ	e
	Windows Desktop	Windows 7

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

Select Context	
User Profile	Device Profile

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

Find Payload	General	
General	Name *	Per App VPN
WI-FI		
VPN	Version	1
Credentia s	Description	
Restrictions	Deployment	Manarod
Defender Exploit Guard	Deployment	manageu
Data Protection	Assignment Type	Auto ~
Windows Hello	Allow Removal	Always
Firewall (Legacy)		
Firewall	Managed By	markus.heinraad@gmail.com
Anti-Virus		
Encryption	Smart Groups	markus.neinraad@gmaii.com (markus.neinraad@gmaii.com)
Windows Updates	L L	Start typing to add a group
Proxy	Exclusions	NO YES
OEM Updates		
SCEP		VIEW DEVICE ASSIGNMENT
Application Control	Additional Assignment Criteria	Fnable Scheduling and install only during selected time periods
Windows Licensing	receiver an easignment of itema	Change server and an instant only during selected time periods
BIOS	Removal Date	M/D/YYYY
Klosk		

- 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

Add a New Window	vs Desktop Profile	
Find Payload	VPN	
General Password	Connection Info	
Wi-Fi	Connection Name *	Livefire Intranet VPN
VPN	Connection Type *	Workspace ONE Tunnel
Restrictions	Server *	uag-uem.euc-livefire.com:443
Defender Exploit Guard	Device Traffic Rules	Default - Default
Data Protection	Desktop Client	Default - Default Livefire Tunnel
Windows Hello		

- 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 XML	< <u>CustomConfiguration</u> > < <u>ServerCertSN</u> >*euc-livefire.com <u ServerCertSN>
Trusted Network Detection	
ONS Resolution via Tunnel Gateway	
Domain (i)	
euc-livefire.com	
ADD NEW DOMAIN	
Θ	_
SAVE AND PUBLISH CANCEL	
PUBLISH CANCEL	

- 9. In the **VPN** window, next to:
  - Custom Configuration XML, enter the following
    - <CustomConfiguration> <ServerCertSN>\*.euclivefire.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

(←) → C <sup>a</sup>				
🖏 Workspace ONE UEM			markus.heinraad@gmail.com	
GETTING STARTED	Users User Groups Administrators	> > >	Devices List View Filters »	DEVICE
			Last Seen 🔺	General Info Mark VMware Virtual Platform Windows Desktop 10.0.18363 e 21 markus.heinraad@gmail.com UEM Managed   Corporate - Dedicated
83 ACCOUNTS			-	Mark VMware7,1 Windows Desktop 10.0.18363 1 8c markus.neinraao@gmail.com UEM Managed   Corporate - Dedicated
APPS & BOOKS			□	Mark Android Android 11.0.0 X5X0 markus.heinraad@gmail.com UEM Managed   Corporate - Dedicated

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

	Device Info		
	Organization Group		
	markus.heinraad@gmail.com		
	Smart Groups		
	All Devices, All Corporate Dedicated Devices, markus.heinraad@gmail.com (Organization Gr		
	Serial Number		
	VMware-42 00 55 e2 d3 d0 85 15-a7 2e a0 cc 6 c1 8c		
	Build Version/Revision Number		
L	Computer Name W10EXT01A OEM		
_			
grant2	TRNEL	Add	•
grant2 Devi	TRNEL	Add	~
grantz Devi Ma	TRNEL s Jun View ark VMware7,1 Windows Desktop 10.0.1	Add	~
grant2 Devi Ma	TRNEL s S Lite Vew ark VMware7,1 Windows Desktop 10.0.1 ##71   1001885   Ownership Corporate - Descase	Add	~
grant2 Devi Mia VMw Summ	TRNEL SES > List View ark VMware7,1 Windows Desktop 10.0.1 ret3   100.18883   Ownering Corporate -Deciceed ry Compliance Profiles Baseline <u>Apps</u> podates Corten	Add : More Y	~
grant2 Devi VMw Summ	TRNEL UIST View ark VMware 7,1 Windows Desktop 10.0.1 ere 7,1   10.1888   Ownership Corporate - Dedicated ary Compliance Profiles Baselin Apps polates Conten allation Status Last Scan. Pricey, November 19, 2021 4:41 PM	Add : More ♥	~
grant2 Devi Mit VMw Summ	TRNEL Ust Ver ark VMware7,1 Windows Desktop 10.0.1 ret31   10.1888   Ownering Corporate -Dedicated ary Compliance Profiles Baseline <u>Apps</u> jodates Corren allation Status Last Scan. Friday, November 19, 2021 4.41 PM	Add : More ↓ App Status	<ul> <li>Inst</li> </ul>
grant2 Devi VMw Summ Inst	TRNEL Ses S Litt View ark VMware7,1 Windows Desktop 10.0.1 sre71   10.1883   Ownersnp:Corporate-Dedicate3 sey Compliance Profiles Baselin Apps polates Conten allation Status Last Scan: Priday, November 19.2021 4:41 PM	Add :: More ↓ App Status @hot masted	Ins: Not

- 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

Run Shut down or sign out
🖾 Run 🛛 🕹
Type the name of a program, folder, document, or Internet Välko resource, and Windows will open it for you.
Open: \\rdsh-01a.euc-livefire.com\corpdocs
\\rdsh-01a.euc-livetire.com\corpdocs
OK Cancel Browse
⊕ Type here to search     O

- 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

@ Run	X X	o
0	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
Open:	mstsc.exe v	
d	OK Cancel Browse	
م 🗄	D Type here to search	

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

- X					
-	Remote Desktop Connection	þ			
Computer: User name: You will be as	tdah-01a.euc-livefire.com EUC-LIVEFIRE\Administrator sked for credentials when you o	connect.	¥		
Show O	ptions	Con	nect	He	lp ql

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

Windows Security X					
Enter your credentials					
These credentials will be used to connect to rdsh-01a.euc- livefire.com.					
EUC-LIVEFIRE\Administrator					
••••••					
Remember me					
More choices					
ОК	Cancel				

- 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

		-			
Q VI	dware Netlink Supervisor Se	rvice			
VMware Scanner Redirection Client					
Whyare Serial Com Redirection Client service					
Q, VI	🤐 VMware Snapshot Provider				
Contract Con					
Q VMware Tools					
WMware USB Arbitration Service					
S VI	Aware Workspace ONE Tuni	nel Service			
🔍 Volume Shadow Copy					
Children Volumetric Audio Compositor Service					
Q, W	Q WalletService				
Q W	🙀 WarpJITSvc				
<u>.</u> w	eb Account Manager				
/					
C Services					
File Action View	Help				
(= =) 🔃 🔄	2 🗟 🚺 🖬 🕨 🔳	II I)			
🔍 Services (Local)	Name	^			
	SVMware Hub Health I	Monitoring Service			
	VMware Snapshot Pro	ovider			
	VMware SVGA Helper	Service			
	UMware Tools				
	WMware Workspace	NIC Towned Consist			
	Q Volume Shadow	Check			
	Volumetric Aud c	Stop			
	WalletService	Pause			
	WarpJITSvc	Resume			
	Web Account Ma	Pertort			
	WebClient	NESLAN			
	Wi-Fi Direct Servi	All Tasks	> vice		
	C Windows Audio	Defrech	_		
	Windows Audio E	Nerresh			
	Windows Backup	Properties			
	Windows Biomet	11sts			
	Windows Camera	нер			
1					
	Windows Connect No	ow - Config Registr	ar		

#### 13. In the Services MMC

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

0	tds 🖏	Srdsh-01a.euc-livefire.com	× +
Resyste Bin de	ethiopan 🗧	$\leftrightarrow$ $\rightarrow$ C (i) rdsh-01a.eu	ic-livefire.com
Scoreje Giorenie	Workspace 0		
			This site can't be reached
Meresself			rdsh-01a.euc-livefire.com refused to connect.
Edge sefexare esti policiu.	Di: Tunnel will a ap		Try: Checking the connection Checking the proxy and the firewall ERR_CONNECTION_REFUSED
			Reload
dethiquid			

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-livefire.com** server.



15. In the **Run** window, next to **Open:** type \\rdsh-01a.euc-livefire.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-livefire.com
  - Retest RDP to RDSH-01a.euc-livefire.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-

## About the author Reinhart Nel

https://www.livefire.solutions/meet-the-team/reinhartnel/

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