

This PDF was generated on September 2023 and was current at the time of download. To check for the latest version please visit
<https://techzone.vmware.com/resource/deploying-vmware-workspace-one-tunnel-workspace-one-operational-tutorial>

Deploying VMware Workspace ONE Tunnel: Workspace ONE Operational Tutorial

VMwareWorkspace ONE

Table of contents

Deploying VMware Workspace ONE Tunnel: Workspace ONE Operational Tutorial	5
Overview	5
Audience	5
Getting Started with Workspace ONE Tunnel	6
Prerequisites	6
Confirm that Tunnel Service is Configured	6
Tunnel Mode (Per-App vs Full Device Tunnel)	7
Per-App Tunnel	8
Full Device Tunnel	8
Supported Platforms	8
Feature availability based on Management Mode and Device Platform	8
Per-App Tunnel Support for MAM Mode Workflow	8
Configuration Requirements for MAM	9
Understanding Device Traffic Rules	10
What are Device Traffic Rules?	10
Server Traffic Rules	10
Device Traffic Rules	10
Device Traffic Rules Wildcard Guidelines and use of asterisk (*)	13
Supported Wildcard and use of asterisk (*)	13
IP and Port Ranges Format Support on Device Traffic Rules	13
Publishing Device Traffic Rules	14
Save and Publish Device Traffic Rules Flow	14
Save Device Traffic Rules Flow	14
Identify the VPN Profile Status (Installed, Not Installed, Pending Install, and Assigned)	14
New Device Traffic Rules Sync Process	15
Trusted Network Detection	17
Trusted Network Detection on Windows Devices	17
Trusted Network Detection based on DNS Suffix	17
Trusted Network Detection Based on Probe URL	17
Trusted Network Detection on Android	18
Next Steps	19
Deploying Workspace ONE Tunnel for iOS	20
High-Level Architecture	20
Prerequisites	20
Configuring Device Traffic Rules for iOS	21
Distributing Workspace ONE Tunnel for iOS	24

Distribute Workspace ONE Tunnel as Public App (Apple Store)	24
Distribute Workspace ONE Tunnel as Purchased App (Apple Business Manager)	27
Creating Per-App VPN Profile for iOS	29
Configuring Workspace ONE Web for Per-App Tunnel	32
Testing Safari Domains with Per-App Tunnel	34
Testing Per-App Tunnel on iOS	36
Troubleshooting the Workspace ONE Tunnel on iOS	37
Deploying Workspace ONE Tunnel for macOS	40
High-Level Architecture	40
Prerequisites	40
Configuring Device Traffic Rules for macOS	41
Distributing Workspace ONE Tunnel for macOS	46
Creating Per-App VPN Profile for macOS	48
Testing Per-App Tunnel on macOS	49
Validate Per-App Tunnel based on Device Rules	50
Extending Tunnel Configuration for Kerberos SSO Extension in macOS	50
.....	51
Validate No Pre-existing Kerberos Tickets	51
Validate Kerberos Application or Website Fails	51
Define the Kerberos Extension in Device Traffic Rules	51
Configure Kerberos Profile Payload	55
Validate Kerberos Tickets	57
Troubleshooting Workspace ONE Tunnel on macOS	59
Ensure Tunnel is Configured	60
Validate Per-App VPN Profile	60
Validate Advanced Tunnel Information	61
Review Tunnel-Related Unified Logging	62
General VPN Network Extension Troubleshooting	63
Deploying Workspace ONE Tunnel for Windows Desktop	64
High-Level Architecture	64
Prerequisites	64
Configuring Device Traffic Rules for Windows	65
Distributing Workspace ONE Tunnel for Windows	71
Creating Per-App VPN Profile for Windows Desktop	79
Custom Configuration XML for Windows Desktop	80
Testing Per-App Tunnel on Windows	82
Launch Internal Website with an Authorized Application	82
Launch Internal Website with an Unauthorized Application	82

Launch a Defined Application to Demonstrate Blocked Domains	83
Test RDP Connections	83
Test SMB Share Connections	84
Troubleshooting Workspace ONE Tunnel on Windows	85
Troubleshoot Workspace ONE Tunnel Installation	85
Troubleshoot Workspace ONE Tunnel Client Connectivity	89
Deploying Workspace ONE Tunnel for Android	94
High-Level Architecture	94
Prerequisites	94
Configuring Device Traffic Rules for Android	95
Distributing Workspace ONE Tunnel for Android	97
Android Considerations	100
Creating Per-App VPN Profile for Android	100
Configuring Workspace ONE Web for Per-App Tunnel	102
Testing Per-App Tunnel on Android	104
Troubleshooting Workspace ONE Tunnel on Android	109
Troubleshoot Device Connectivity	110
Collect Logs Automatically	111
Advanced: Collect Logs Manually on Android	112
Summary and Additional Resources	113
Additional Resources	113
Changelog	113
About the Author and Contributors	114
Feedback	114

Deploying VMware Workspace ONE Tunnel: Workspace ONE Operational Tutorial

Overview

Note: This tutorial was created using Windows 10, but the basic principles and tasks outlined also apply to your deployment of Windows 11.

VMware provides this operational tutorial to help you with your [VMware Workspace ONE®](#) environment. In this tutorial, explore how to configure and deploy the VMware Workspace ONE Tunnel app across iOS, Android, macOS, and Windows platforms to enable Per-App Tunnel on a managed device. Procedures include enable per-app tunneling on managed devices and SDK-enabled applications, configuration of Tunnel policies, deployment of the client and profiles to devices, and general lifecycle maintenance.

Audience

This operational tutorial is intended for IT professionals, network and security administrators, and Workspace ONE administrators of existing production environments. Both current and new administrators can benefit from using this tutorial. Familiarity with networking in a virtual environment, knowledge of Tunnel Service on [VMware Unified Access Gateway™](#) or [VMware Secure Access™](#), and [VMware Workspace ONE® UEM](#) is assumed.

Getting Started with Workspace ONE Tunnel

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 organizations may take a least-privilege approach to enterprise access, ensuring only defined 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 includes client certificates on the allowlist 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:

- Tunnel Service configured in VMware Unified Access Gateway or VMware Secure Access (latest release recommended)
- Workspace ONE UEM 2302 and later
- A device for the platform you plan to use (Windows, macOS, Android, or iOS)

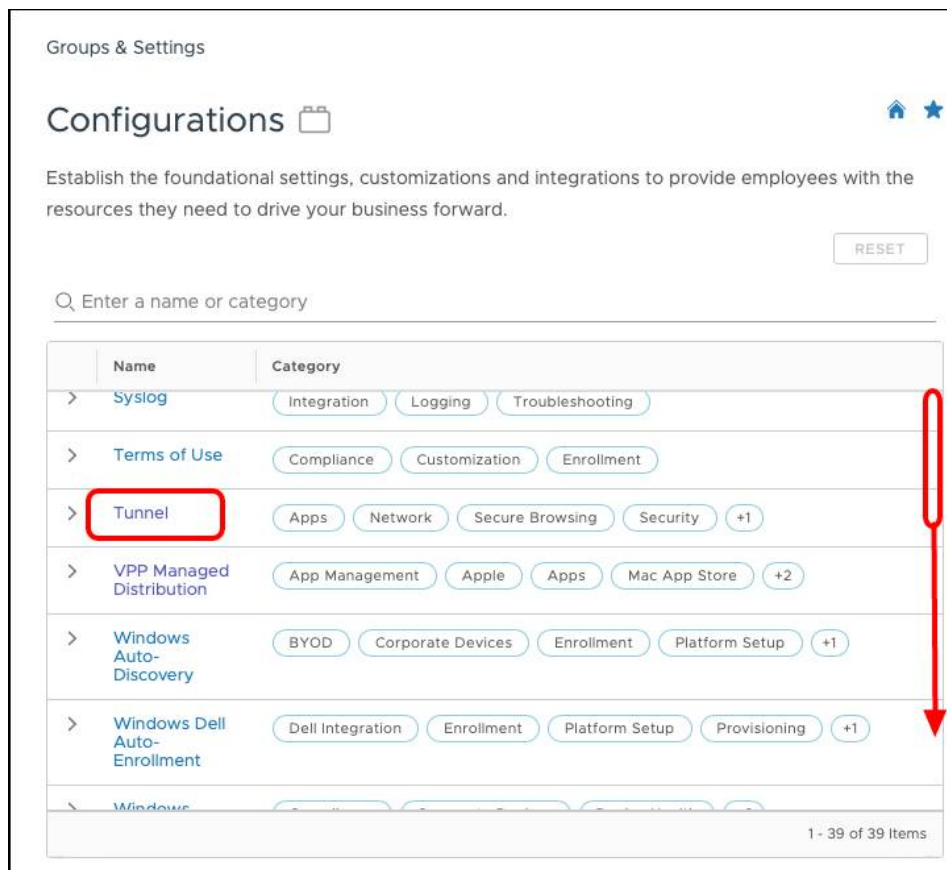
Ensure the following settings are enabled in the Workspace ONE UEM Console:

- Organization Group created and set as Customer Type
- UEM REST API enabled and setting override
- Device Root Certificate issued
- VMware Tunnel configured

Confirm that Tunnel Service is Configured

The remainder of this section assumes that Tunnel Service is properly configured and running on the Unified Access Gateway or on the VMware Secure Access. For more details, see [Configuring the VMware Tunnel Edge Service: Workspace ONE Operational Tutorial](#).

1. In the Workspace ONE UEM console, navigate to **Groups & Settings > Configurations**.
2. Scroll through the list of configurations if necessary and select **Tunnel**.



3. Select **Test Connection** and confirm that both the *Console to AWCM* and *Tunnel to API* tests report **Success** and the Tunnel server reports *service status UP*.

Test Connection

Connection	Status
Console to AWCM	Success
Tunnel to API	Success

[LESS DETAILS](#)

Below table shows the various connections that each Tunnel server in your environment is making for it to be functional.

IP Address	Service Status	Version	API Last Sync Time
	UP	22.12.photon.40	2022-08-23T20:26:17.000

This status confirms that the Tunnel Service is up and running on the server-side, and properly communicating with Workspace ONE UEM.

Tunnel Mode (Per-App vs Full Device Tunnel)

VMware Tunnel provides two modes for tunneling traffic: Per-Application or Full Device. Each mode is configured as part of the Device Traffic Rules and assigned to a device based on the Profile configuration. A device cannot perform Per-App and Device Tunnel at the same time.

Per-App Tunnel

Per-App Tunnel restricts tunnel traffic only to authorized applications and destinations (domain) specified by the UEM administrator when configuring the Device Traffic Rules.

Full Device Tunnel

On Full Device Tunnel configuration, traffic is restricted based on the authorized destinations (domains or IPs), regardless of the application. Full Device mode on Windows requires Workspace ONE Desktop Tunnel 2.1.8+ for all MDM use cases. For standalone enrollment use cases the Workspace ONE Desktop Tunnel version 3.1 is required and will support Per-App and Full Device tunnel mode. Consolidating the MDM and standalone workflows in a unified Windows Tunnel client is on our roadmap.

Supported Platforms

Workspace ONE Tunnel app is available for managed and unmanaged devices providing Per-App and Full Device Tunnel across multiple platforms. Only TCP and UCP traffic will be routed to the Workspace ONE Tunnel App; ICMP-based traffic used by ping utilities is not supported. The Workspace ONE Tunnel app on Windows and macOS platforms now supports Standalone enrollment without Workspace ONE Intelligent Hub or any device management.

Tunnel Mode (Per-App and Full Device) is available based on the device platform and how it is managed as described in the following table.

Feature availability based on Management Mode and Device Platform

Management	Tunnel Mode	Win10	macOS	iOS	Android
UEM Managed	Per-App	✓	✓	✓	✓
	Full Device	✓	✗	✗	✓
Registered Mode (unmanaged)	Per-App	✓	N/A ¹	✓*	✓*
	Full Device	✓	N/A ¹	N/A ²	N/A ²
App Level (MAM/Standalone)	Per-App	✓	✗	✓*	✓*
	Full Device	✓	✓	✓	✓

* Requires use of the Tunnel module (aka Tunnel SDK) available on Workspace ONE SDK.

Standalone method does not require Intelligent Hub; enrollment is done through the Workspace ONE Tunnel App.

N/A1 – Management mode not supported on the specific platform.

N/A2 – Not applicable for the specific Tunnel mode.

For more information, see [Supported Platforms for VMware Workspace ONE Tunnel](#).

For more information on Standalone requirements, see [Configuring VMware Tunnel Client for Standalone enrollment](#).

Per-App Tunnel Support for MAM Mode Workflow

Many organizations do not need to manage devices for their mobile fleets for various reasons, including possible privacy or legal issues. However, they might need to distribute mobile applications to access internal resources, so Workspace ONE UEM offers the flexibility of using a standalone catalog through Intelligent Hub that works independently of the MDM feature.

Applications that leverage the Workspace ONE SDK, such as Workspace ONE Web, can be configured to access internal web applications through Per-App Tunnel. The Workspace ONE Tunnel app is not required for this scenario. Also, organizations that develop mobile internal apps can be integrated with Workspace ONE SDK to enable access from unmanaged devices. Workspace ONE SDK is available on iOS and Android platforms.

In a MAM mode scenario, users do not have to enroll the device as UEM Managed and the Workspace ONE Tunnel app is not required, but rather they can:

1. Use SDK-Enabled apps like Boxer or Web that will manage the registration of the device and be identified as App Level registration on UEM.
2. Use the Intelligent Hub app in registered mode to access the Intelligent Hub catalog part of Workspace ONE UEM. This catalog distributes all application types; public, purchased, internal, and Web. Although end-user devices are not enrolled in MDM, you can access a device record in the Workspace ONE UEM console.

In both cases, the device record is for auditing purposes and the status of these devices in the UEM console displays as App Level (#1) or Hub Registered (#2).

Configuration Requirements for MAM

Settings Global / ACME Corp ▾

- > System
- > Devices & Users
- > Apps
 - > App Scan
 - Workspace ONE Web
 - > Workspace ONE
 - Container
 - Inbox
- > Settings and Policies
 - Security Policies
 - Settings
 - Profiles
 - Microsoft Intune® App Protection Policies
- > Content
- > Email

AirWatch App Tunnel

ENABLED DISABLED ⓘ

App Tunnel Mode VMware Tunnel ▾

Tunnel Proxy for Backwards Compatibility

ENABLED DISABLED ⓘ

Allow all non-FQDN URLs through App tunnel

YES NO ⓘ

Content Filtering

ENABLED DISABLED ⓘ

Geofencing

ENABLED DISABLED ⓘ

Data Loss Prevention

ENABLED DISABLED ⓘ

Network Access Control

ENABLED DISABLED ⓘ

To enable Tunnel for SDK-based apps, navigate to **Groups and Settings > Apps > Settings and Policies > Security Policies** in the Workspace ONE UEM Console.

1. Select **Enabled** to enable the AirWatch App Tunnel.
2. Select **VMware Tunnel** for the App Tunnel Mode.

After that, define the Device Traffic Rules for the iOS and Android SDK-enabled applications which will be covered later as part of this tutorial.

As a reminder, when using the MAM workflow and registered mode using the Workspace ONE Intelligent Hub, the SDK-enabled apps must be deployed through the Intelligent Hub catalog, and the Workspace ONE Tunnel app is not required.

The Workspace ONE Tunnel app can be deployed as a standalone app and perform enrollment without Workspace ONE Intelligent Hub or any device management. In this scenario, Workspace ONE UEM will only contain the device record.

Understanding Device Traffic Rules

This section discusses the two types of network traffic rules—server traffic rules and device traffic rules.

What are Device Traffic Rules?

Network traffic rules allow you to set granular control over how the VMware Tunnel Service directs traffic from devices.

Workspace ONE UEM defines two types of network traffic rules in support of Workspace ONE Tunnel:

- Server Traffic Rules
- Device Traffic Rules

You can create device traffic rules to control how devices handle traffic on the device Per-Application or Full Device.

Server Traffic Rules

The Server Traffic Rules enable you to manage how application traffic is routed throughout your network after traversing the Tunnel Service on Unified Access Gateway infrastructure. Specifically, if you require the use of proxies in your network or for external access, these proxies can be defined and configured as part of Server Traffic Rules.

Configuration of Service Traffic Rules will not be covered in this tutorial. For additional information, see [Configure Server Traffic Rules](#) in VMware Docs.

Device Traffic Rules

The *Device Traffic Rules* define how traffic from specified applications (Per Application) or devices (Full Device) is routed by the Workspace ONE Tunnel application. The device traffic rules serve as a locally enforced Access Control List, defining which apps and destinations should be blocked, tunneled, proxied, or bypass the tunnel completely.

Under Manage Traffic Assignments, administrators can create multiple Device Traffic Rule sets to segment traffic to internal resources, such as rules for employees' devices that are less restricted than access to contractor devices.

- Each traffic assignment (Device Traffic Rule Set) contains multiple rules.
- A profile can only have a single traffic assignment (Device Traffic Rule Set).
- A device can only apply a single VPN profile at any one time.

Manage Traffic Assignments requires Workspace ONE UEM 2011, otherwise, a single Device Traffic Rule set can be created.

Manage Traffic Assignments

Manage the available Device Traffic Rule sets.

ADD

DELETE

	Assignment Name	Number of rules	Default	Tunnel Mode
<input type="radio"/>	Employee basic sites	4	Yes	Per Application
<input type="radio"/>	Contractor only	1	No	Per Application
<input type="radio"/>	Employee extended rules	2	No	Per Application
<input type="radio"/>	IT (Corp Devices)	2	No	Full Device

CLOSE

For each device traffic rule, you must set a Tunnel Mode to determine if traffic will be tunneled Per-Application or Full Device, then defined rules are ranked in order of execution. Multiple device traffic rules can be created and assigned to a profile that uses smart groups to determine the device assignment of the rules.

As an example, in device traffic rules set for Per-Application tunnel mode, every time a specified application is opened, the Tunnel client evaluates the Device Traffic Rule assigned to it before making any routing decisions. If no set rules match the situation, the Tunnel applies the default action. The default action behavior can vary per platform:

- On the iOS platform, the default action set for **all managed applications with tunnel profile associated except for Safari** and applies to domains not mentioned in a rule. If no rules are specified, the default action applies to all domains and all managed applications associated with VPN Profile.
- On the macOS platform, the default action set for **all macOS applications specified on the DTR rules** applies to domains not mentioned in a rule. At least one rule must be defined and when it doesn't match any rule the default action applies to all domains and all macOS applications mentioned above in the Rank.
- On the Windows 10+ platform, the default action set for **all Windows applications specified on the DTR rules** applies to domains not mentioned in a rule. At least one rule must be defined and when it doesn't match any rule the default action applies to all domains and all Windows applications mentioned above in the Rank.
- On the Android platform, the default action set for **all Android managed applications with tunnel profile associated** and applies to domains not mentioned in a rule. If no rules are specified, the default action applies to all domains and all managed applications associated with VPN Profile.

More information about the specifics of device traffic rules per platform will be covered as part of this tutorial in the following chapters.

The device traffic rules help to separate personal and corporate traffic. Think of a scenario where the end-user can check their personal email, visit social media, and so on, without having their personal traffic inspected. We provide privacy where a traditional VPN cannot.

Per-Application Traffic Rules

When configuring the Device Traffic Rules and setting Tunnel Mode to Per Application, the administrator is required to configure the rules per application and domain. These rules will be used by the Workspace ONE Tunnel application to restrict the tunnel traffic only to authorized applications and domains.

Device Traffic Rules

Assignment Name *

Employee basic sites

Tunnel Mode

Per Application

Add rules to Tunnel, Block or Bypass the network traffic using VMware Tunnel

ADD RULE

MANAGE APPLICATIONS

Rank	Application	Action	Destination
1	<div> <div>Safari - iOS</div> <div>Safari - macOS</div> <div>Microsoft Remote Desktop - Android</div> <div>Web - Workspace ONE - Android</div> <div>Web - Workspace ONE - iOS</div> <div>Chrome (64 bit) - WinRT</div> <div>Microsoft Edge - WinRT</div> </div>	TUNNEL	<div> <div>*airwlab.com,</div> <div>*internet.airwlab.com,</div> <div>*vmware.com,</div> <div>*salesforce.com</div> </div>
2	<div> <div>Safari - iOS</div> <div>Web - Workspace ONE - Android</div> <div>Web - Workspace ONE - iOS</div> <div>Chrome (64 bit) - WinRT</div> <div>Microsoft Edge - WinRT</div> </div>	BLOCK	<div> <div>*facebook.com,</div> <div>*match.com,</div> <div>*instagram.com,</div> <div>*cnn.com</div> </div>
3	All Other Apps	BYPASS	*

CANCEL

SAVE

SAVE AND PUBLISH

Note the following:

1. Tunnel Mode for the Device Traffic Rules Set.
2. Per-Application Rules.
3. Default Action Rule that will be performed when the client traffic doesn't match rules 1 and 2.

Full Device Traffic Rules

When the Tunnel Mode is set to Full Device, traffic is restricted based on the domains specified in the rules. Note: You cannot configure applications as part of this rule.

Full Device mode requires Workspace ONE UEM 2102+, Workspace ONE Desktop Tunnel 2.1+, and it is available only on Windows 10+.

Device Traffic Rules

Assignment Name
IT (Corp Devices)

Tunnel Mode
Full Device

Add rules to Tunnel, Block or Bypass the network traffic using VMware Tunnel

ADD RULE

Rank	Action	Destination
1	TUNNEL	*airwlab.com, *salesforce.com, *force.com, *vmware.com, *login.microsoftonline.com, *office.com, *espn.com
2	BLOCK	*facebook.com, *match.com, *instagram.com, *cnn.com
3	BYPASS	*

CANCEL SAVE

Note the following:

1. Tunnel Mode for the Device Traffic Rules Set.
2. Full Device Rules.
3. Default Action Rule that will be performed when the client traffic doesn't match rules 1 and 2.

Device Traffic Rules Wildcard Guidelines and use of asterisk (*)

When defining the Device Traffic Rules destination, the administrator can enter a list of domains to allow, block, or bypass traffic. The wildcard is supported for the hostnames and multiple entries must be separated by comma (,).

Supported Wildcard and use of asterisk (*)

You can use wildcard characters for your hostnames. Wildcards must follow the format:

- *.<domain>.*
- *<domain>.*
 - Includes primary domain and subdomains - for example, www.example.com, example.com, store.example.com
- *.* — You cannot use this wildcard for Safari domain rules (iOS and macOS specific)
- — You cannot use this wildcard for Safari domain rules (iOS and macOS specific)

IP and Port Ranges Format Support on Device Traffic Rules

Use of IPs and port ranges are only supported for Device Traffic Rules on Windows 10+ devices. The following list contains supported formats for the IPv4 & Port range when applying the Device Traffic Rules (DTR).

1. Single IP
 - a. 10.10.0.1 or 10.10.10.1/32
2. IP range or subnet
 - a. 10.10.10.1/24
 - b. 10.10.0.0/16
3. Single Port
 - a. *.example.com:80, 10.10.10.1:80, 10.10.11.1/32:80

- b. *.example.com:[443], 10.10.11.1/24:[443]
- 4. Port Range
 - a. *.example.com:[80-443], 10.10.10.1:[80-443],10.10.11.1/32:[80-443]
 - b. 10.10.11.1/24:[80-443]
- 5. List of Ports
 - a. *.example.com:[80,443], 10.10.10.1:[80,443],10.10.11.1/32:[80,443]
 - b. 10.10.11.1/24:[80,443]
- 6. List of Ports and Ranges
 - a. *.example.com:[80,443, 8080-8085], 10.10.10.1:[80,443,8080-8085],10.10.11.1/32:[80,443,8080-8085]
 - b. 10.10.11.1/24:[80,443,8080-8085]

Publishing Device Traffic Rules

When making changes to the Device Traffic Rules those need to be sent to the device to take effect, this process requires synchronization between device and UEM, and can be applied to existing managed devices or only new enrolled devices. This chapter describes the difference between *Save* and *Save and Publish* device traffic rules set, in addition to how the changes will be sent to the device.

Save and Publish Device Traffic Rules Flow

When the administrator changes the Device Traffic Rules and clicks **Save and Publish**, an updated version of the VPN profile mapped to the Device Traffic Rules will be created and queued for all the assigned devices. That process will reissue the client certificate as part of the profile to the device with a new thumbprint.

The Tunnel client app might not be able to establish a connection with Tunnel Service until the new VPN profile gets installed on the device. Forcing a sync on the device can speed up the profile installation but in environments with a large number of devices, this process can take additional time.

The **Save and Publish** option is only available on the default Device Traffic Rules set.

Save Device Traffic Rules Flow

When the administrator changes the Device Traffic Rules set and clicks **Save**, the Device Traffic Rules get mapped to the profile, but the updated Device Traffic Rules are not replaced for the devices where the VPN profile is already installed. Device Traffic Rules are only updated for the newly enrolled devices or for the devices that have the VPN profile reinstalled.

Save is the only option available for a non-default Device Traffic Rules set - this means that after you change the device traffic rule set and hit save, you must push a new version of the VPN profile to current devices where the profile was already deployed.

Identify the VPN Profile Status (Installed, Not Installed, Pending Install, and Assigned)

As mentioned previously, publishing a device traffic rule or changes on the VPN Profile will create a new profile version and queue it to all assigned devices. The tunnel client might not be able to establish a connection with the Tunnel Service until the new profile comes down to the device. The administrator can monitor the deployment status of the new VPN profile with the following steps:

Locate the VPN profile under the Resources / Profiles & Base Lines / Profiles and click the View link to identify the total number of profiles not installed, installed and assigned. Click the Not Installed hyperlink to push the profile manually.

Locate the device under the Devices / List View, select the Profile page and point to the Profile Status. Selecting the profile allows you to send a command to remove or install the profile on the respective device.

The screenshot shows the Workspace ONE UEM console interface. The left sidebar contains navigation options like Dashboard, List View, Details View, Lifecycle, Compliance Policies, Certificates, Provisioning, Peripherals, and Devices Settings. The main content area displays the 'Details View' for a device named 'jdoe iPad iOS 14.6.0 GHKK'. The 'Profiles' tab is selected and highlighted with a red box. Below the tabs, a table lists the profiles installed on the device. The 'Per App Tunnel iOS' profile is highlighted with a red box and has a 'Pending Install' status.

Status	Profile Details	Organization Group	Configuration Type	Assignment Type
✓	Cloud Web Security Cert - Apple	ACME Corp	Device	Automatic
✗	Enterprise Wifi	ACME Corp	Device	Optional
✓	iOS Security Restrictions	ACME Corp	Device	Automatic
⚙	Per App Tunnel iOS	ACME Corp	Device	Automatic
✓	Single Sign On configuration	ACME Corp	Device	Automatic

New Device Traffic Rules Sync Process

A new process to sync Device Traffic Rules (DTR) will be implemented on the Workspace ONE Tunnel App to minimize the push of the Tunnel profile to the device every time the DTR changes. This new process, as of today, is only available for Android and requires Workspace ONE UEM 2209+ and Workspace ONE Tunnel version 2209.

The new process requires you to enable the Workspace ONE Tunnel client to request the DTR from a Tunnel API endpoint (hosted on UEM) automatically on every launch or every 4 hours (default). The new Tunnel API endpoint is identified as <http://ws1-api-server/DevicesGateway/devices/{deviceuuid}/tunnel/{tunnelconfiguuid}/configuration?device-traffic-rule-set-uuid={dtr-set-uuid}> (TunnelConfigurationSyncEndpointUrl) and is invoked by the Workspace ONE Tunnel client to obtain the new DTR.

- By default, the client syncs DTR every 4 hours.
- This value can be changed via the **client_sync_interval** key in Custom Settings on the Tunnel Configuration Page. The value is specified in **minutes**.

Workspace ONE Tunnel client would reach the TunnelConfigurationSyncEndpointUrl on every launch, so modifying the `client_sync_interval` is not recommended unless you have a critical use case. The following table provides the sync interval recommendation based on the number of devices enrolled.

Number of devices in the environment	Sync Interval
1 - 50,000	15 minutes
50,000 - 100,000	30 minutes
100,000 - 200,000	60 minutes
200,000 - 500,000	120 minutes
500,000 - 1,000,000	240 minutes

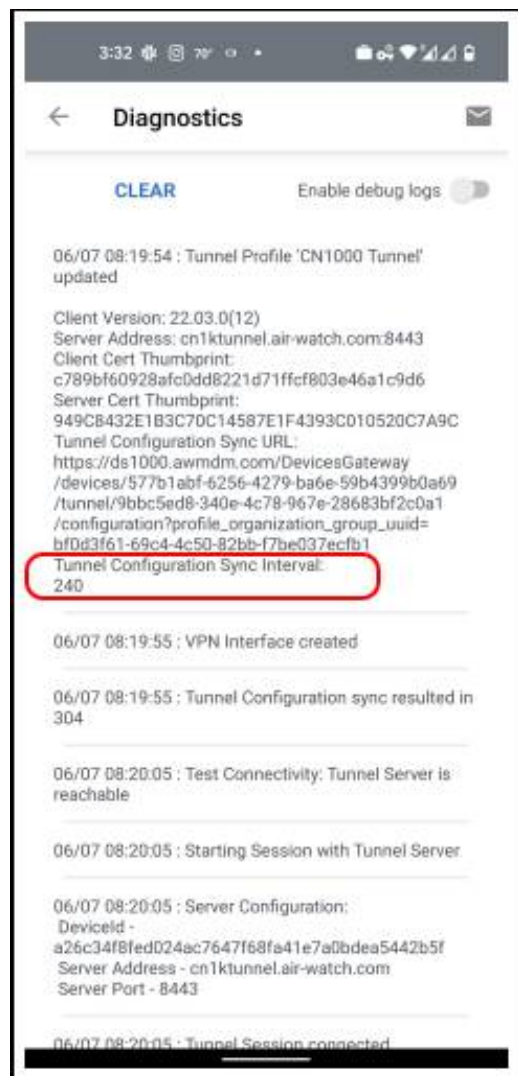
To verify if the tunnel client can sync with the endpoint, open the Diagnostics UI.

Tunnel Client Codes in the UI:

- 200 - DTR was modified in UEM and successfully synced.

- 304 - sync triggered but no changes in DTR.
- 204 - sync triggered but admin has possibly deactivated FF and has not republished the profile to remove sync settings.

To ensure that the client received the settings, the Diagnostics UI displays the Sync Interval and Sync URL as well.



Trusted Network Detection

Trusted Network Detection is a mechanism in the Workspace ONE Tunnel app that determines whether to establish a connection with the Tunnel Service to tunnel access to corporate applications. If the device is connected to the corporate network and trusted network detection is configured, the Workspace ONE Tunnel app does not tunnel traffic to the corporate applications.

When setting up a Trusted Network Detection in UEM Tunnel Configuration, routing is dependent on DNS and will ignore HOSTS file entries.

Currently, Trust Network Detection is supported on Windows 10+ and Android platforms.

Trusted Network Detection on Windows Devices

For Windows 10+ devices, Trusted Network Detection is configured as part of the Per-App VPN payload, and can be configured leveraging DNS suffix or internal URL (probe URL).

Trusted Network Detection based on DNS Suffix

When using DNS suffix, Workspace ONE Tunnel compares the DNS suffix defined on the device against the list of trusted networks configured on the Trusted Network Detection field to determine if the device is on the trusted network or not.

Administrators can add a list of domains separated by a comma into the Trusted Network Detection field (see the following screenshot) and that will leverage DNS suffix. Workspace ONE Tunnel fails to connect when the device is on a trusted network.

The screenshot displays the 'VPN' configuration page. Under the 'Connection Info' section, the 'Connection Name' is 'Per App Tunnel (Windows)', 'Connection Type' is 'Workspace ONE Tunnel', 'Server' is 'ws1.sa.gsm.vmware.com:443', and 'Device Traffic Rules' is 'Corporate (Windows)'. The 'Desktop Client' has 'ENABLE' and 'DISABLE' buttons. The 'Custom Configuration' section has a 'Custom Configuration XML' field. The 'Trusted Network Detection' field is highlighted with a red box and contains the text 'airwlab.com'. Below this, the 'DNS Resolution via Tunnel Gateway' section has an 'Enhanced Domain Resolution' section with 'ENABLE' and 'DISABLE' buttons.

Trusted Network Detection Based on Probe URL

When using Probe URL (recommend method), Workspace ONE Tunnel will make HTTP calls against the list of private URLs defined in the custom configuration probe URLs to determine if the device is on the trusted network or not.

Administrators can add a list of domains separated by a comma into the Custom Configuration XML field (see the following screenshot) using the `TrustedNetworkProbeUrl` XML tag. Workspace ONE Tunnel fails to connect when the device is on a trusted network.

VPN

Connection Info

Connection Name *

Connection Type *

Server *

Device Traffic Rules

Desktop Client ⓘ

Custom Configuration

Custom Configuration XML

```
<?xml version="1.0" encoding="utf-16"?>
<CustomConfiguration>
<TrustedNetworkProbeUrl>https://probeurl.airwlab.com,
http://probeurl2.airwlab.com</TrustedNetworkProbeUrl>
</CustomConfiguration>
```

 ⓘ

Trusted Network Detection ⓘ

DNS Resolution via Tunnel Gateway

Enhanced Domain Resolution ⓘ

Trusted Network Detection on Android

For Android devices, Trusted Network Detection is configured on the Workspace ONE Tunnel app through App Config, using the `TrustedNetworkProbeUrl` key, and the value is a list of URLs separated by a comma that can optionally have http/https scheme and an assigned port.

Format examples:

- `<internal-site>`
- `<internal-site>:<port>`
- `http://<internal-site>`
- `http://<internal-site>:80`
- `https://<internal-site>`
- `https://<internal-site>:443`

Workspace ONE Tunnel app for Android determines if the device is on the internal network based on the device's ability to reach the private URLs defined as part of the `TrustedNetworkProbeUrl`.

Tunnel - Workspace ONE - Assignment

- ✓ Distribution
- ✓ Restrictions
- Application Configuration**

Application Configuration

EMM Managed Access

Only devices enrolled in EMM will be allowed to install the app and receive policies below.

Managed Access ☒

Send Configuration ☒ ⓘ

PrivacyPolicyLink ⓘ

DisplayPrivacyDialog ⓘ

PolicyAllowFeatureAnalytics ⓘ

PolicyAllowCrashReporting ⓘ

DisplayWelcomeScreen ⓘ

CustomSettings ⓘ

TrustedNetworkProbeUrl ⓘ

FilterDiagnosticsView ⓘ

Next Steps

The procedures in this tutorial consist of the following:

- Device Traffic Rule configuration
- Deployment of Per-App VPN Profile
- Deployment of Workspace ONE Tunnel Client
- Testing configurations on the chosen device

The procedures are almost the same for each platform. To ensure you understand any existing particularity and stay focused on the platform of your choice, the following steps in this tutorial are organized per platform.

- [Deploying Workspace ONE Tunnel for iOS](#)
- [Deploying Workspace ONE Tunnel for macOS](#)
- [Deploying Workspace ONE Tunnel for Windows Desktop](#)
- [Deploying Workspace ONE Tunnel for Android](#)

Deploying Workspace ONE Tunnel for iOS

Per-App Tunneling helps users to access critical information using applications on their devices from their devices. Mobile flows help users perform business-critical tasks from a single app — streamlining the user experience.

Leveraging Per-App Tunnel allows you to control which applications are on a device and what internal resources the applications have access to by automatically activating or deactivating Per-App VPN access, based on which applications are active. By enabling remote access, you no longer need to provide a device-wide VPN on your devices, which can allow unintended or unauthorized apps or processes to access your VPN. In this tutorial, you configure and deploy VMware Workspace ONE Tunnel to enable the Per-App Tunnel component on managed devices.

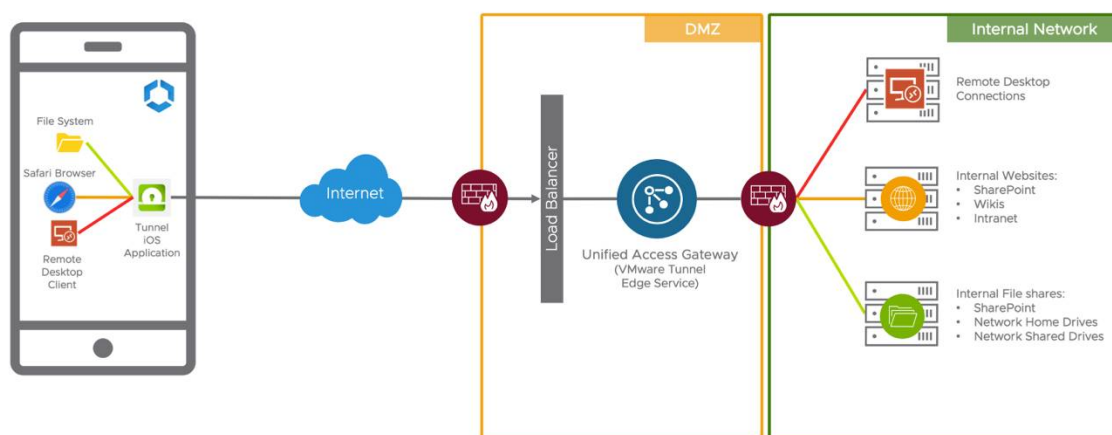
These exercises involve the following components:

- **Workspace ONE Tunnel** - The app used on the device to securely connect to the Unified Access Gateway to provide Per-App Tunnel functionality, also referred to as Tunnel Client.
- **Unified Access Gateway** - The virtual appliance where the VMware Tunnel edge service is installed, and to which the tunnel client connects.
- **Per-App Tunnel** - Component of VMware Tunnel edge service for connecting to a secure tunnel channel on a per-application basis, which is controlled and configured by the VPN profile payload and Device Traffic Rules.
- **Per-App VPN Profile and Device Traffic Rules** - The Workspace ONE UEM configuration is pushed to the device that contains the Per-App Tunnel configurations. Every time a specified application is opened, the Workspace ONE Tunnel client evaluates the Device Traffic Rules assigned to it before making any routing decisions and establishes a Per-App tunnel connection with the Unified Access Gateway based on the Per-App VPN Profile configuration.

High-Level Architecture

Workspace ONE Tunnel iOS Application

Example of Per-App VPN Remote Access



The device contains the applications required by the end-user to perform their daily job. Some applications require access to internal resources to function. Those applications, based on Per-App VPN configuration, use Workspace ONE Tunnel which communicates with the Tunnel Service on Unified Access Gateway hosted on the DMZ, to validate if the device requesting access is in compliance or not before authorizing access through the internal resource.

Prerequisites

Before you can configure the Per-App Tunnel component for iOS, you must have the following components installed and configured:

- Workspace ONE UEM version 2011 and later
- iOS 10.3+ device enrolled in Workspace ONE UEM

- VPN Tunnel must be configured before you can add it as an application
- Workspace ONE Tunnel application for iOS
 - Deploy Workspace ONE Tunnel using volume purchased licenses from Apple Business Manager or Apple School Manager.
 - Workspace ONE Administrators must upload the Location token from Apple Business Manager to sync licenses to Workspace ONE UEM for managed distribution.

Configuring Device Traffic Rules for iOS

First, because Apple's Mail, Calendar, and Contacts applications may contain both corporate and personal data, administrators must take an extra step to define corporate-owned domains which should be marked for Per-App Tunnel.

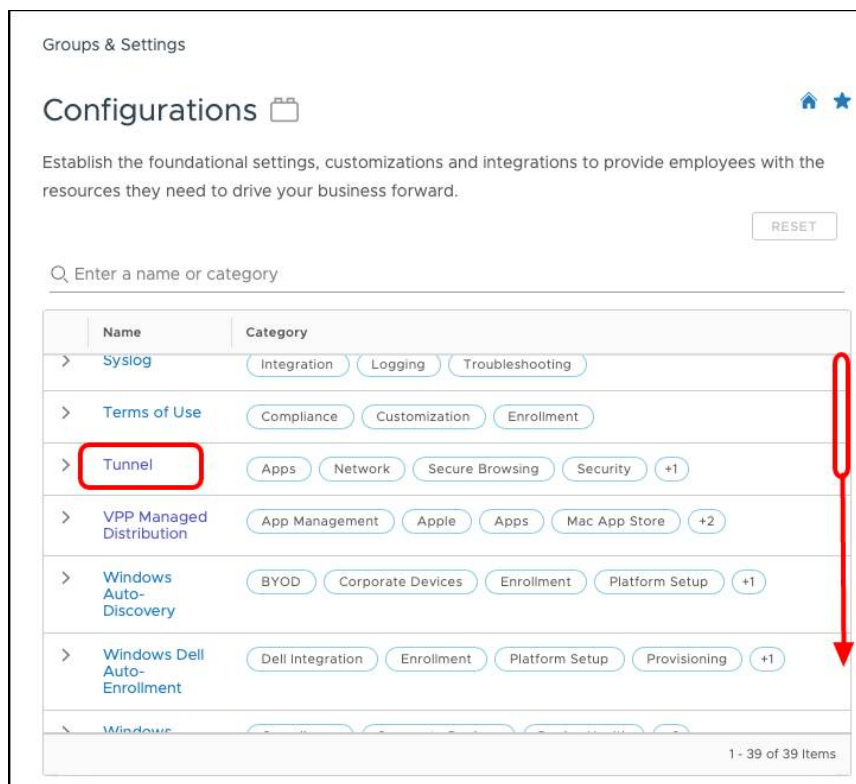
Device traffic rules provide a centralized location to configure which domain traffic uses per-app tunneling. When a Workspace ONE administrator configures devices for Safari on iOS, Workspace ONE automatically merges these parameters into the VPN payload sent to iOS devices. These parameters allow the VMware Tunnel edge service to apply the appropriate device traffic rules for those specific domains.

Second, Safari is another app that may be used for personal use on a corporate device. As such, Safari cannot be configured to tunnel all traffic. Device traffic rules for Safari must specify the domain and top-level domain component (for example, `vmware.com`) although an asterisk (*) may be used to wildcard subdomains (for example, `*.vmware.com`).

Note: Domain values used in this section are examples only. Your values will differ.

In the Workspace ONE UEM console:

1. Navigate to **Groups & Settings > Configurations**.
2. Select **Tunnel**.



3. From the Device Traffic Rules tile, click **Edit**.
4. Click **Add** or the **Default** assignment to manage the device traffic rules.
Administrators can create multiple Device Traffic Rules that will be assigned to the Per-APP VPN profile and will deploy to the devices based on the smart group assigned to the Profile. The first device traffic rule assignment created will be set as default.

Manage Traffic Assignments

Manage the available Device Traffic Rule sets.

ADD DELETE

	Assignment Name	Number of rules	Default	Tunnel Mode
<input type="radio"/>	Default	0	Yes	Per Application

CLOSE

5. Observe the default device traffic rule.

Device Traffic Rules

Assignment Name: **Default**

Tunnel Mode: Per Application

BYPASS

Add rules to Tunnel, Block or Bypass the network traffic using VMware Tunnel

ADD RULE MANAGE APPLICATIONS

Rank	Application	Action	Destination
1	All Other Apps	BYPASS	

CANCEL SAVE SAVE AND PUBLISH

1. Update the Assignment Name with the name of your choice.
2. Observe (or modify) the default action which applies to all iOS applications selected to use Per-App VPN **except Safari**:
 - i. **Tunnel** – All apps, except Safari, on the device configured for Per-App Tunnel send network traffic through the tunnel. For example, set the Default Action to Tunnel to ensure all configured apps without a defined traffic rule use the Workspace ONE Tunnel for internal communications.
 - ii. **Block** – Blocks all apps, except Safari, on the device configured for Per-App Tunnel from sending network traffic. For example, set the Default Action to Block to ensure that all configured apps without a defined traffic rule cannot send any network traffic regardless of destination.
 - iii. **Bypass** – All apps, except Safari, on the device configured for Per-App Tunnel bypass the tunnel and connect to the Internet directly. For example, set the Default Action to Bypass to ensure all configured apps without a defined traffic rule bypass the Workspace ONE Tunnel to access their destination directly.
 - iv. **Proxy** – Redirect traffic to the specified HTTPS proxy for the listed domains. The proxy must be HTTPS and must follow the correct format: <https://example.com:port>.

3. Click **ADD RULE**.

6. Build the device traffic rule.

Add rules to Tunnel, Block or Bypass the network traffic using VMware Tunnel

[ADD RULE](#) [MANAGE APPLICATIONS](#)

Rank	Application	Action	Destination
1	<div> <input checked="" type="checkbox"/> Safari - iOS <input type="checkbox"/> Safari - macOS <input type="checkbox"/> AirWatch Container - iOS <input type="checkbox"/> AirWatch Learn - iOS <input checked="" type="checkbox"/> Web - Workspace ONE - iOS <input type="checkbox"/> Android workspace - Android <input type="checkbox"/> AirWatch Secure Browser - And... <input type="checkbox"/> AirWatch Email Client - Android <input type="checkbox"/> All Applications </div>	TUNNEL	*.aapp..weuc.com, *.weuc.com

[CANCEL](#) [SAVE](#) [SAVE AND PUBLISH](#)

1. Click the drop-down for the *Applications* list. Alternatively, select **All Applications** to apply the rule to all iOS applications listed in the drop-down, which are the ones that you assigned the Per-App VPN profile.
2. Select one or more iOS apps for which this rule applies.
3. Enter one or more destinations to control via Workspace ONE Tunnel.
4. Select the Action to apply for the selected apps when they attempt to access the specified destinations.

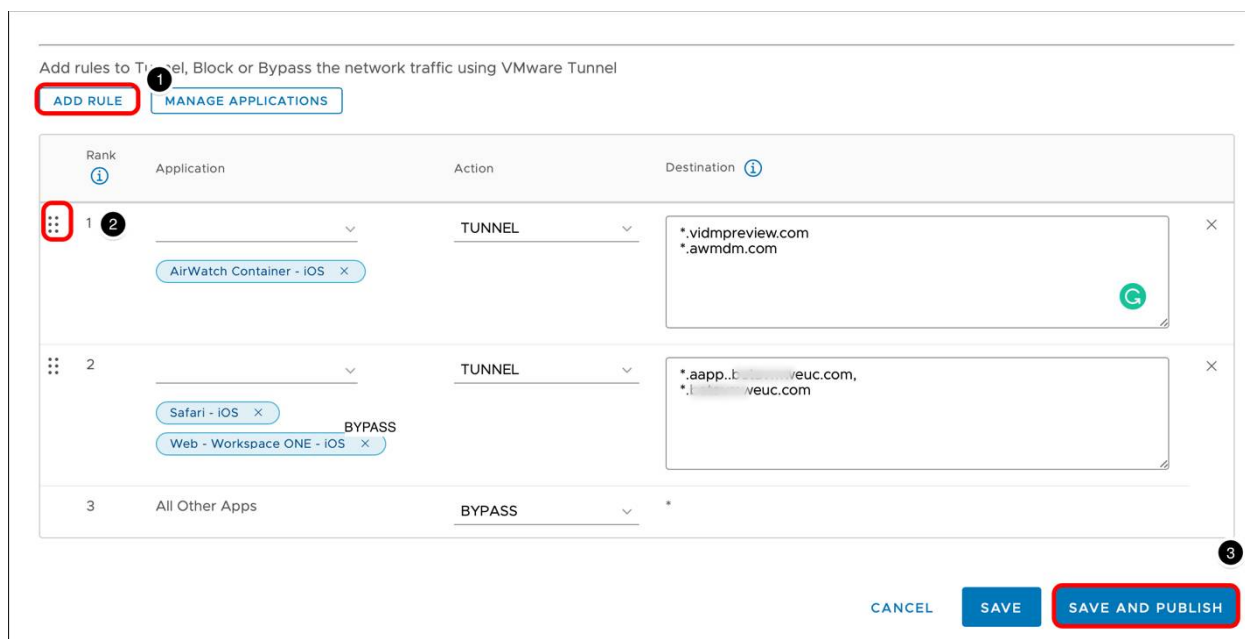
For more information on the formats (wildcards, IP, ports) allowed into the Destination field, see the *Device Traffic Rules Destination formats supported* chapter.

Tip: iOS apps are automatically added to the *Applications* selection list after you enable an application for Per-App Tunnel when creating assignments in Resources.

Note: Wildcards must follow one of these formats:

- *.<domain>.*
- *<domain>.*
- *.* — You cannot use this wildcard for Safari rules.
- * — You cannot use this wildcard for Safari rules.

7. Add additional rules and publish.



1. Click Add Rule and repeat step 6 for any additional required rules.
2. Drag the rules to adjust your Device Traffic Rules priority.
3. After the Device Traffic Rules are configured as necessary, click Save and Publish.

Distributing Workspace ONE Tunnel for iOS

Workspace ONE Tunnel is an iOS application available for free on the App Store. It is also available for managed distribution volume licensing through Apple Business Manager and Apple School Manager. In both cases, the Workspace ONE Tunnel app can be deployed over-the-air through Workspace ONE UEM as a:

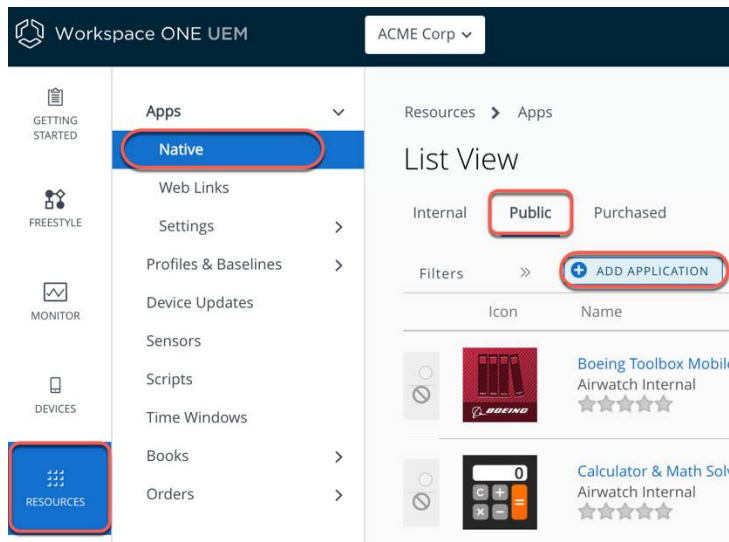
- **Public App** - this method pushes the application to the device from App Store and is recommended when your organization doesn't use Apple VPP program.
- **Purchased App** - Workspace ONE Tunnel app is free, however, it is also available for managed distribution volume licensing through Apple Business Manager and Apple School Manager. Use device-based licensing to distribute Workspace ONE Tunnel to corporate-managed iOS devices. If your organization has access to Apple Business Manager and you want to manage the license distribution, use this method.

This section demonstrates how to obtain Workspace ONE Tunnel and assign it to devices as Public or Purchased App.

Note: The VPN tunnel profile should already be configured as part of the Prerequisites.

Distribute Workspace ONE Tunnel as Public App (Apple Store)

1. Add Workspace ONE Tunnel as public app.



- a. In the Workspace ONE UEM console, navigate to **Resources > Native > Public > Add Application**.
2. Search for Workspace ONE Tunnel on the Apple store.

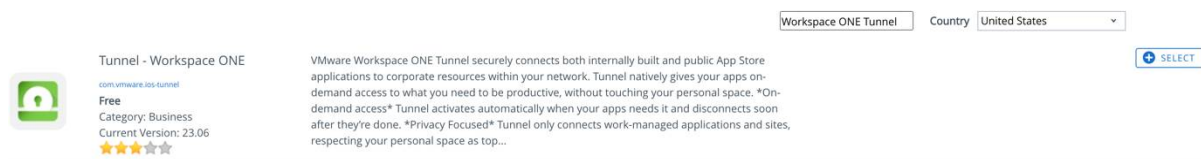
Managed By

Platform*

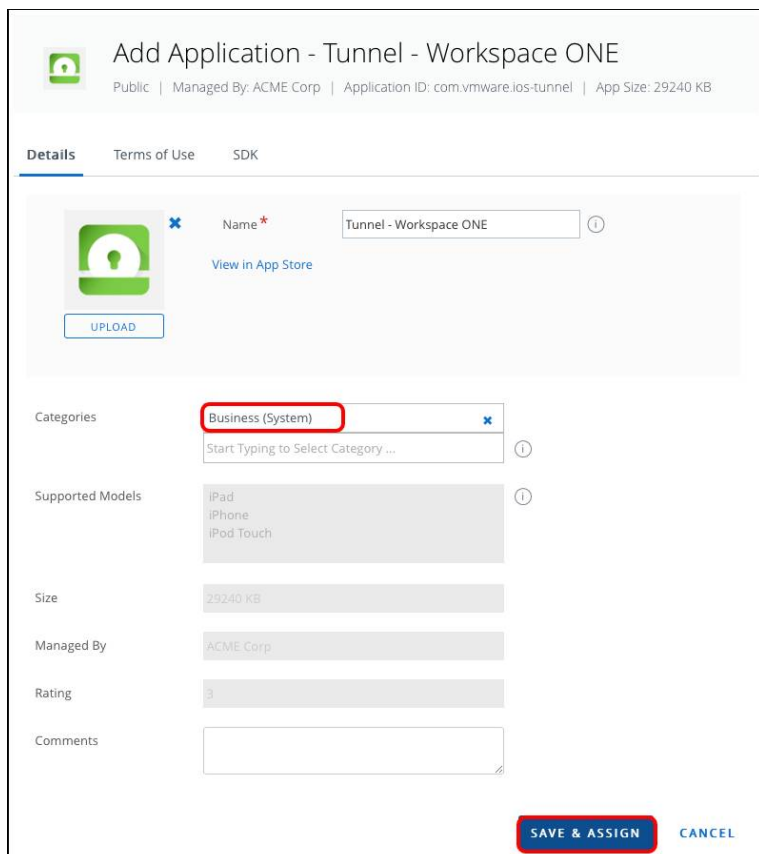
Source

Name*

- a. Select **Apple iOS** as Platform.
 - b. Select **Search App Store** for Source.
 - c. Enter **Workspace ONE Tunnel**.
 - d. Click **Next**.
3. From the search result, click **select** for Tunnel – Workspace ONE.



4. Save and add the assignment.



Add Application - Tunnel - Workspace ONE
Public | Managed By: ACME Corp | Application ID: com.vmware.ios-tunnel | App Size: 29240 KB

Details | Terms of Use | SDK

Name * Tunnel - Workspace ONE ⓘ

Categories Business (System) ⓘ

Supported Models iPad, iPhone, iPod Touch ⓘ

Size 29240 KB

Managed By ACME Corp

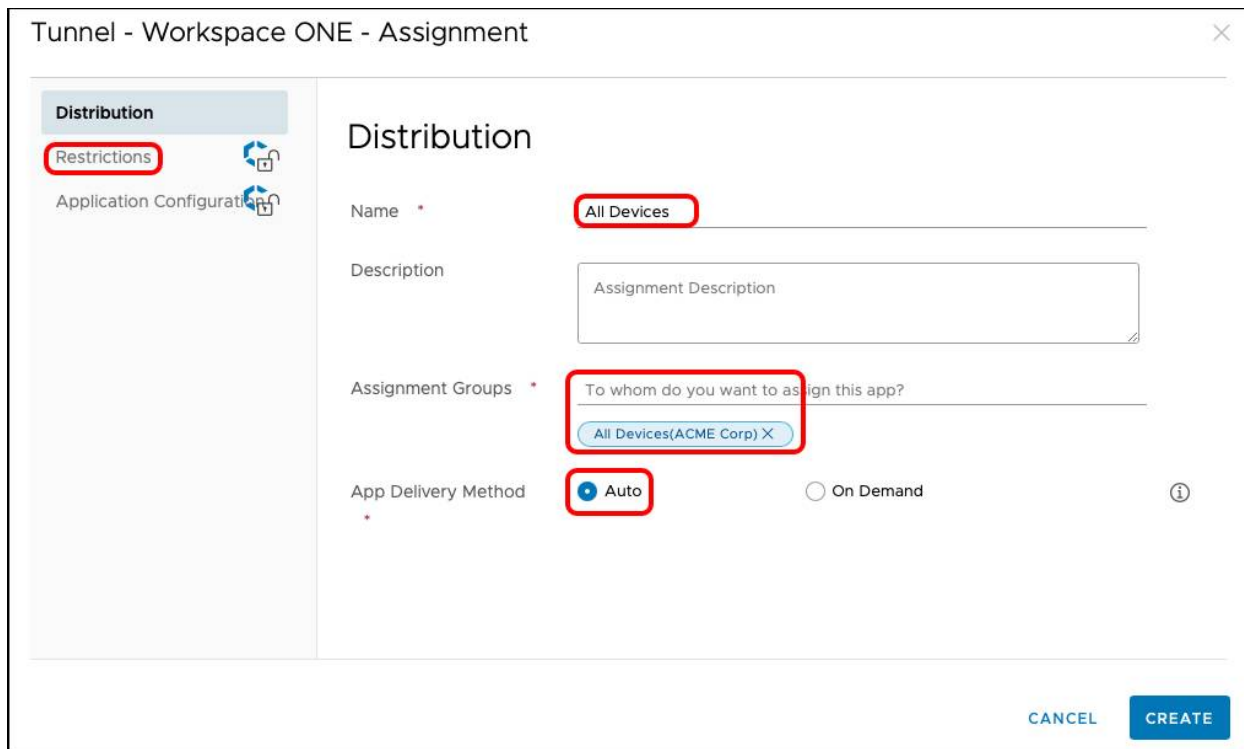
Rating 3

Comments

SAVE & ASSIGN CANCEL

- Select **Business (System)** for the Categories; this is not required; however it will show the Tunnel app under the specific category in the Intelligence Hub Catalog.
- Click **Save & Assign**.

5. Define the Assignment.



Tunnel - Workspace ONE - Assignment

Distribution

Restrictions ⓘ

Name * All Devices ⓘ

Description Assignment Description ⓘ

Assignment Groups * To whom do you want to assign this app?
All Devices(ACME Corp) X ⓘ

App Delivery Method * Auto ⓘ On Demand ⓘ

CANCEL **CREATE**

Tunnel - Workspace ONE - Assignment

✓ Distribution

Restrictions

Application Configuration

Restrictions

EMM Managed Access Hide ^

EMM managed access defines which devices will be able to install this app from Intelligent Hub.

If this setting is disabled, all registered devices will be able to install this app.

If this setting is enabled:

- Only EMM managed devices will be able to install this app.
- If this app is secured by Workspace ONE SDK version 20.10 or later, access will be blocked unless the app is managed by EMM. To ensure this app is managed, enable the setting 'Make App MDM Managed if User Installed' on the Restrictions tab.

Managed Access ☐

Remove On Unenroll ☐ ⓘ

Prevent Removal ☐ ⓘ

Prevent Application Backup ☐ ⓘ

Make App MDM Managed if User Installed ☒ ⓘ

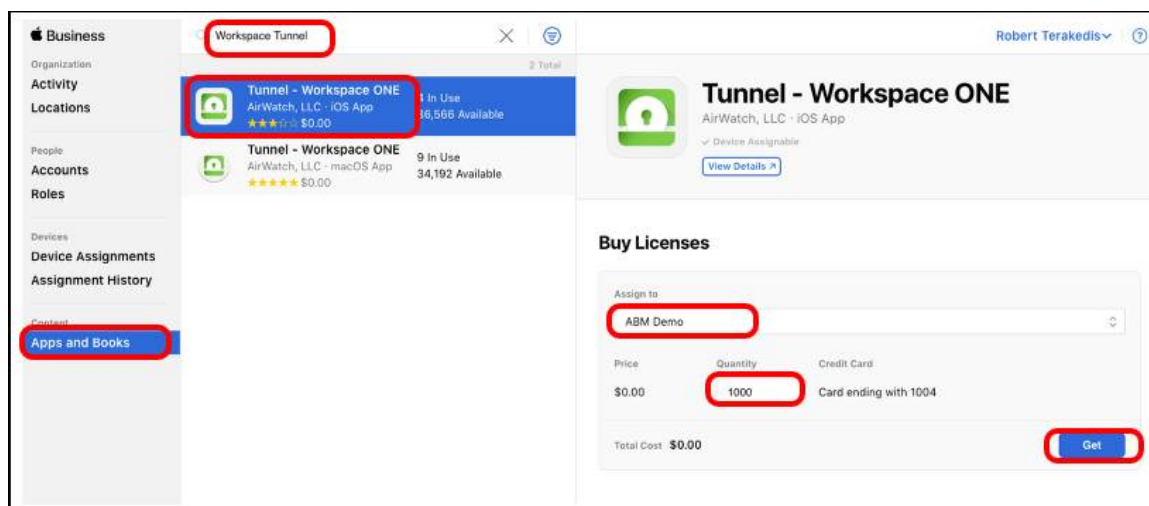
CANCEL CREATE

- Enter **All Devices** for Name.
- Select **All Devices** for Assignment Groups or a specific group of devices that you want to target for the tunnel deployment.
- Select **Auto** for App Delivery Method.
- Click **Restrictions**.
- Turn **ON** the Make App MDM Managed if User Installed.
- Click **Create**.

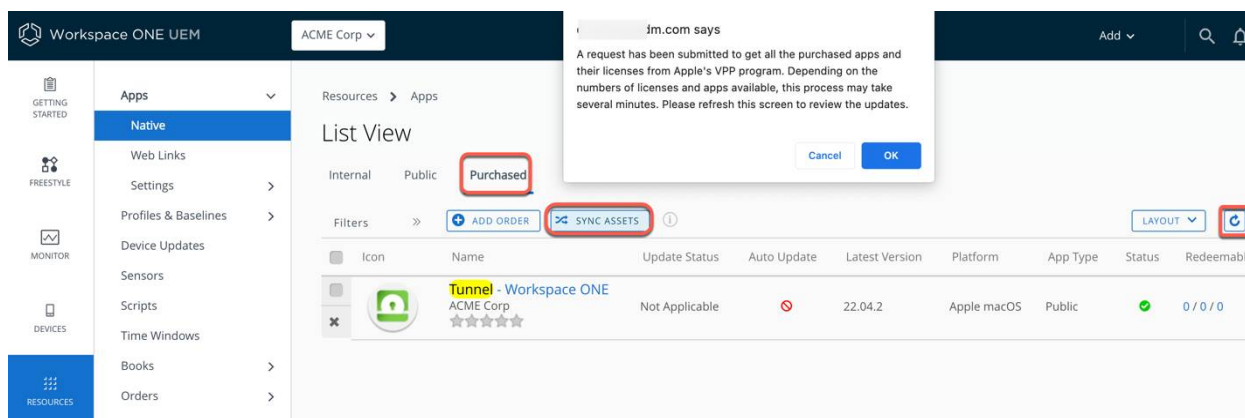
6. Click **Save**, and then click **Publish**.

Distribute Workspace ONE Tunnel as Purchased App (Apple Business Manager)

- Get Workspace ONE Tunnel licenses.



- In Apple Business Manager (or Apple School Manager), click **Apps and Books**.
 - Search for *workspace tunnel* in the search text box.
 - Select **Tunnel - Workspace ONE** for iOS.
 - Select the location for which you have uploaded the sToken into Workspace ONE UEM.
 - Enter the quantity of licenses you want to purchase.
 - Click **Get**. The button changes to *Purchasing* and when the purchase is complete changes back to *Get*.
- Sync assets in Workspace ONE UEM.



- In the Workspace ONE UEM console, click **Resources**.
 - Expand **Apps** and click **Native**.
 - Select **Purchased**.
 - Click **Sync Assets**.
 - Click **OK** on the dialog box.
 - Wait a few moments and click **Refresh** to update the app list.
 - Click the **Workspace ONE Tunnel app for iOS** in the app list.
- Enable device assignment.
 - Click **Enable Device Assignment**.
 - Click **OK** to confirm device-based licensing.
 - Click **Save & Assign**.
 - Click **Add Assignment**.
 - Edit Assignment.

Tunnel - Workspace ONE - Edit assignment [X]

Assignment

Assignment for License Codes can be done by Smart Groups only

Active	Assignment Group (Smart Group)	Devices	Allocated	Redeemed
<input checked="" type="radio"/>	All Devices @ TM-Apple	0	100	0

License Codes By Smart Group

Create New Smart Group

+ Add Assignment

Deployment

Assignment Type* **AUTO** **ON DEMAND** ⓘ

SAVE **CANCEL**

License Summary

- Total: 1000
- On Hold: 0
- Allocated: 100
- Unallocated: 900
- Redeemed: 0

- a. Click **Add Assignment**.
- b. Select an Assignment Group (or alternatively, create a new smart group containing the targeted devices).
- c. Enter a number of licenses to allocate. Allocate up to the total number of unallocated licenses.
- d. Select **Auto**.
- e. Click **Save**.
6. Save Assignment.
 - a. If more assignments are necessary, click Add Assignment and repeat the steps in [Edit Assignment](#).
 - b. Click Save and Publish, then click Publish when all assignments have been added.

Creating Per-App VPN Profile for iOS

For iOS 7+ devices and Android Enterprise devices, you can force selected applications to connect through your corporate VPN. Your VPN provider must support this feature, and you must publish the applications as managed applications.

In this exercise, you configure the iOS profile which configures the tunnel client on the device to allow only designated applications to access content on internal servers.

1. To add a new profile, click **Add** and then click **Profile**.
2. Select **Apple iOS**.
3. Select **Device Profile**.
4. Configure General profile settings.

The screenshot shows the 'iOS Add a New Apple iOS Profile' window. On the left, a sidebar lists various profile types: General, Passcode, Restrictions, Wi-Fi, VPN (highlighted with a red box), Email, Exchange ActiveSync, Notifications, LDAP, CalDAV, Subscribed Calendars, CardDAV, Web Clips, Credentials, SCEP, and Global HTTP Proxy. The main area is titled 'General' and contains the following fields:

- Name *: Per-App VPN (highlighted with a red box)
- Version: 1
- Description: (empty)
- Deployment: Managed
- Assignment Type: Auto
- Allow Removal: Always
- Managed By: TM-Apple
- Smart Groups: All Devices (TM-Apple) (highlighted with a red box)
- Exclusions: NO

- a. Enter the name, such as Per-App VPN in this example screenshot.
 - b. Select the name of your device's smart group, and select that group. For example, select **All Devices (your@group.shown.here)** as the assigned Smart Group.
 - c. Click **VPN** then click **Configure**.
5. Configure the VPN payload.

VPN

Connection Info

Connection Name * VPN Configuration

Connection Type * **Workspace ONE Tunnel**

Server * TCP://tunnel.ariwlab.com:443

Device Traffic Rule Sets **Default - Default**

Per-App VPN Rules ☒

IOS7

Enable VMware Tunnel ☒ ⓘ

Provider Type AppProxy

Safari Domains

+

Mail Domains

+

Contacts Domains

+

Calendar Domains

+

Associated Domains

+

Excluded Domains

+

+ -

SAVE AND PUBLISH

CANCEL

- Select **Workspace ONE Tunnel** from the Connection Type drop-down menu.
- Select **Default** as the Device Traffic Rules that will be assigned to this profile.
- Ensure the **Enable VMware Tunnel** is selected.
- Add any Mail, Contacts, and Calendar Domains. *Do not configure Safari Domains - these are configured in the VMware Tunnel Configuration later in this guide.*
- Click **Save & Publish** then click **Publish**.

Note: Safari Domains should be configured in the Device Traffic Rules for Workspace ONE Tunnel.

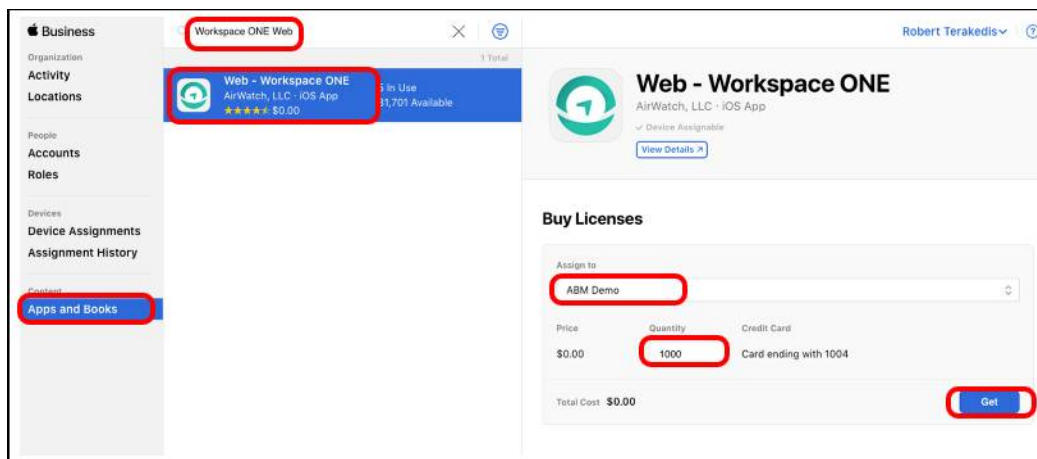
Configuring Workspace ONE Web for Per-App Tunnel

Workspace ONE Web is part of the secure productivity app suite from VMware. Administrators can deploy Workspace ONE Web when data loss and copy/paste restrictions are critical to the business use case. In this exercise, you distribute and configure Workspace ONE Web for Per-App Tunnel on iOS.

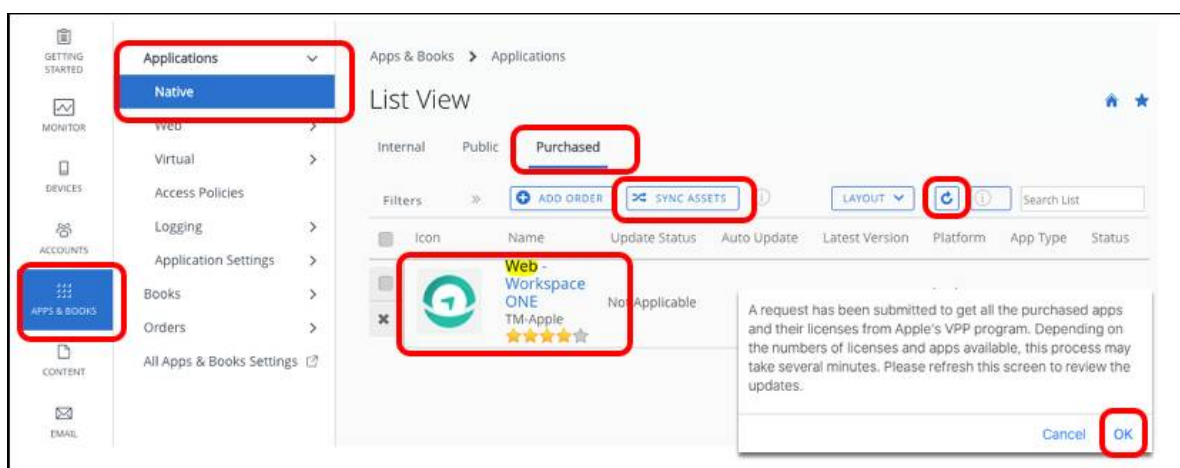
This section demonstrates how to obtain Workspace ONE Web and assign it to devices as Purchased App using the integration of Workspace ONE UEM and Apple Business Manager.

Workspace ONE Web is available for free on App Store. To deploy as a Public App managed by Workspace ONE UEM, follow the same steps described in the previous chapter to deploy Workspace ONE Tunnel.

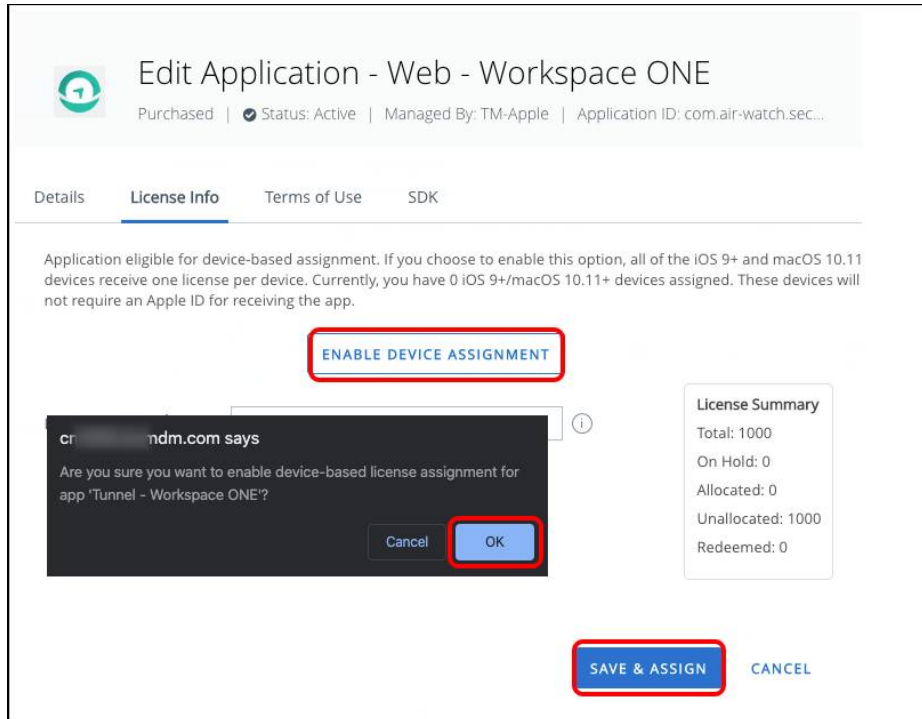
1. Get Workspace ONE Web licenses. In Apple Business Manager (or Apple School Manager):



- a. Click **Apps and Books**.
 - b. Search for *Workspace ONE Web* in the search text box.
 - c. Select **Web - Workspace ONE for iOS**.
 - d. Choose the location for which you have uploaded the sToken into Workspace ONE UEM.
 - e. Enter the quantity of licenses you want to purchase.
 - f. Click **Get**. The button changes to *Purchasing* and when the purchase is complete, it changes back to *Get*.
2. Sync assets in Workspace ONE UEM.



- a. In the Workspace ONE UEM console, click **Resources**.
 - b. Expand **Applications** and click **Native**.
 - c. Click **Purchased**.
 - d. Click **Sync Assets**.
 - e. Click **OK** on the dialog box.
 - f. Wait a few moments and click **Refresh** to update the app list.
 - g. Click the **Web - Workspace ONE** app for iOS in the app list.
3. Enable device assignment.



- a. Click **Enable Device Assignment**.
 - b. Click **OK** to confirm device-based licensing.
 - c. Click **Save & Assign**.
4. Click **Add Assignment**.
 5. Edit assignment.

Web - Workspace ONE - Edit assignment ✕

Assignment

Assignment for License Codes can be done by Smart Groups only

Active	Assignment Group (Smart Group)	Devices	Allocated	Redeemed
<input checked="" type="radio"/>	All Devices @ TM-Apple License Codes By Smart Group Create New Smart Group	0	100	0

[+ Add Assignment](#)

Deployment

Assignment Type* **AUTO** **ON DEMAND** ⓘ

Remove On Unenroll **ENABLED** **DISABLED** ⓘ

Prevent Application Backup **ENABLED** **DISABLED** ⓘ

Make App MDM Managed if User Installed **ENABLED** **DISABLED** ⓘ

Use VPN **ENABLED** **DISABLED** ⓘ

Per-App VPN Profile* **Per-App VPN @ TM-Apple** ⓘ

Send Application Configuration **ENABLED** **DISABLED** ⓘ

Send Application Attributes **ENABLED** **DISABLED** ⓘ

SAVE **CANCEL**

License Summary
Total: 1000
On Hold: 0
Allocated: 100
Unallocated: 900
Redeemed: 0

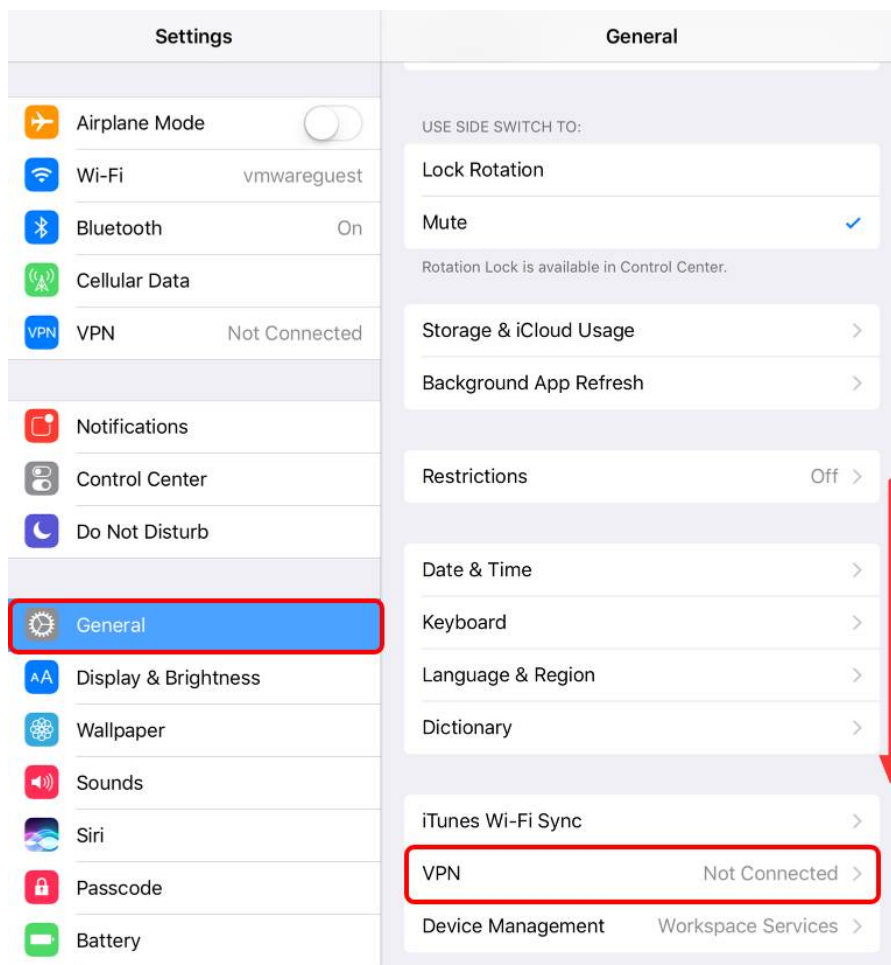
iOS 9+

- a. Click **Add Assignment**.
 - b. Select an Assignment Group (or alternatively, create a new smart group containing the targeted devices).
 - c. Enter a number of licenses to allocate. Allocate up to the total number of unallocated licenses.
 - d. Select **Auto** for Assignment Type.
 - e. Select Enabled for Remove on Unenroll.
 - f. Select Enabled for Prevent Application Backup.
 - g. Select Enabled for Make App MDM Managed if User Installed.
 - h. Select Enabled and then select the Per-App VPN profile created in *Creating Per-App VPN Profile for iOS*.
 - i. Click Save.
6. Save assignment.
- a. If more assignments are necessary, click **Add Assignment** and repeat the steps in Edit Assignment.
 - b. Click **Save and Publish**, then click **Publish** when all assignments have been added.

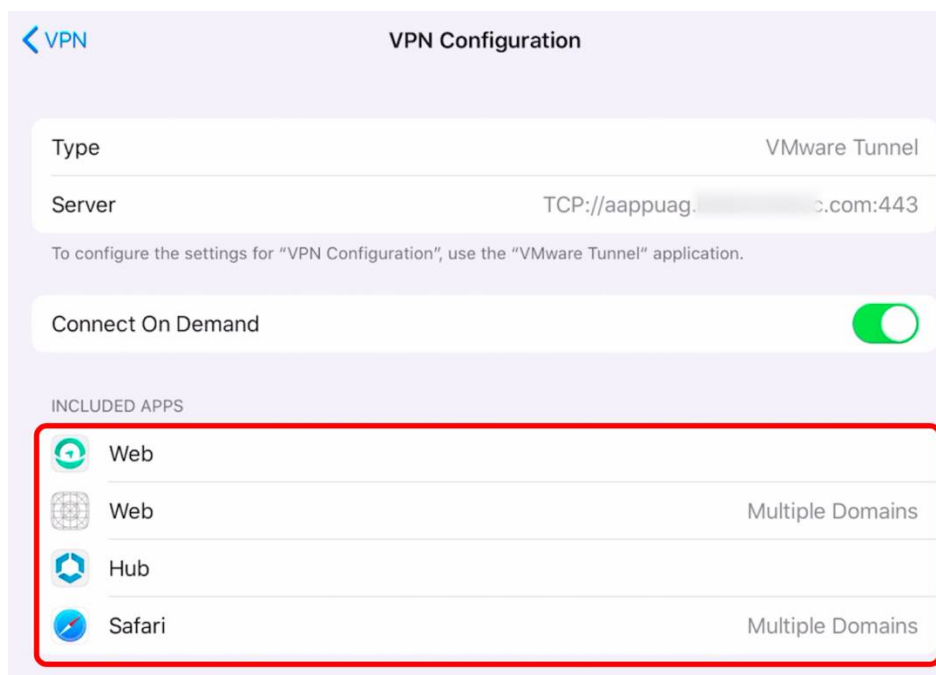
Testing Safari Domains with Per-App Tunnel

Now that the VPN profile includes a domain in the Safari Domains list, you can confirm that these settings have updated on the device and test the settings in the native Safari application.

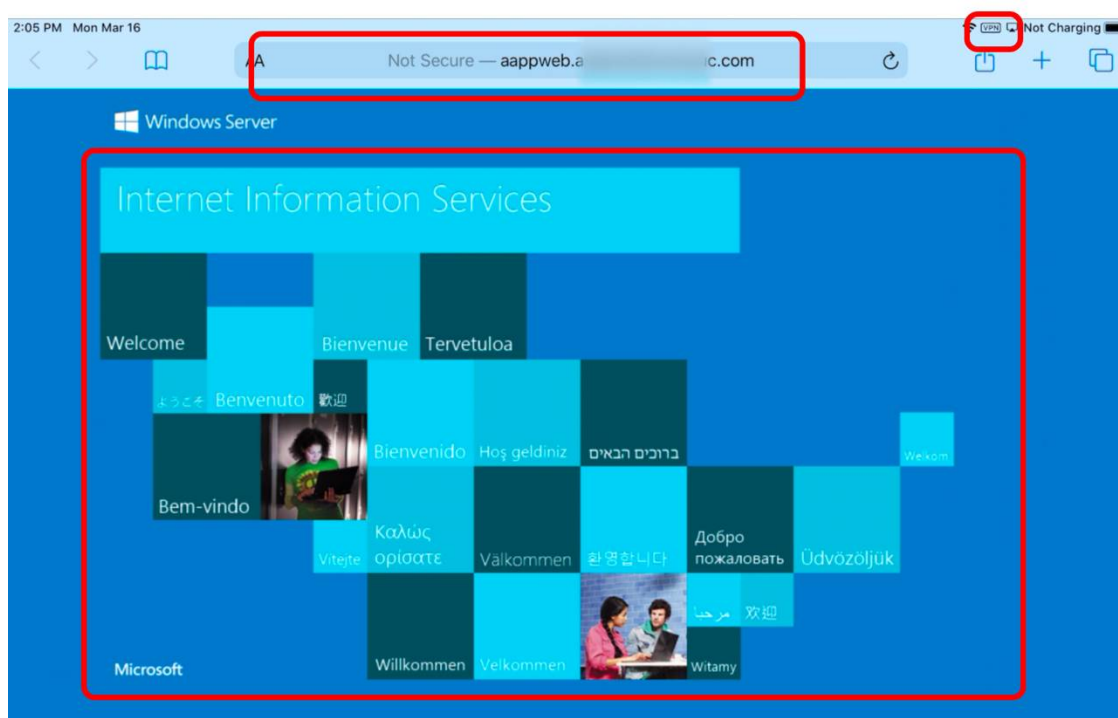
1. Tap **Settings**.
2. Open VPN settings.



- a. Tap **General** and scroll down to the VPN section.
- b. Tap **VPN**.
3. Tap **VPN Configuration** from your Per-App VPN profile.
4. Verify included Per-App VPN apps.



- a. All managed applications from the Workspace ONE UEM Console that are enabled to use Per-App VPN and have an associated Device Traffic Rule appear in this list. Note that Safari is displayed to show that domains are configured for tunneling in Safari.
5. Next, tap the **Safari** icon. The VPN icon *should not* be displayed in the toolbar.
6. Browse to the internal URL.



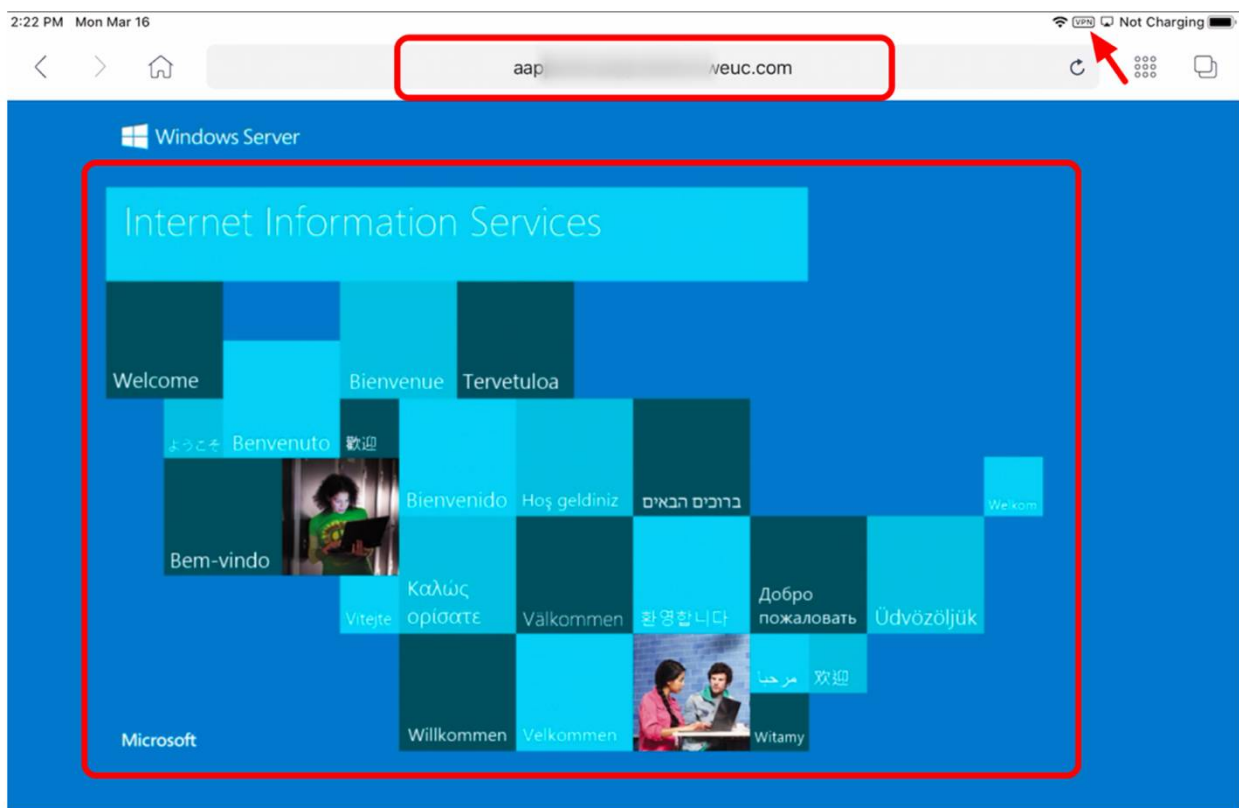
- a. Enter the URL for a website that is accessible only through VPN.
- b. Confirm that the VPN indicator is displayed when iOS launches the VPN and connects.
- c. Confirm that the internal page loads.

Testing Per-App Tunnel on iOS

Now that the enrolled device has received the settings configured in the Workspace ONE UEM Console, you are ready to begin testing the Per-App Tunnel functionality. The applications assigned in the previous exercises should push down during enrollment. The VMware Tunnel and Workspace ONE Web applications should be installed on your device.

In this exercise, launch Workspace ONE Web and access the internal website. Then verify that, although the VPN connection is active, other applications on the device cannot access the tunnel or internal resources.

1. Launch Workspace ONE Web.
 - a. Press the Home button on your device to return to the Launchpad. Swipe right to see the downloaded applications, if needed.
 - b. Tap the Workspace ONE Web icon to launch the application. If prompted, select OK to allow the Web to send your device push notifications.
2. Create and confirm password.
 - a. If prompted, create a passcode for Workspace ONE Web.
 - b. Click **Next**.
 - c. Confirm the passcode by entering it again.
 - d. Click **Confirm**.
3. Tap **I understand** to accept the Privacy prompt.
4. Tap **I agree** to accept the Data sharing prompt.
5. Access the internal website with Workspace ONE Web.



- a. When the application launches, enter the URL for your intranet website.
- b. Confirm that the VPN icon appears, indicating the connection is active. The application now connects to Workspace ONE UEM and retrieves the settings for your Organization Group.
- c. Confirm that the website loads.

Note: Depending on the Workspace ONE Web and SDK settings configured at your particular organization group level, the address bar may not be editable. This configuration is called *Kiosk Mode*. To work around this, there are two options which can be configured at **Groups & Settings > Configurations > Workspace ONE Web**:

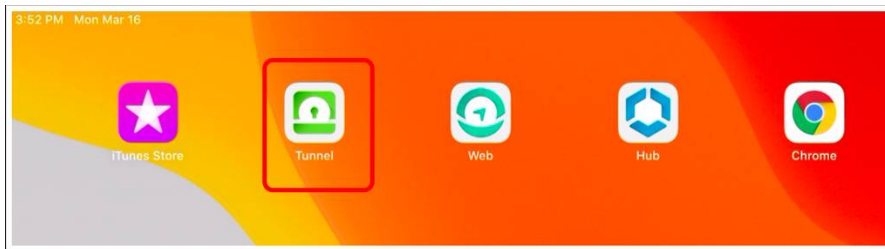
- Click the **Bookmarks** tab, click **Override** (if necessary), click **Add Bookmark**, enter a name and URL for the testing URL, and click **Save**.
- Scroll the settings to *Kiosk Mode* and click **Disabled**. Click **Save**.

These changes affect the *Default settings for Workspace ONE Web* in this Organization Group and all inherited organization groups unless otherwise configured.

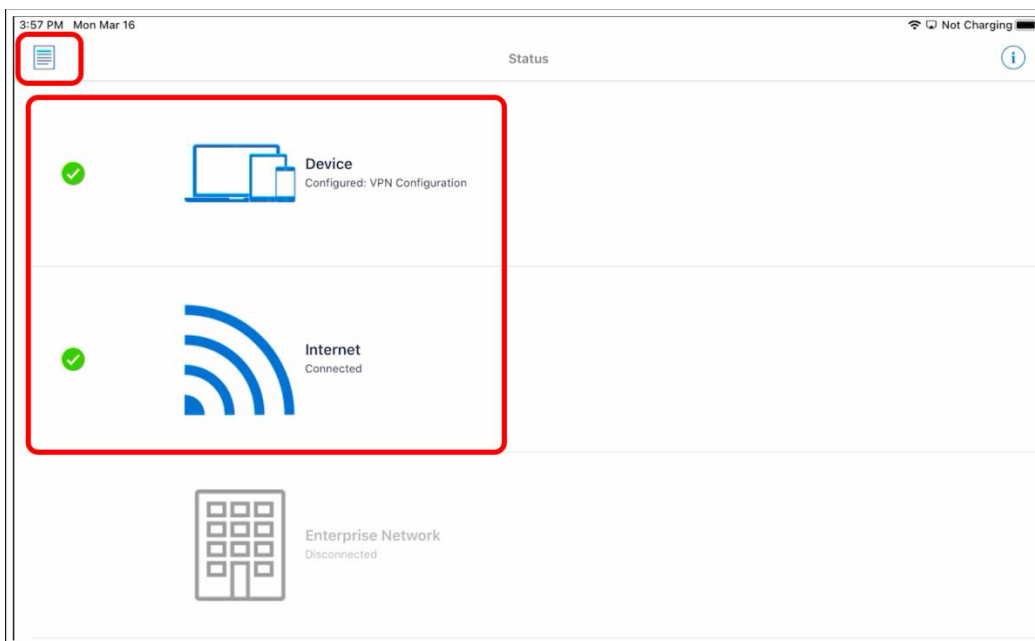
Troubleshooting the Workspace ONE Tunnel on iOS

This section contains some basic steps to troubleshooting Per-App Tunnel on iOS.

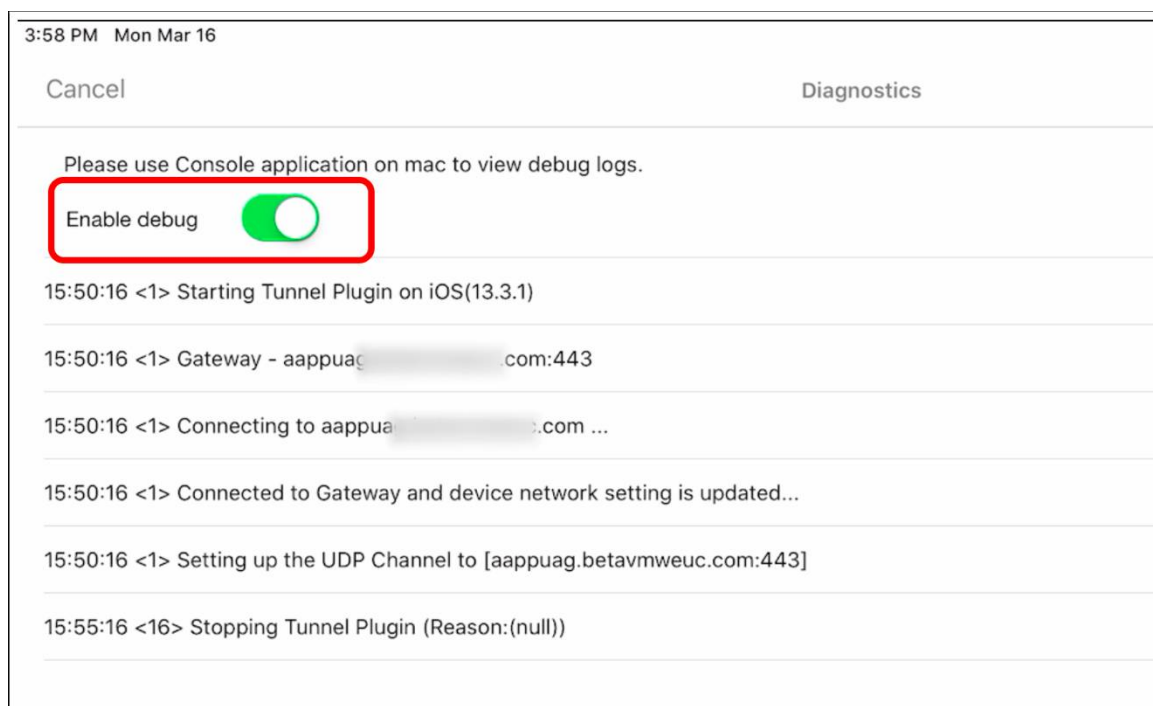
1. On an enrolled iOS device, tap **Tunnel**.



2. Tap **Continue**.
3. Tap **I understand** to accept the Privacy prompt.
4. Tap **I agree** to accept the Data sharing prompt.
5. Validate device connectivity.



- a. Ensure the device and Internet connectivity are OK (showing a green check mark symbol).
 - b. Tap the logging icon.
6. Activate the **Enable debug** toggle.



Tip: With **Enable Debug** turned on, Workspace ONE administrators can view logging information for the iOS device as follows:

1. Plug the iOS device into a device running macOS.
2. Ensure the iOS device trusts the connection to macOS.
3. Connect to Console, by either:
 - a. Open Apple Configurator 2 and double-click the test iOS device. Click **Console** to view the output from the device.
 - b. Open **Console.app** and select the iOS device from the left side.
4. Search for **tunnel** or **iOSAppProxyProvider**.

Deploying Workspace ONE Tunnel for macOS

Per-App Tunneling helps users to access critical information using applications on their devices from their devices. Mobile flows help users perform business-critical tasks from a single app — streamlining the user experience.

Leveraging Per-App Tunnel allows you to control which applications are on a device and what internal resources the applications have access to by automatically activating or deactivating Per-App VPN access, based on which applications are active. By enabling remote access, you no longer need to provide a device-wide VPN on your devices, which can allow unintended or unauthorized apps or processes to access your VPN. In this tutorial, you configure and deploy VMware Workspace ONE Tunnel to enable the Per-App Tunnel component on managed devices.

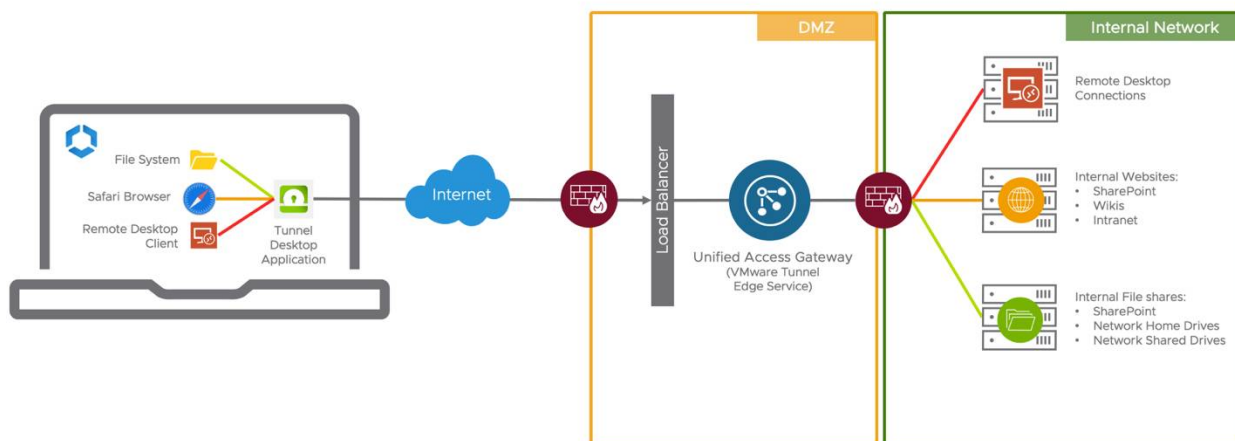
These exercises involve the following components:

- **Workspace ONE Tunnel** – The app used on the device to securely connect to the Unified Access Gateway to provide Per-App Tunnel functionality, also referred to as Tunnel Client.
- **Unified Access Gateway** – The virtual appliance where the VMware Tunnel edge service is installed, and to which the tunnel client connects.
- **Per-App Tunnel** – Component of VMware Tunnel edge service for connecting to a secure tunnel channel on a per-application basis, which is controlled and configured by the VPN profile payload and Device Traffic Rules.
- **Per-App VPN Profile and Device Traffic Rules** – The Workspace ONE UEM configuration is pushed to the device that contains the Per-App Tunnel configurations. Every time a specified application is opened, the Workspace ONE Tunnel client evaluates the Device Traffic Rules assigned to it before making any routing decisions and establishes a Per-App tunnel connection with the Unified Access Gateway based on the Per-App VPN Profile configuration.

High-Level Architecture

Workspace ONE Tunnel macOS Application

Example of Per-App VPN Remote Access



The device contains the applications required by the end-user to perform their daily job. Some applications require access to internal resources to function. Those applications, based on Per-App VPN configuration, use Workspace ONE Tunnel which communicates with the Tunnel Service on Unified Access Gateway hosted on the DMZ, to validate if the device requesting access is in compliance or not before authorizing access through the internal resource.

Prerequisites

Before you can perform the steps in this exercise, you must have the following components installed and configured:

- Workspace ONE UEM version 2302 and [later](#)
- macOS Mojave and later enrolled in Workspace ONE UEM
- The latest version of macOS Tunnel from Apple macOS App Store
 - Deploy Workspace ONE Tunnel using volume purchased licenses from Apple Business Manager or Apple School Manager.
 - Workspace ONE Administrators must upload the Location token from Apple Business Manager to sync licenses

to Workspace ONE UEM for managed distribution.

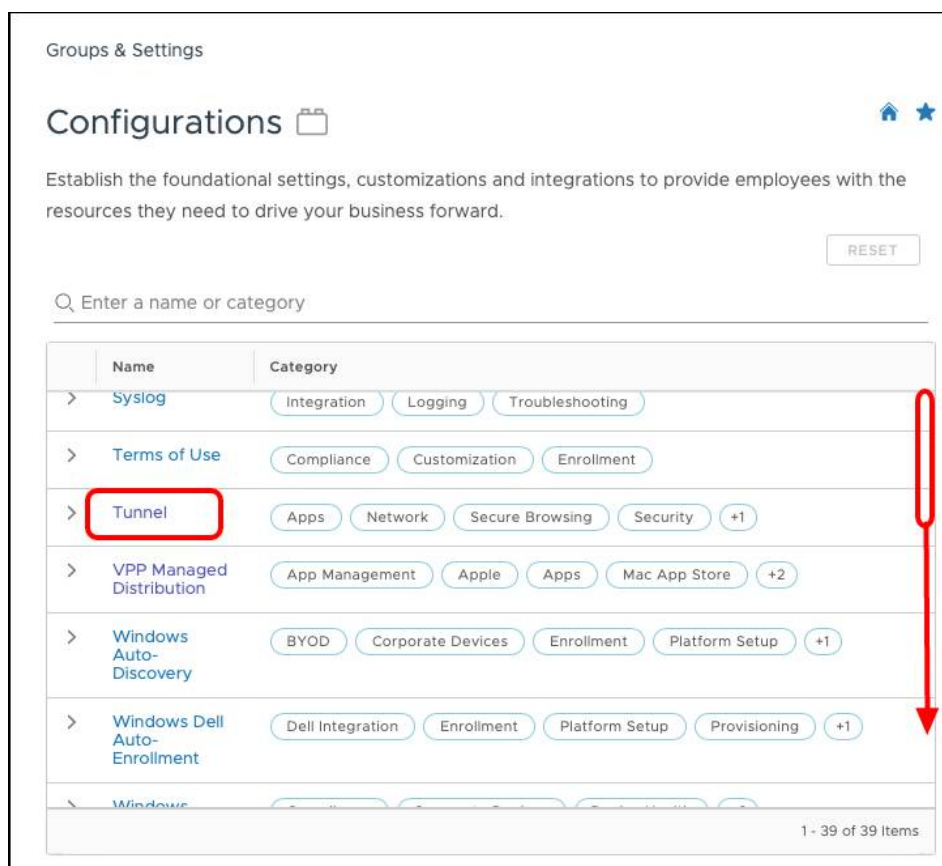
Configuring Device Traffic Rules for macOS

First, because the Apple Mail, Calendar, and Contacts applications might contain both corporate and personal data, administrators must take an extra step to define corporate-owned domains, which should be marked for Per-App VPN. The Mail, Calendar, and Contacts apps do not automatically adhere to *device traffic rules*. Administrators *must* specify which domains are corporate-owned by enabling the Mail, Contacts, and Calendar domains parameters in the VPN profile payload. Enabling these parameters in the VPN payload allows VMware Tunnel edge service to apply the appropriate device traffic rules for those specific domains.

Second, Safari is another app that might be used for personal use on a corporate device. As such, Safari cannot be configured to tunnel all traffic. Device traffic rules for Safari must specify the domain and top-level domain component (for example, vmware.com), although an asterisk (*) may be used to wildcard subdomains (for example, *.vmware.com).

Note: Domain values used in this section are examples only. Your values will differ.

1. Access configurations.
 - a. In the Workspace ONE UEM console, click **Groups & Settings**.
 - b. Click **Configurations**.
2. Scroll through the list of configurations and select **Tunnel**.



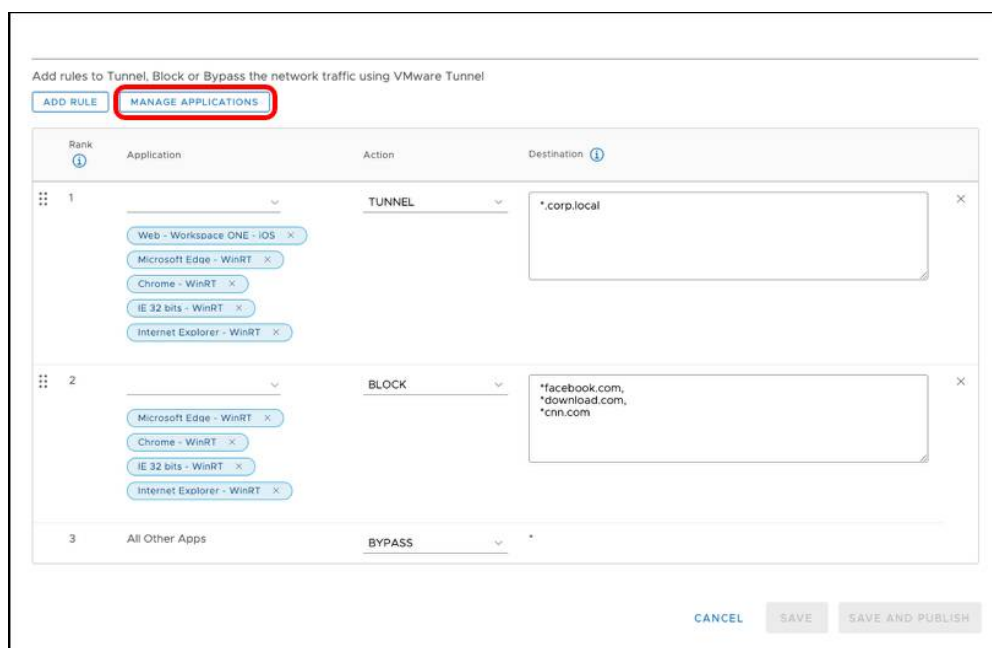
3. Edit Device Traffic Rule sets.
 - a. From within the Device Traffic Rules information block on the *Tunnel Configuration* page, click **Edit**.
4. Add or modify device traffic rule set.



Introduced in Workspace ONE UEM 2011, Device Traffic *Rule Sets* expand the functionality of device traffic rules allowing for granular assignment of rule sets to different groups of users and devices. Device Traffic Rule Sets are assigned when creating the per-app VPN profile in a later step.

To get started with Device Traffic Rule Sets, perform the following in the *Manage Traffic Assignments* screen:

- a. If no other Device Traffic Rule Sets exist (or a new rule set is required), click **Add** to create a new Device Traffic Rule Set.
 - b. If modifications to an existing rule set are required, click the Device Traffic Rule Set name.
5. Enter a name for the Device Traffic Rule Set (or if necessary, modify the name of an existing rule set).
 6. Click **Manage Applications**.



7. Click **Add** to add a new application for device traffic rules.
8. Define the application.

- Select **macOS** for Platform.
- Enter the friendly name of the application, for example, **Firefox Browser**. The friendly name is displayed in the Device Traffic Rule.
- Enter the application's package id, which is the **Identifier** value displayed by running the command:
`codesign -dv --entitlements - /path/to.app`
- Enter the application's designated requirement, which is displayed to the right of the **=>** sign of the following command: `codesign -d -r- /path/to.app`
- For macOS 10.15 (Catalina) and later, enter a path if creating a device traffic rule for a binary or command-line utility bundled within an application. For example, the executable `vmware-remotemks` must be allowlisted with path details along with the VMware Horizon Client application.
- Click **Save**.

Using Firefox as an example, a Workspace ONE administrator would see the commands and values as follows:

```
techzone@testmac ~ % codesign -dv --entitlements - /Applications/Firefox.app
Executable=/Applications/Firefox.app/Contents/MacOS/firefox
Identifier=org.mozilla.firefox
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20500 size=415 flags=0x10000(runtime) hashes=4+5 location=embedded
Signature size=9018
Timestamp=Oct 1, 2019 at 9:08:41 PM
Info.plist entries=26
TeamIdentifier=43AQ936H96
Runtime Version=10.11.0
<<< trimmed for length >>>
techzone@testmac ~ % codesign -d -r- /Applications/Firefox.app
Executable=/Applications/Firefox.app/Contents/MacOS/firefox
designated => anchor apple generic and certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or anchor apple
generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "43AQ936H96"
```

As highlighted in the terminal output, the necessary information is as follows:

Package ID: **org.mozilla.firefox**

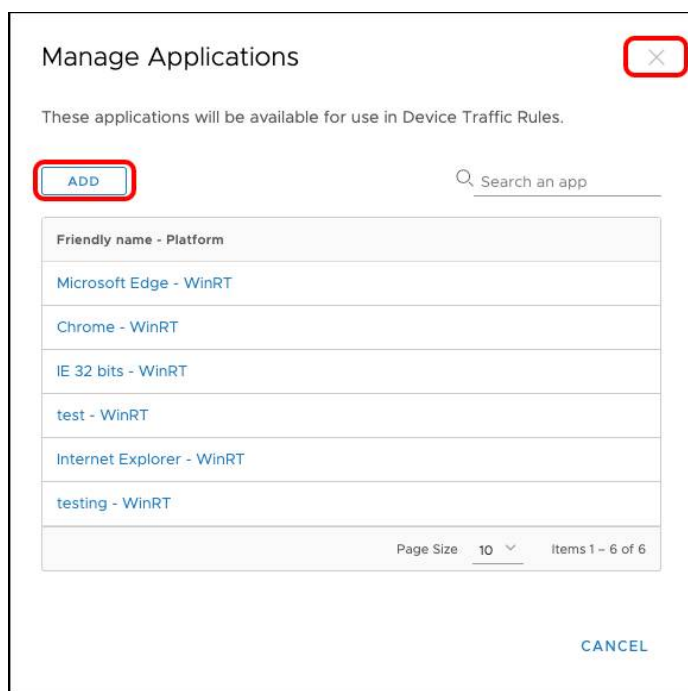
Designated Requirement: **anchor apple generic and certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "43AQ936H96"**

Caution: Some apps spawn *helper* applications to assist with background tasks. One particular example of this is Google Chrome, which performs network functions outside the **Google Chrome.app** process in a Google Chrome Helper process. In this case, the helper application must be added to the Device Traffic Rule, otherwise, specific settings must be changed client-side.

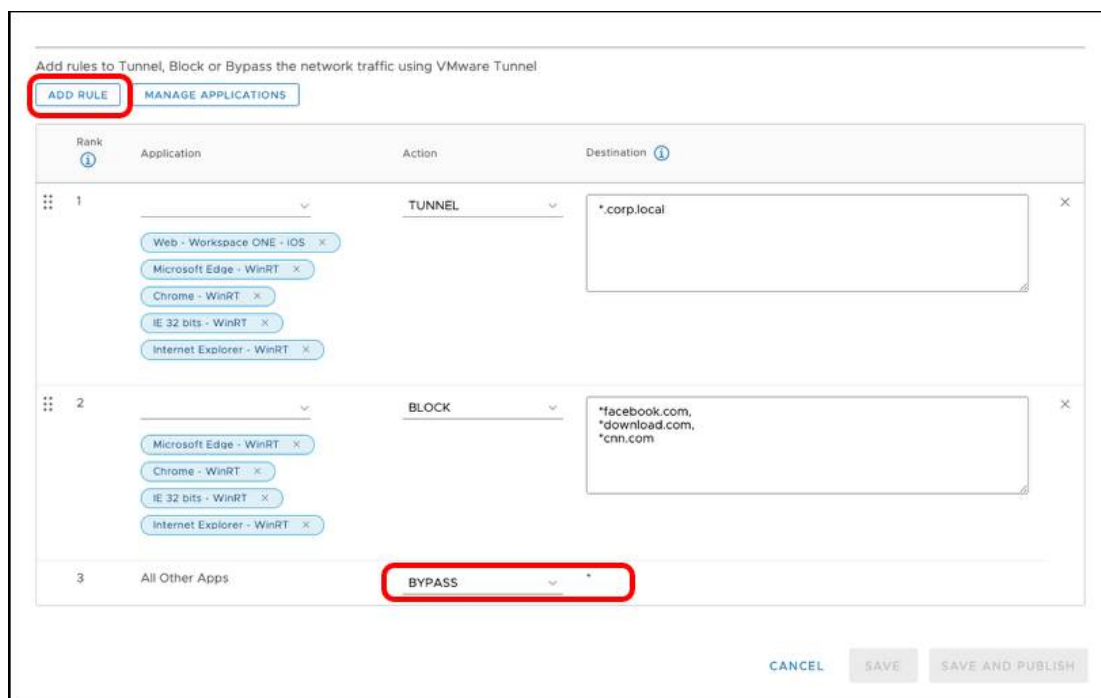
In the case of Google Chrome, perform the following:

- In the URL field, type [chrome://flags](#)

- Search for *network* in the Search Flags text box.
 - Set *Runs network service in-process* to **Enabled** and relaunch Google Chrome before proceeding with testing.
9. Add new application for device traffic rules.



- If more applications are needed for the rule set, click Add and repeat starting at Define the Application.
 - If all the required applications have been defined, click the [X] to close the Manage Applications window.
10. Add device traffic rule.



- Observe (and optionally modify) the default action which applies to all macOS applications except Safari:
 - Tunnel – All apps, except Safari, on the device configured for Per-App Tunnel send network traffic through the tunnel. For example, set the Default Action to Tunnel to ensure all configured apps without a defined traffic rule use the Workspace ONE Tunnel for internal communications.
 - Block – Blocks all apps except Safari, on the device configured for Per-App Tunnel from sending network traffic. For example, set the Default Action to Block to ensure that all configured apps without a defined

traffic rule cannot send any network traffic regardless of destination.

- iii. Bypass – All apps, except Safari, on the device configured for Per-App Tunnel bypass the tunnel and connect to the Internet directly. For example, set the Default Action to Bypass to ensure all configured apps without a defined traffic rule bypass the Workspace ONE Tunnel to access their destination directly.
- iv. Proxy - Redirect traffic to the specified HTTPS proxy for the listed domains. The proxy must be HTTPS and must follow the correct format: <https://example.com:port>.

b. Click Add Rule.

11. Build device traffic rule.

Add rules to Tunnel, Block or Bypass the network traffic using VMware Tunnel

ADD RULE **MANAGE APPLICATIONS**

Rank	Application	Action	Destination
1	<input type="checkbox"/> Web - Workspace ONE - iOS <input type="checkbox"/> Microsoft Edge - WinRT <input type="checkbox"/> Chrome - WinRT <input type="checkbox"/> IE 32 bits - WinRT <input type="checkbox"/> test - WinRT <input type="checkbox"/> Internet Explorer - WinRT <input type="checkbox"/> testing - WinRT <input checked="" type="checkbox"/> Microsoft Edge Beta - macOS <input checked="" type="checkbox"/> Firefox Browser - macOS <input type="checkbox"/> All Applications	TUNNEL	*.airwlab.com
2	<input type="checkbox"/> Web - Workspace ONE - iOS <input type="checkbox"/> Microsoft Edge - WinRT <input type="checkbox"/> Chrome - WinRT <input type="checkbox"/> IE 32 bits - WinRT <input type="checkbox"/> Internet Explorer - WinRT	TUNNEL	*.corp.local
3	<input type="checkbox"/> Microsoft Edge - WinRT <input type="checkbox"/> Chrome - WinRT <input type="checkbox"/> IE 32 bits - WinRT <input type="checkbox"/> Internet Explorer - WinRT	BLOCK	*facebook.com, *download.com, *cnn.com
4	All Other Apps	BYPASS	*

CANCEL **SAVE** **SAVE AND PUBLISH**

- a. In the newly created device traffic rule, click the down arrow to display the Application list.
- b. Select one or more triggering applications to control with this rule. In case you select All Applications, the rule will be applied only to Safari and macOS applications selected in additional rules defined as part of the Device Traffic Rules.
- c. Enter one or more comma-separated fully qualified domain names as destinations to which Workspace ONE Tunnel should apply the Device Traffic Rule. A single asterisk (*) can be used as a wildcard for subdomains.
- d. Select the Appropriate Action for Workspace ONE Tunnel to perform on traffic from the selected apps:
 - i. Tunnel – Sends app network traffic for specified domains through the tunnel to your internal network.
 - ii. Block – Blocks all traffic sent to specified domains.

- iii. Bypass – Bypasses the Workspace ONE Tunnel so the application accesses specified domains directly.
- iv. Proxy – Redirect traffic to the specified HTTPS proxy for the listed domains. The proxy must be HTTPS and must follow the correct format: <https://example.com:port>.
- e. If necessary, adjust the Device Traffic Rules rank in the list. Lower-numbered rank is the highest priority.
- f. If necessary, click Add Rule and repeat steps in *Build Device Traffic Rule* until you have added all the necessary Device Traffic Rules for your organization.
- g. Click Save and Publish to send the updated DTR's to all devices to which the DTR is assigned.

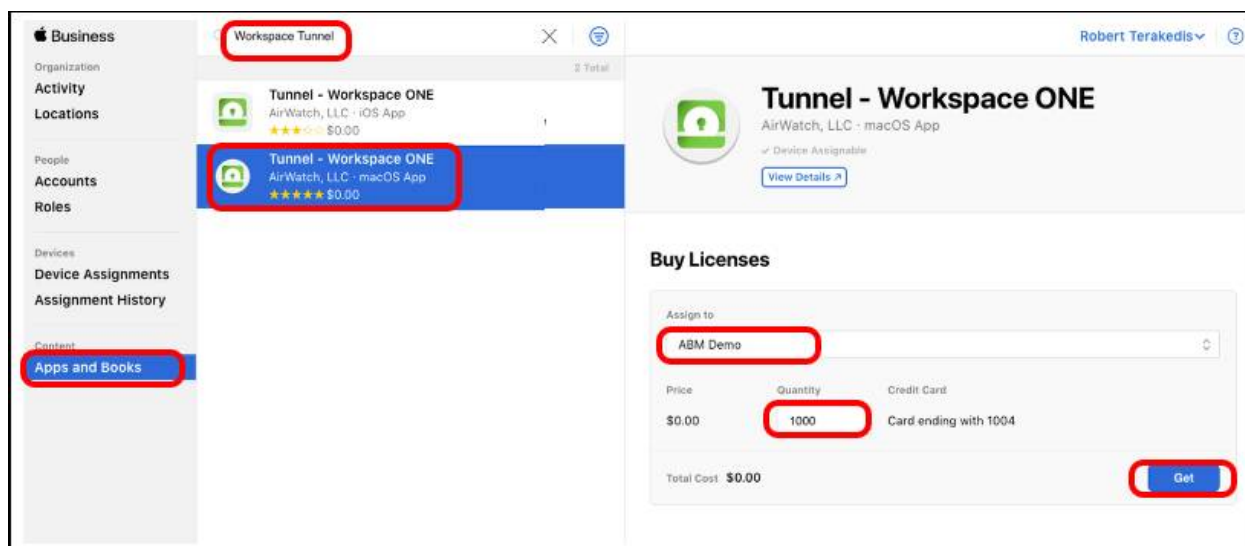
For more information on the formats (wildcards, IP, ports) allowed into the Destination field, see the *Device Traffic Rules Guidelines and use of asterisk* chapter.

Distributing Workspace ONE Tunnel for macOS

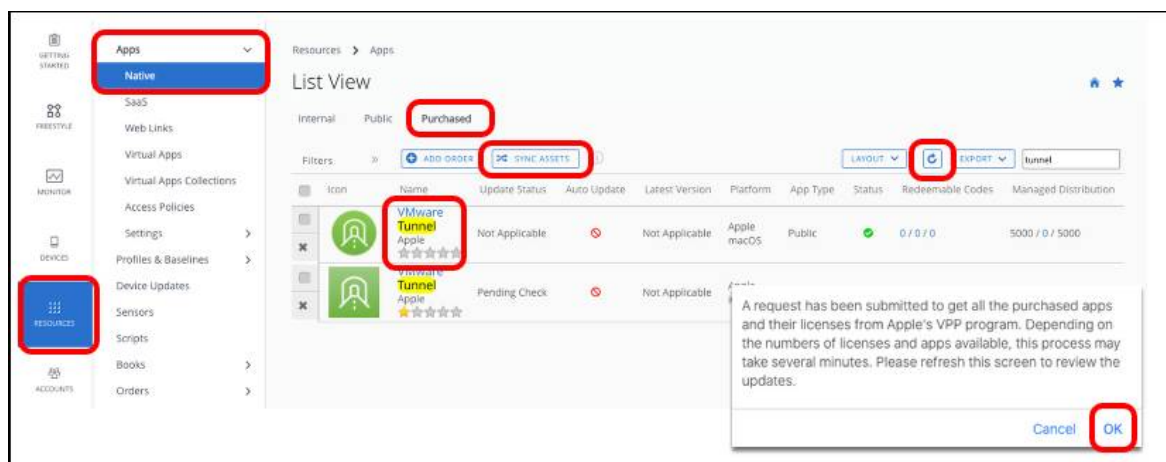
Workspace ONE Tunnel is a macOS application available for free on the Mac App Store. It is also available for managed distribution volume licensing through Apple Business Manager and Apple School Manager. Use device-based licensing to distribute Workspace ONE Tunnel to managed macOS devices. This section demonstrates how to purchase Workspace ONE Tunnel and assign it to devices.

Note: The VPN tunnel should already be configured as part of the Prerequisites.

1. Get Workspace ONE Tunnel licenses.



- a. In Apple Business Manager (or Apple School Manager), click **Apps and Books**.
 - b. Search for *workspace tunnel* in the search text box.
 - c. Select **Tunnel - Workspace ONE** for macOS.
 - d. Choose the location for which you have uploaded the sToken into Workspace ONE UEM.
 - e. Enter the quantity of licenses you want to purchase.
 - f. Click **Get**. The button changes to *Purchasing* and when the purchase is complete changes back to *Get*.
2. Sync assets in Workspace ONE UEM.



- a. In the Workspace ONE UEM console, click **Resources**.
 - b. Expand **Applications** and click **Native**.
 - c. Click **Purchased**.
 - d. Click **Sync Assets**.
 - e. Click **OK** on the dialog box.
 - f. Wait a few moments and click **Refresh** to update the app list.
 - g. Click the Workspace ONE Tunnel app in the app list.
3. Enable device assignment.

Edit Application - Tunnel - Workspace ONE
Purchased | Status: Active | Managed By: TM-Apple | Application ID: com.vmware.macos-tunnel

Details | **License Info** | Terms of Use

Application eligible for device-based assignment. If you choose to enable this option, all of the iOS 9+ and macOS 10.11+ devices receive one license per device. Currently, you have 0 iOS 9+/macOS 10.11+ devices assigned. These devices will not require an Apple ID for receiving the app.

ENABLE DEVICE ASSIGNMENT

Licenses on hold * 0

License Summary
Total: 1000
On Hold: 0
Allocated: 0
Unallocated: 1000
Redeemed: 0

SAVE & ASSIGN CANCEL

- a. Click **Enable Device Assignment** and click **OK** for the Are you sure? prompt.
 - b. Click **Save & Assign**.
4. Click **Add Assignment**.
 5. Edit assignment.

VMware Tunnel - Assignment

Distribution

Name * **Default**

Description
Assignment Description

License Distribution *
Purchased App License Assignment By Smart Group

Assignment Groups	Allocated	Redeemed
To whom do you want to assign this app?	1	0
Apple X 0 Devices		

License Summary

Total:	5000
On Hold:	0
Allocated:	1
Unallocated:	4999
Redeemed:	0

ADD

App Delivery Method * **Auto** On Demand

CANCEL **CREATE**

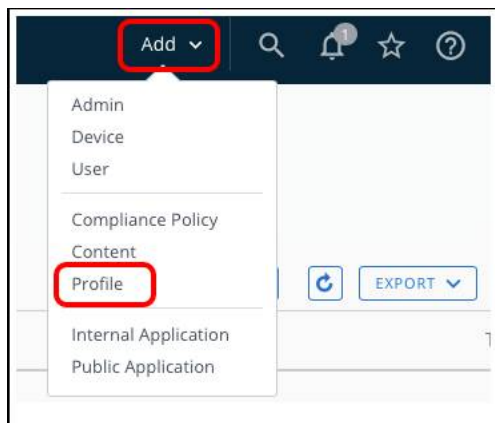
- a. Enter a name for the Distribution
 - b. Select an Assignment Group (or alternatively, create a new smart group containing the targeted devices).
 - c. Enter a number of licenses to allocate. Allocate up to the total number of unallocated licenses.
 - d. Select **Auto** for Assignment Type.
 - e. Click **Create**.
6. Save assignment.
 - a. If more assignments are necessary, click Add Assignment and repeat the steps in *Edit Assignment*.

- b. Click Save and then Publish when all assignments have been added.

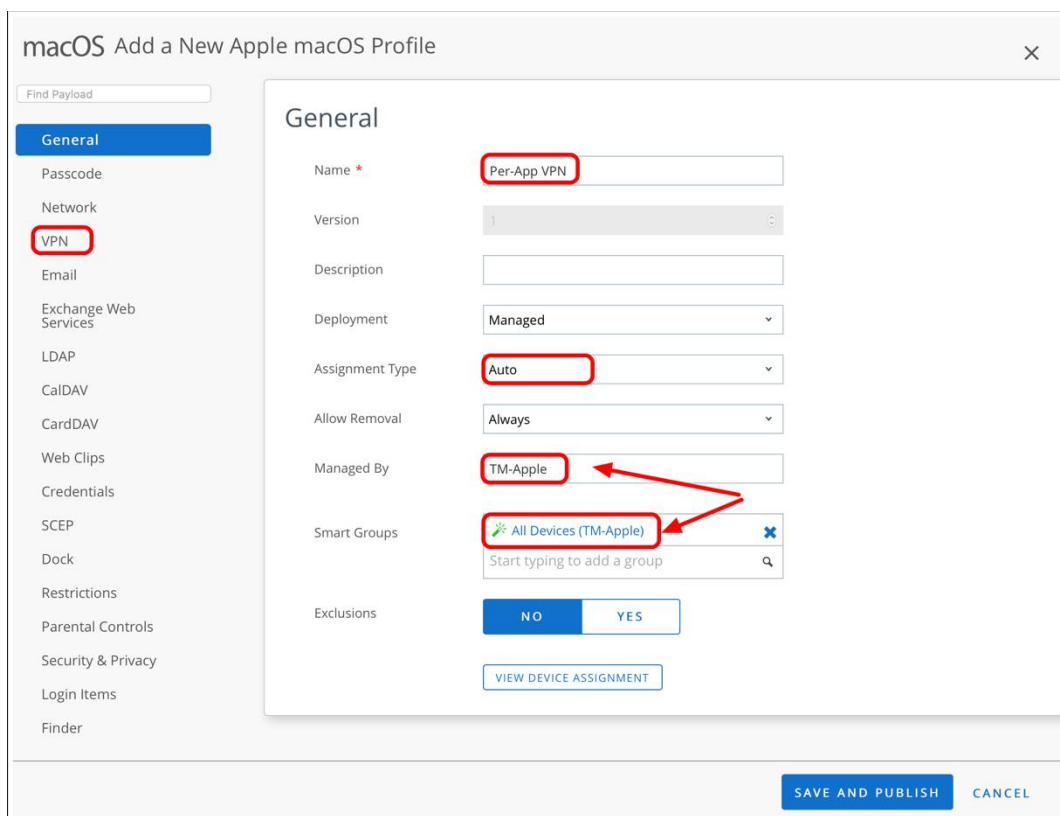
Creating Per-App VPN Profile for macOS

Before device traffic rules take effect on macOS, Workspace ONE administrators must deploy a VPN profile payload that configures macOS to leverage Workspace ONE Tunnel. In this exercise, you create the macOS profile which configures the tunnel client on the device to allow only designated applications to access content on internal servers.

1. To add a new profile, click **Add** and then click **Profile**.



2. Select **macOS**.
3. Select **User Profile**.
4. Configure General profile settings.



- a. Enter a name for the profile, for example, Per-App VPN.
 - b. Select **Auto** as the assignment type.
 - c. Select one or more **Smart Groups** to assign the VPN profile (or create a new smart group).
 - d. Click the **VPN** payload then click **Configure**.
5. Configure VPN payload.

macOS Add a New Apple macOS Profile

VPN

⚠ Manage Safari domains and apps using Device Traffic Rules in the Tunnel Configuration. Defined app policies will automatically apply to this profile.

Connection Info

Connection Name * VMware Per-App VPN

Connection Type * Workspace ONE Tunnel

Server * TCP://tunnel.airwlab.com:443

Device Traffic Rule Sets Tutorial

Per-App VPN Rules ☒ OS X 10.11

Provider Type AppProxy

Enable Mail Domains ☒ macOS 10.15

Match Domain or Host

Mail Domains

+ ADD

Enable Contacts Domains ☐ macOS 10.15

Enable Calendar Domains ☐ macOS 10.15

Enable Associated Domains ☐ macOS 11.0

Enable Excluded Domains ☐ macOS 11.0

Authentication

User Authentication Certificate

SAVE AND PUBLISH CANCEL

- Enter a name for the Per-App VPN Connection, for example, VMware Per-App VPN.
- Select Workspace ONE Tunnel as the Connection Type.
- Choose the Device Traffic Rule Set (as configured in *Configuring Device Traffic Rules for macOS*) to be assigned via this Profile Payload.
- If required, select the check boxes for Enable Mail Domains, Enable Contacts Domains, and Enable Calendar Domains.
- For each check box, enter a domain that should be tunneled.
- If multiple domains are required, click Add to enter an additional domain. Repeat as necessary.
- Click Save and Publish.

6. Click **Publish**.

Testing Per-App Tunnel on macOS

With the settings configured in the Workspace ONE UEM Console, administrators can test the Per-App Tunnel functionality on an enrolled device. The Workspace ONE Tunnel assigned in the previous exercises should install automatically during enrollment. As part of testing, the applications defined in the Device Traffic Rules should be deployed as described in [Deploying Third-Party macOS Applications: VMware Workspace ONE Operational Tutorial](#).

As a reminder, the prerequisites for testing Per-App Tunnel on macOS include the following:

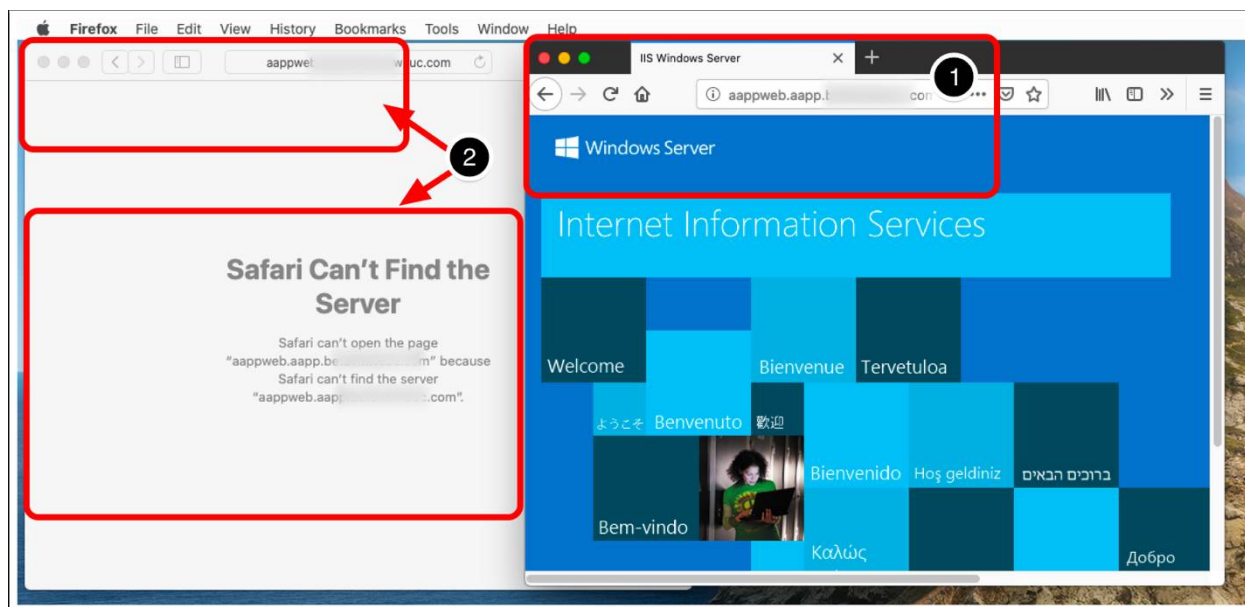
- Tunnel Edge Service configured on Unified Access Gateway
- Device Traffic Rules configured in Workspace ONE UEM
- Workspace ONE Tunnel and additional apps defined in Define Traffic Rules deployed to an enrolled device running

macOS

- A valid endpoint that is not accessible to the apps on the device except via per-app Tunnel

Validate Per-App Tunnel based on Device Rules

1. Open an app specified in a Device Traffic Rule and ensure the application attempts to connect to the mapped domain name(s).
2. Open an app that is not specified in a Device Traffic Rule, such as Safari (which will not adhere to the default Device Traffic Rule due to the wildcard mapping). Ensure the same mapped domain name does not work.



In the section of this tutorial where device traffic rules were created for macOS, Firefox was the allowed application. In the screenshot, note that Firefox is launched and attempted connection to an approved (wildcard) destination (#1). Also, observe that Safari (which was not granted access to the tunnel) cannot connect to the endpoint.

Extending Tunnel Configuration for Kerberos SSO Extension in macOS

With macOS Catalina, Apple introduced a new single sign-on (SSO) extension framework and included a built-in Kerberos SSO extension. The Kerberos SSO extension syncs passwords between a user's account in Active Directory and the local macOS account. It also brings Kerberos SSO functionality directly into the OS via MDM-manageable payloads. This tutorial aims to help experienced Workspace ONE administrators to configure the Kerberos SSO extension for macOS Catalina, and enable off-network access for the extension through per-app tunneling.

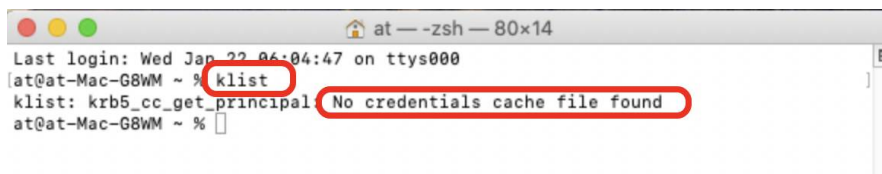
IMPORTANT: This document is provided as a courtesy to aid anyone wishing to test the functionality. This document was created around the time macOS Catalina was released. Kerberos Ticketing worked as expected at that time, but the Kerberos SSO Extension had a known bug that prevented AD password sync and change over per-app tunnel. Since then, the Kerberos SSO Extension has continued to work for network-connected devices.

However, Kerberos SSO over per-app tunneling has been in varying states of functioning depending on major, minor, and development builds of the OS. We encourage customers interested in this functionality to test and file feedback with Apple (using [Apple's Feedback Assistant](#)) and also with VMware.

Software Prerequisites	Configuration Prerequisites
<p>Before using this section of the tutorial, Workspace ONE administrators must ensure the following software version prerequisites are met:</p> <ul style="list-style-type: none"> • Workspace ONE UEM version 2302+ • macOS Catalina 10.15.0+ <p>Optionally, if configuring the SSO Extension to use Per-App Tunnel, administrators should meet these additional prerequisites:</p> <ul style="list-style-type: none"> • Unified Access Gateway 3.8+ • VMware Tunnel app for macOS version 4.1+ 	<p>Before using this section of the tutorial, Workspace ONE administrators must complete the following types of configurations within their environment:</p> <ul style="list-style-type: none"> • Microsoft Active Directory • Internal Websites or applications configured for Kerberos Authentication <ul style="list-style-type: none"> - Microsoft IIS should be configured for Windows Authentication with <i>Negotiate</i> as the primary enabled provider. When connecting to the IIS-hosted site from a web browser configured in the Device Traffic Rule, the browser should prompt for Username/Password prior to completion of this section as macOS should have no Kerberos awareness.

Validate No Pre-existing Kerberos Tickets

1. Press CMD+SpaceBar (⌘+Space) and enter terminal into the Finder window.
2. Select **Terminal** to open Terminal.app.
3. Enter `klist` and press Return on the keyboard.
4. Ensure that there are no Kerberos Tickets and the command returns *No credentials cache file found*.

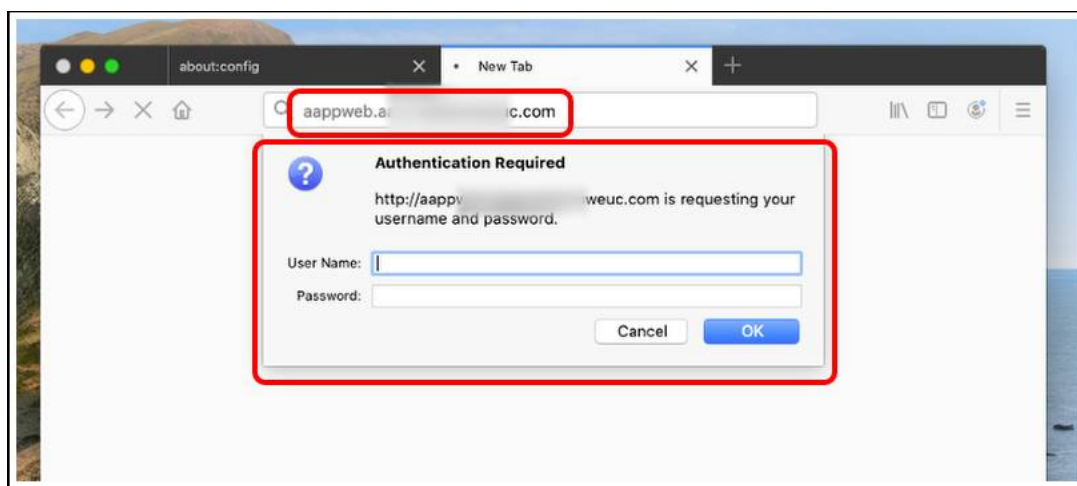


```

at — zsh — 80x14
Last login: Wed Jan 22 06:04:47 on ttys000
at@at-Mac-G8WM ~ % klist
klist: krb5_cc_get_principal: No credentials cache file found
at@at-Mac-G8WM ~ %
  
```

Validate Kerberos Application or Website Fails

1. Launch an application which should be Kerberos-enabled. If using a website, browse to the Kerberos-enabled website.

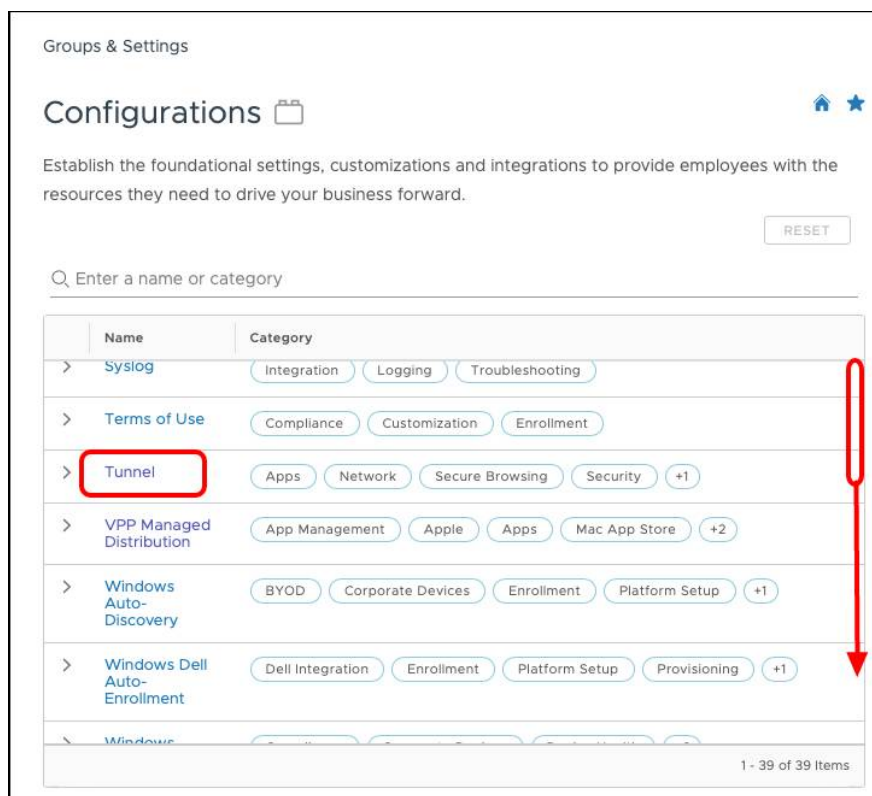


2. Note that authentication either fails (as there are no Kerberos tickets) or reverts to a non-Kerberos authentication type (such as certificate authentication or username/password).

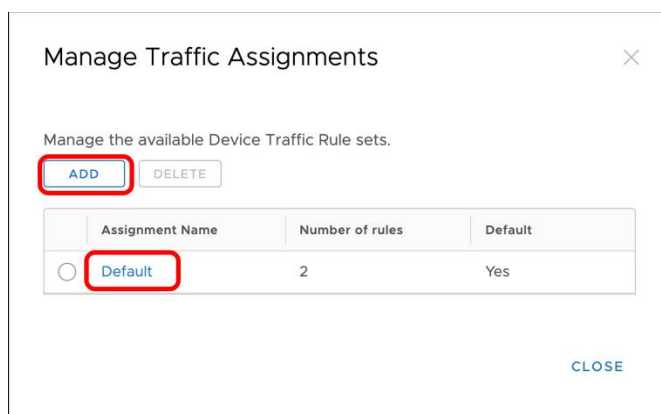
Define the Kerberos Extension in Device Traffic Rules

To connect the SSO Kerberos Extension over Per-App Tunnel, you must add the appropriate device traffic rules to the Tunnel configuration to support this. This section covers how to add the appropriate device traffic rules.

1. Access configurations.
 - a. In the Workspace ONE UEM console, click **Groups and Settings**.
 - b. Click **Configurations**.
2. Scroll through the list of configurations and select **Tunnel**.



3. Edit Device Traffic Rule sets.
 - a. From within the Device Traffic Rules information block on the *Tunnel Configuration* page, click **Edit**.
4. Add or modify device traffic rule set.



Introduced in Workspace ONE UEM 2011, Device Traffic *Rule Sets* expand the functionality of device traffic rules allowing for granular assignment of rule sets to different groups of users and devices. Device Traffic Rule Sets are assigned when creating the per-app VPN profile in a later step.

To get started with Device Traffic Rule Sets, perform the following in the *Manage Traffic Assignments* screen:

- a. If no other Device Traffic Rule Sets exist (or a new rule set is required), click **Add** to create a new Device Traffic Rule Set.
 - b. If modifications to an existing rule set are required, click the Device Traffic Rule Set name.
5. Enter a name for the Device Traffic Rule Set (or if necessary, modify the name of an existing rule set).

Device Traffic Rules

Assignment Name: **Default**

Add rules to Tunnel, Block or Bypass the network traffic using VMware Tunnel

BYPASS

Rank	Application	Action	Destination
1	Web - Workspace ONE - iOS Microsoft Edge - WinRT Chrome - WinRT IE 32 bits - WinRT Internet Explorer - WinRT	TUNNEL	*.corp.local
2	Microsoft Edge - WinRT Chrome - WinRT IE 32 bits - WinRT Internet Explorer - WinRT	BLOCK	*facebook.com, *download.com, *cnn.com
3	All Other Apps	BYPASS	*

CANCEL SAVE SAVE AND PUBLISH

6. Click **Manage Applications**.
7. Click **Add** to add a new application for device traffic rules.
8. Define the application.

Add Application

Add application details for setting app traffic policies.

Platform: **macOS**

Friendly Name: **Kerberos SSO Extension**

Package ID: **com.apple.AppSSOKerberos.KerberosExtension**

Designated Requirement: **identifier "com.apple.AppSSOKerberos.KerberosExt"**

Path: **/System/Library/PrivateFrameworks/AppSSOKerber**

CANCEL **SAVE**

- a. Select **macOS** for Platform.
- b. Enter the friendly name of the application, for example, Kerberos SSO Extension. The friendly name is displayed in the Device Traffic Rule.
- c. Enter the application's package id (com.apple.AppSSOKerberos.KerberosExtension), which is the **Identifier** value displayed by running the command:

```
codesign -dv --entitlements -
```

/System/Library/PrivateFrameworks/AppSSOKerberos.framework/Plugins/KerberosExtension.appex/Contents/MacOS/KerberosExtension

- d. Enter the application's Designated Requirement (identifier "com.apple.AppSSOKerberos.KerberosExtension" and anchor apple), which is displayed to the right of the => sign of the following command:

codesign -d -r -

/System/Library/PrivateFrameworks/AppSSOKerberos.framework/Plugins/KerberosExtension.appex/Contents/MacOS/KerberosExtension

- e. Enter the following path:

/System/Library/PrivateFrameworks/AppSSOKerberos.framework/Plugins/KerberosExtension.appex/Contents/MacOS/KerberosExtension

- f. Click **Save**.

9. Define additional applications (macOS BigSur and later).

For macOS Big Sur and later, follow the same process defined in *Add macOS Application to Rule Builder* and *Define the Application*, configure these additional applications. These additional configurations allow the full functionality of the Kerberos SSO Extension with regards to Active Directory password sync and change.

AppSSOAgent:

- a. **Platform:** macOS
- b. **Friendly Name:** Kerberos SSO AppSSOAgent
- c. **Package ID:** com.apple.AppSSOAgent
- d. **Designated Requirement:** identifier "com.apple.AppSSOAgent" and anchor apple
- e. **Path:**
/System/Library/PrivateFrameworks/AppSSO.framework/Support/AppSSOAgent.app/Contents/MacOS/AppSSOAgent

KerberosMenuExtra:

- f. **Platform:** macOS
- g. **Friendly Name:** Kerberos SSO KerberosMenuExtra
- h. **Package ID:** com.apple.KerberosMenuExtra
- i. **Designated Requirement:** identifier "com.apple.KerberosMenuExtra" and anchor apple
- j. **<No Path Required>**

10. Add device traffic rule.

Device Traffic Rules

Assignment Name
Default

Add rules to Tunnel, Block or Bypass the network traffic using VMware Tunnel

ADD RULE **MANAGE APPLICATIONS**

Rank	Application	Action	Destination
1	<input type="checkbox"/> IE 32 bits - WinRT <input type="checkbox"/> test - WinRT <input type="checkbox"/> Internet Explorer - WinRT <input type="checkbox"/> testing - WinRT <input type="checkbox"/> Kerberos SSO KerberosMenuExtra - ... <input type="checkbox"/> Kerberos SSO Extension - macOS <input type="checkbox"/> Kerberos SSO AppSSOAgent - macOS <input type="checkbox"/> Microsoft Edge Beta - macOS <input type="checkbox"/> Firefox Browser - macOS <input type="checkbox"/> All Applications	TUNNEL	*.apple.com, *.apple.com
2	<input type="checkbox"/> Microsoft Edge - WinRT <input type="checkbox"/> Chrome - WinRT <input type="checkbox"/> Internet Explorer - WinRT	BLOCK	*facebook.com, *download.com, *cnn.com
3	All Other Apps	BYPASS	*

CANCEL **SAVE** **SAVE AND PUBLISH**

- Click **Add Rule**.
- Click the down arrow in the *Application* column of the new device traffic rule.
- Select the three Kerberos SSO Extension apps you defined in the previous steps:
 - com.apple.AppSSOKerberos.KerberosExtension
 - com.apple.AppSSOAgent
 - com.apple.KerberosMenuExtra
- Select **Tunnel** as the action.
- Configure destination domain names (include wildcards if needed) that match your domain controllers.
- Click **Save and Publish**.

Configure Kerberos Profile Payload

Next, create the Kerberos profile and configure the SSO extension payload.

- Click **Add** and click **Profile**.
- Select **macOS**.
- Select **User Profile**.

Note: The SSO Extension payload is available in both the User and Device context as of Workspace ONE UEM 2011 and later. The choice to use User Profile versus Device Profile will primarily be driven by the certificate used in the payload. In most cases, the certificate/credential should be used from the login keychain, and the Workspace ONE UEM administrator should use a User profile. Otherwise, choose Device Profile to use a certificate/credential from the system keychain.

- Configure General Profile details.

macOS Add a New Apple macOS Profile

Find Payload

General

Passcode

Network

VPN

Credentials

SCEP

Dock

Restrictions

Software Update

Parental Controls

Directory

Security & Privacy

Kernel Extension Policy

Privacy Preferences

Disk Encryption

Login Items

Login Window

Energy Saver

Time Machine

Finder

Accessibility

Printing

General

Name * Kerberos SSO Extension

Version 1

Description

Deployment Managed

Assignment Type Auto

Allow Removal Always

Managed By TM-Apple

Smart Groups All Devices (TM-Apple)

Exclusions NO YES

VIEW DEVICE ASSIGNMENT

Additional Assignment Criteria

☐ Enable Scheduling and install only during selected time periods

- a. Enter a name for the profile, for example, Kerberos SSO Extension.
 - b. Select **Auto** as the Assignment Type.
 - c. Select one or more Smart Groups to assign the SSO Extension profile (or create a new smart group).
5. Configure SSO extension payload.

macOS Add a New Apple macOS Profile

SSO

General

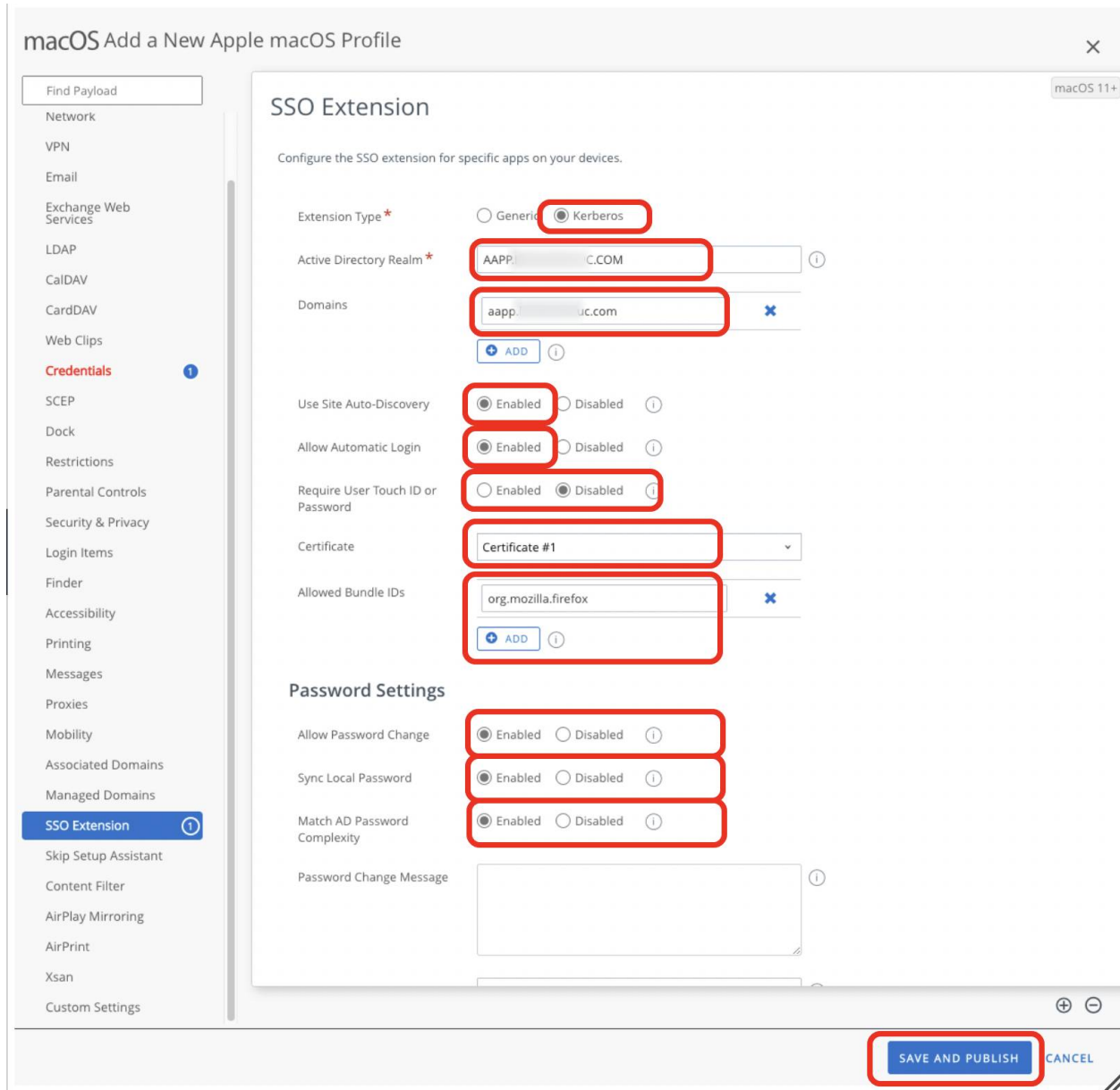
Associated Domains

SSO Extension

SSO Extension

CONFIGURE

- a. Search for the SSO payload.
 - b. Click SSO Extension.
 - c. Click Configure.
6. Modify and save SSO extension payload.



- a. Select **Kerberos** for Extension Type.
- b. Enter the Active Directory Realm (*in capital letters*) where the user logs in. For example, AAPP.XXXX.COM.
- c. Enter the Active Directory hosts and domains that can be authenticated through the extension. For example, aapp.xxxx.com.
- d. Select whether the extension should use active directory and DNS to discover its AD site.
- e. Select whether the extension should save passwords to the keychain.
- f. Select whether the user should be required to use biometrics or a password to use the keychain.
- g. Select the Certificate Credential that should be used for authenticating in the SSO Extension.
- h. Enter a list of application Bundle IDs allowed to use the Kerberos Ticket Granting Ticket. If more than one app is allowed, click **Add** to add additional bundle IDs.
- i. Select whether to allow users to initiate directory password changes from the extension.
- j. Select whether to keep the local macOS user account password synchronized with the Active Directory account password.
- k. Select whether passwords must meet Active Directory's definition of complex.
- l. Optionally, scroll down to configure additional parameters with regards to password settings.
- m. Click **Save and Publish**.

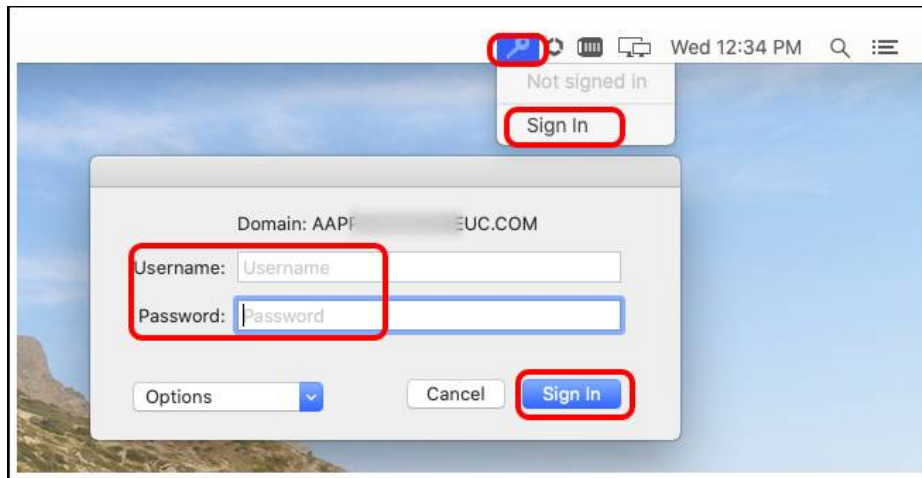
7. Click **Publish** to publish the SSO extension profile.

Validate Kerberos Tickets

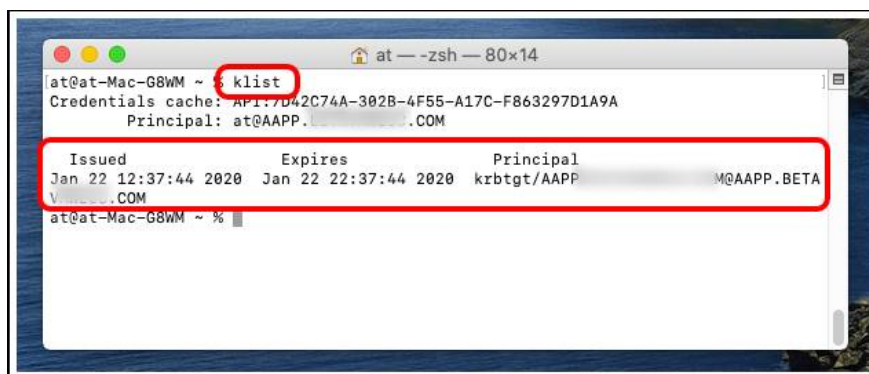
Finally, log in to Kerberos and confirm that the Kerberos credentials are obtained over Per-App VPN by the Kerberos SSO

Extension.

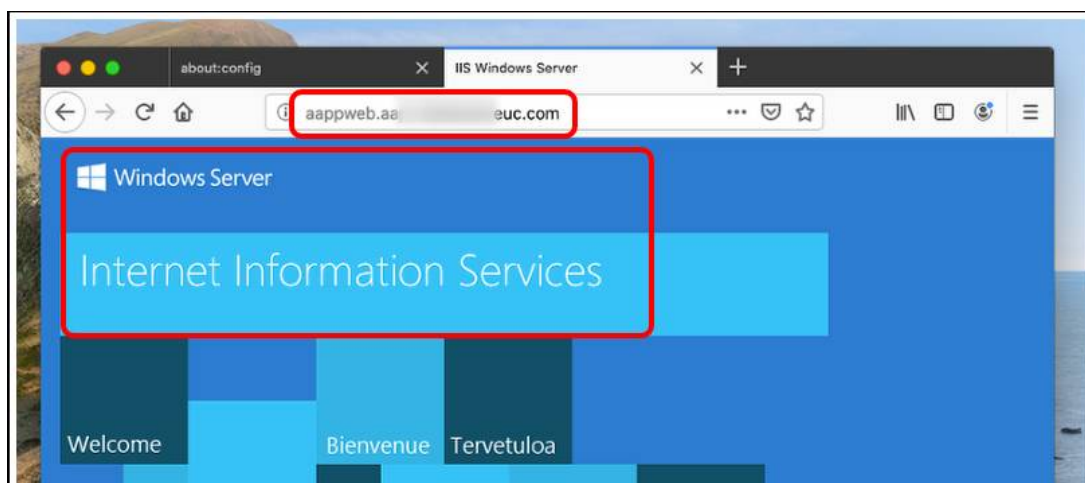
1. Log in to Kerberos extension.



- a. Click the extension (key icon) in the menu bar.
 - b. Click Sign In.
 - c. Enter a user's username and password.
 - d. Click Sign In.
2. Click **Yes** to accept automatic sign-in.
 3. Rerun klist command.



- a. In Terminal.app, enter klist and press return.
 - b. Observe the Kerberos Credential obtained over Per-App VPN by the built-in macOS Catalina Kerberos SSO Extension.
4. Validate Kerberos-enabled application or website.



- a. Launch an application which is Kerberos-enabled. If using a website, browse to the Kerberos-enabled website.

- b. Note the application or website is authenticated without any intervention from the user (no certificate chooser or username/password prompt).

Note: Some applications may require additional configuration to enable Kerberos Authentication. Google Chrome and Firefox also require additional configuration to enable Kerberos Authentication.

For Firefox:

1. Open Firefox and enter `about:config` in the address bar.
2. Search for `negotiate` and then double-click `network.negotiate-auth.trust-uris`.
3. Enter a comma-separated list of domain names that should be enabled for Kerberos Authentication and click Ok.
4. Open a new tab and re-try the Kerberos-enabled website.

For Google Chrome:

1. Create a [Custom Settings](#) payload in a User Profile for the device, targeting `com.google.Chrome` as the PayloadType.
2. Include the following keys in your settings:

```
<key>AuthServerWhitelist</key>
<string>*.domain.name</string>
<key>AuthNegotiateDelegateWhitelist</key>
<string>*.domain.name</string>
```

Caution: Some apps spawn *helper* applications to assist with background tasks. In these cases, the helper apps may be making DNS calls or performing other network tasks requiring the Per-App Tunnel but may not be part of a device traffic rule. One particular example of this is Google Chrome, which performs network functions outside the `Google Chrome.app` process. In this case, the helper application must be added to the device traffic rule, otherwise, specific settings are required to be changed client-side within the application.

As an example, to validate Kerberos-enabled websites in Google Chrome using Per-App Tunnel, perform the following:

1. In the URL field, enter `chrome://flags`
2. Search for `network` in the Search flags text box.
3. Set `Runs network service in-process` to `Enabled` and relaunch Google Chrome before proceeding with testing.

This small change allows Google Chrome to leverage the Per-App Tunnel for connectivity required to query DNS and obtain Kerberos tickets. At the time of writing, the `ForceNetworkInProcess` key was not available in Chrome for macOS and must be enabled by the individual user.

Troubleshooting Workspace ONE Tunnel on macOS

If a Per-App Tunnel problem occurs on macOS, there are a number of places to troubleshoot. This section of the tutorial covers where to troubleshoot on macOS at a high level. Depending on the problem, there might be steps that should be performed on the Unified Access Gateway. However, troubleshooting the Unified Access Gateway is outside the scope of this tutorial. Workspace ONE UEM administrators should contact VMware Support for assistance when troubleshooting Per-App Tunnel, Workspace ONE Tunnel, or the Unified Access Gateway.

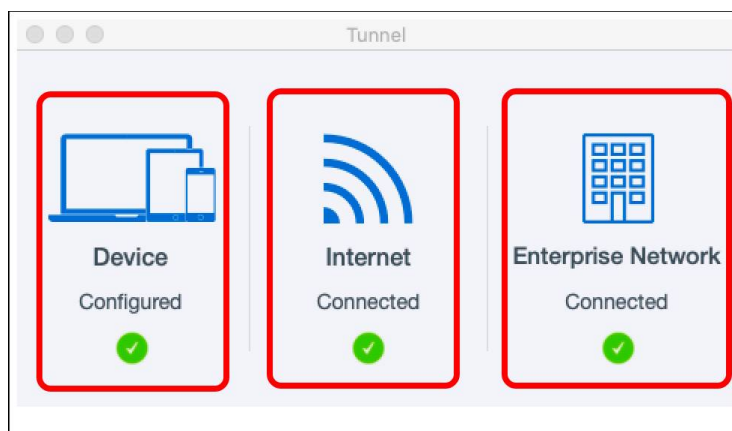
This section covers a high-level set of initial troubleshooting steps.

To begin, open Workspace ONE Tunnel. Click Launchpad and click **VMware Tunnel**.



Ensure Tunnel is Configured

1. Ensure that the **Device Configured** status shows Configured. This indicates that Workspace ONE Tunnel has received configuration data from Workspace ONE UEM. If the status is not configured, try one of the following:

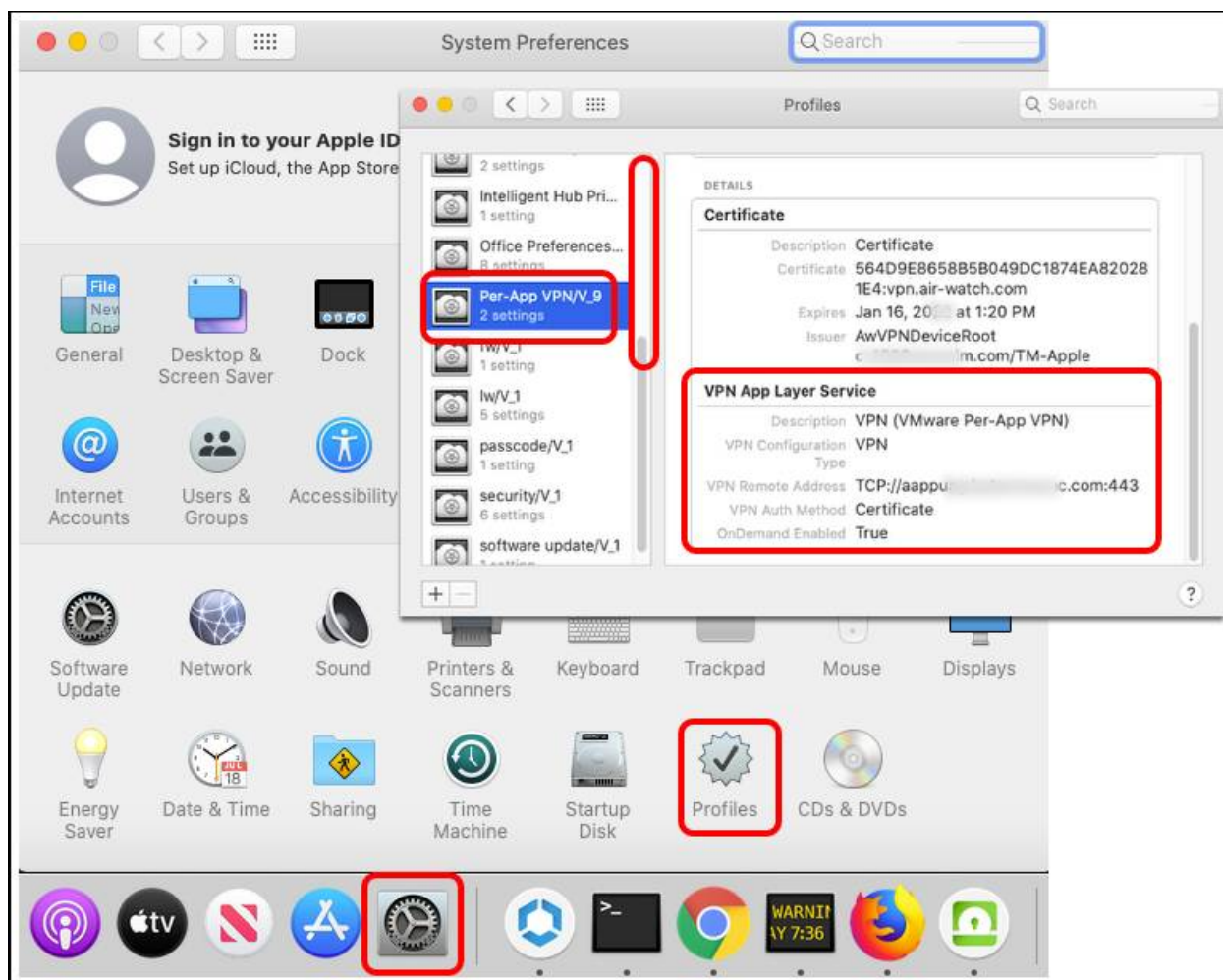


- a. Check the Device Traffic Rules and **Save and Publish** the rules again.
 - b. Check the *last seen* value for the device in the Workspace ONE UEM console. Is the device communicating with Workspace ONE UEM?
 - c. Validate that other MDM commands are being sent to the device. Create an assignment (smart) group containing the single device and attempt to send it a new profile payload.
2. Ensure that the **Internet** status shows Connected. If Tunnel cannot connect to the Internet, it probably cannot connect to the Unified Access Gateway.
 - a. Validate that the device has a working Ethernet or Wi-Fi connection (IP address, subnet mask, gateway, and DNS addresses are present).
 - b. Validate DNS resolution: Open **Terminal** and enter `nslookup uag.fully.qualified.domain` to ensure that an IP address is resolved.
 - c. Validate Connectivity to UAG: Within Terminal, enter `nc -vz uag.fully.qualified.domain uagport` (such as `nc -vz uag.company.com 443`).
 3. Ensure that the **Enterprise Network** status shows Connected. If Workspace ONE Tunnel is disconnected from the Enterprise network, apps cannot use Per-App Tunnel. This might indicate an issue with Workspace ONE Tunnel connecting to the Unified Access Gateway or an issue with Device Traffic Rules.

The remainder of this section details how to troubleshoot Tunnel connectivity.

Validate Per-App VPN Profile

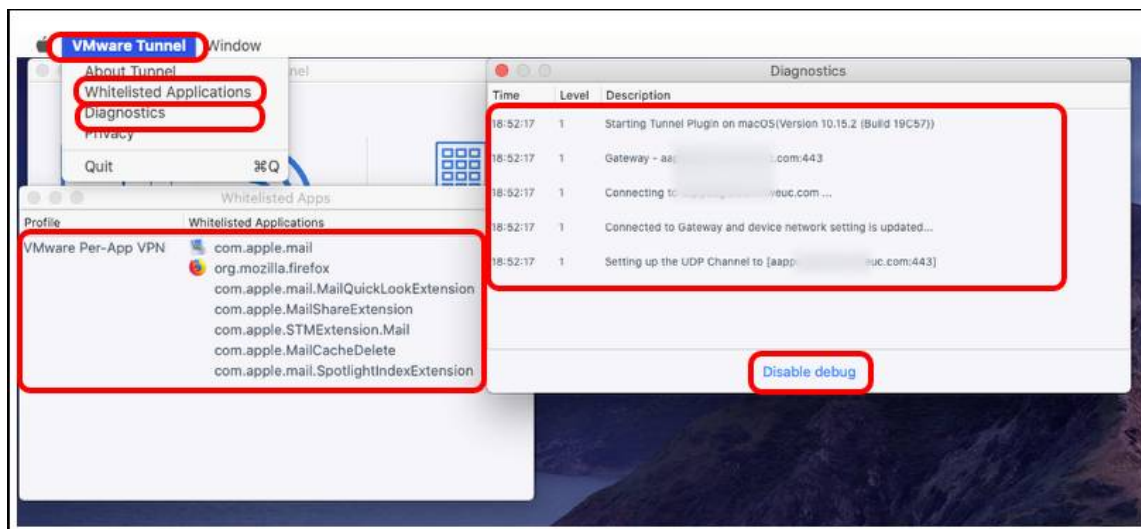
1. Click System Preferences.



2. Double-click Profiles.
3. Scroll through the left panel.
4. Click the Per-App VPN profile that was created.
5. Ensure that the VPN App Layer Service details are correct, especially the VPN Remote Address and the OnDemand Enabled value.
 - a. If the profile is missing or misconfigured, check the profile configuration and re-push the profile to the device from within the UEM Console Device Details view (on the Profiles tab).

Validate Advanced Tunnel Information

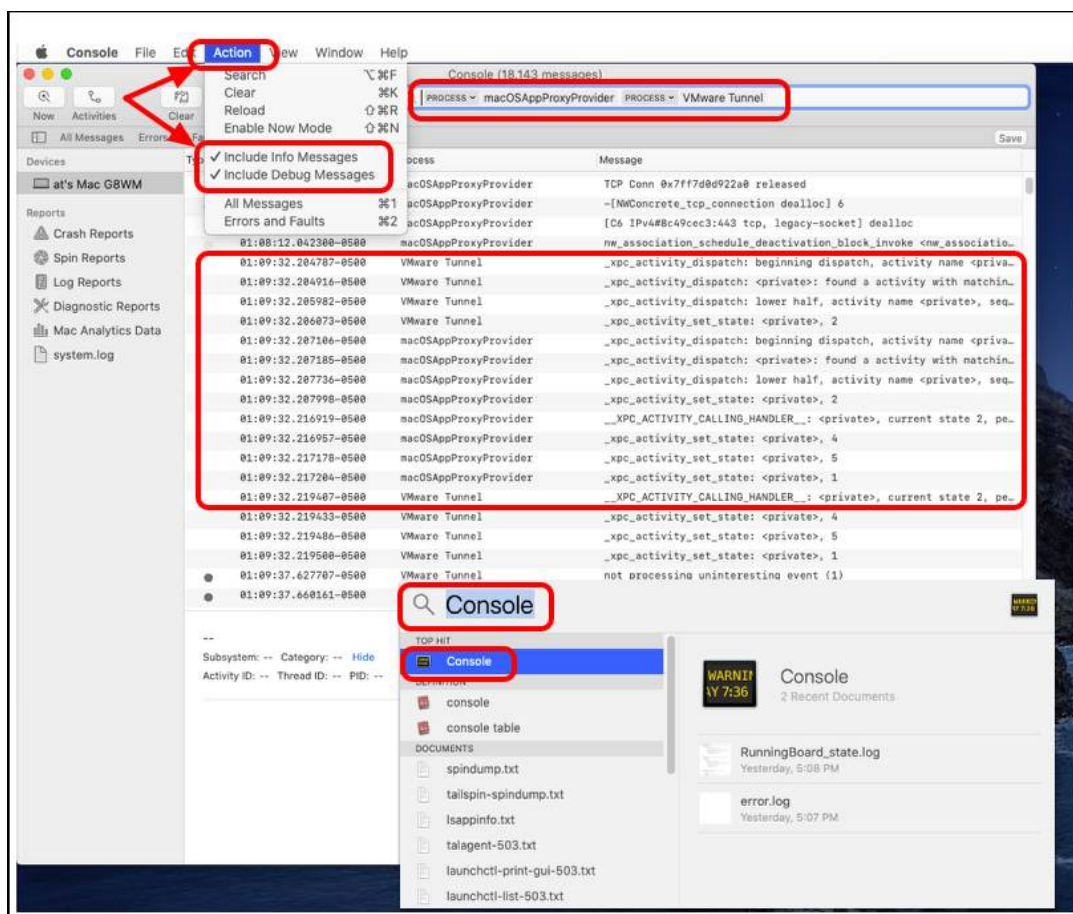
1. Open the Workspace ONE Tunnel client and click the VMware Tunnel menu.



2. Click Whitelisted Applications.
3. Verify that the list of allowlisted applications matches the settings configured in the Device Traffic Rules.
4. From the VMware Tunnel menu (#1), click Diagnostics.
5. Click Enable Debug to get verbose information.
6. Review Diagnostics information.
7. Click Disable Debug when troubleshooting is complete.

Review Tunnel-Related Unified Logging

1. Press CMD+SpaceBar (⌘+Space) and enter console into the Finder window.



2. Select the **Console** application.
3. Enter process:macOSAppProxyProvider into the search bar and press **Return** on the keyboard.
4. Without clearing the contents of the search bar, add an additional filter parameter by adding process:VMware Tunnel into

the search bar and press **Return** on the keyboard.

5. Click the **Action** menu and confirm that **Include Info Messages** and **Include Debug Messages** are selected.

6. Review the logging produced within the Console application.

Tip: If the console filters do not provide any meaningful data, you can optionally attempt to view information and debug messages from entire subsystems. Some filters that may help include:

- `process:macOSAppProxyProvider`
- `any:com.vmware.macos-tunnel`

Also, if troubleshooting Kerberos over the Per-App Tunnel, you can include the following console filters:

- `subsystem:com.apple.appssso`
- `subsystem:com.apple.appssokerberosextension`

The following Terminal command might provide meaningful output: `log stream --debug --predicate '(subsystem == "com.apple.Heimdal") OR (subsystem == "com.apple.AppSSO") OR (subsystem == "org.h5l.gss") OR (subsystem == "com.apple.network") OR (process == "VMware Tunnel") '`

General VPN Network Extension Troubleshooting

Per [Apple's Developer Website \(requires login\)](#), you can use the following commands to gather additional data from the VPN (Network Extension):

- `sudo defaults write /Library/Preferences/com.apple.networkextension.control.plist LogToFile -boolean true`
- `sudo defaults write /Library/Preferences/com.apple.networkextension.control.plist LogLevel -int 7`

Reproduce the issue and then enter this command in Terminal.app:

- `/System/Library/Frameworks/SystemConfiguration.framework/Resources/get-mobility-info`

You should find additional information in the resulting get-mobility-info output file.

You can later deactivate the logging by issuing the following commands:

- `sudo defaults delete /Library/Preferences/com.apple.networkextension.control.plist LogToFile`
- `sudo defaults delete /Library/Preferences/com.apple.networkextension.control.plist LogLevel`

Deploying Workspace ONE Tunnel for Windows Desktop

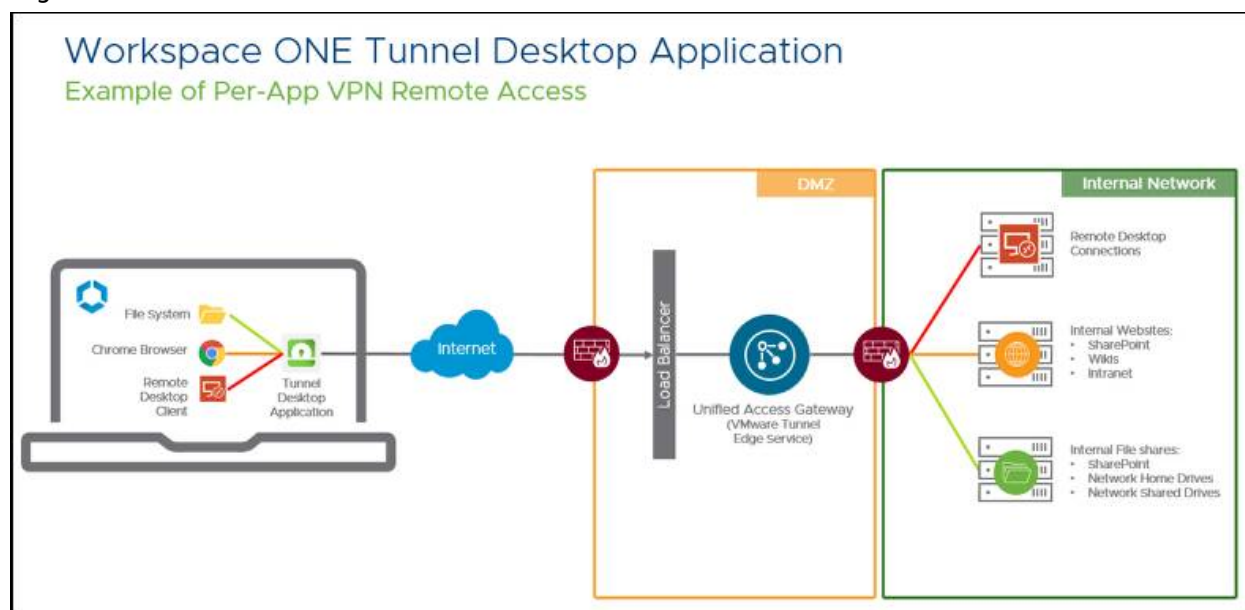
Per-App Tunneling helps users to access critical information using applications on their devices from their devices. Mobile flows help users perform business-critical tasks from a single app — streamlining the user experience.

Leveraging Per-App Tunnel allows you to control which applications are on a device and what internal resources the applications have access to by automatically activating or deactivating Per-App VPN access, based on which applications are active. By enabling remote access, you no longer need to provide a device-wide VPN on your devices, which can allow unintended or unauthorized apps or processes to access your VPN. In this tutorial, you configure and deploy VMware Workspace ONE Tunnel to enable the Per-App Tunnel component on managed devices.

These exercises involve the following components:

- **Workspace ONE Tunnel** – The app used on the device to securely connect to the Unified Access Gateway to provide Per-App Tunnel functionality, also referred to as Tunnel Client.
- **Unified Access Gateway** – The virtual appliance where the VMware Tunnel edge service is installed, and to which the tunnel client connects.
- **Per-App Tunnel** – Component of VMware Tunnel edge service for connecting to a secure tunnel channel on a per-application basis, which is controlled and configured by the VPN profile payload and Device Traffic Rules.
- **Per-App VPN Profile and Device Traffic Rules** – The Workspace ONE UEM configuration is pushed to the device that contains the Per-App Tunnel configurations. Every time a specified application is opened, the Workspace ONE Tunnel client evaluates the Device Traffic Rules assigned to it before making any routing decisions and establishes a Per-App tunnel connection with the Unified Access Gateway based on the Per-App VPN Profile configuration.

High-Level Architecture



The device contains the applications required by the end-user to perform their daily job. Some applications require access to internal resources to function. Those applications, based on Per-App VPN configuration, use Workspace ONE Tunnel which communicates with the Tunnel Service on Unified Access Gateway hosted on the DMZ, to validate if the device requesting access is in compliance or not before authorizing access through the internal resource.

Prerequisites

Before you can perform the steps in this exercise, you must have the following components installed and configured:

- Workspace ONE UEM 2203+
- Windows 10 1704+ or Windows 11+ enrolled in Workspace ONE UEM
- **Latest version** of the Workspace ONE Tunnel Desktop Application
 - Download the installer file: [Workspace ONE Tunnel](#)
 - For more information, see [Supported Platforms for VMware Workspace ONE Tunnel](#)

- VPN tunnel must be configured before you can add it as an application

Note: See [VMware Workspace ONE Tunnel for Windows Release Notes](#) for updates to the client.

Configuring Device Traffic Rules for Windows

This exercise outlines how to configure device traffic rules for Windows. Before you start this section, read the *Device Traffic Rules* chapter for a better understanding of how device traffic rules are managed by Workspace ONE Tunnel.

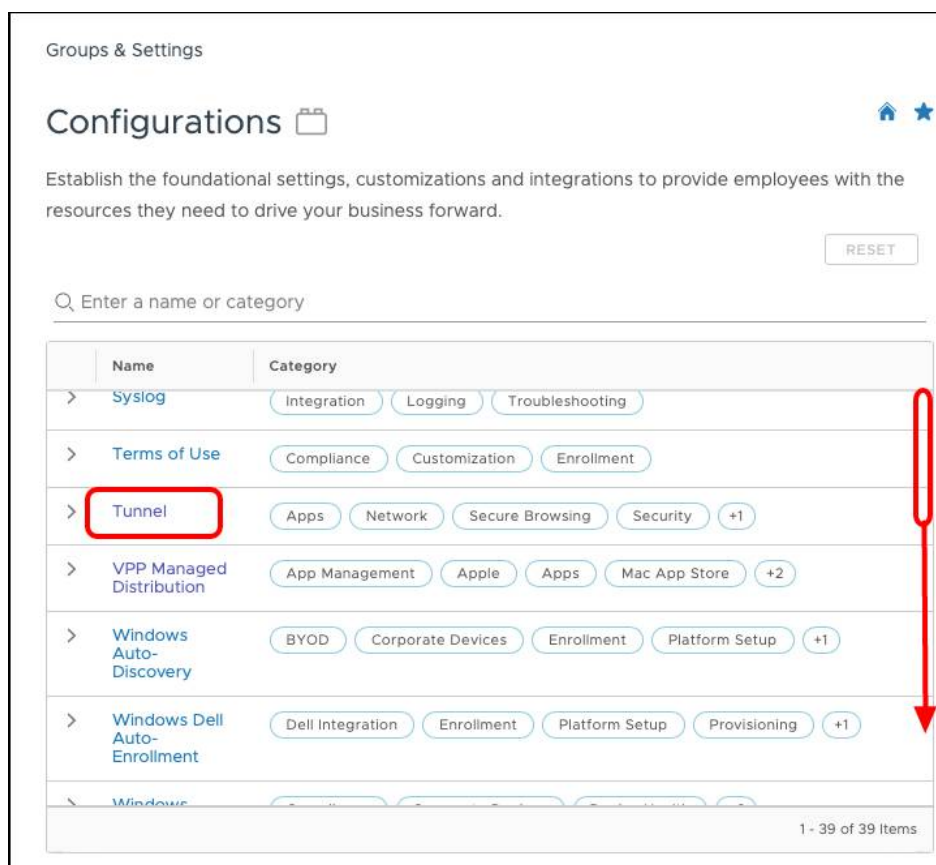
For this example, the user must access internal websites, internal network file shares, and a remote desktop session. To allow secure access, you configure Workspace ONE Tunnel to allow only the applications required.

In this exercise, you configure the following:

- Internal web browser access - defining Chrome as the application
- Internal network file shares - allowing system access
- Remote Desktop Session Connection - defining Microsoft Remote Desktop client as the application

Note: Domain values used in this section are examples only. Your values will differ.

1. Access configurations.
 - a. In the Workspace ONE UEM console, click **Groups & Settings**.
 - b. Click **Configurations**.
2. Scroll through the list of configurations and select **Tunnel**.



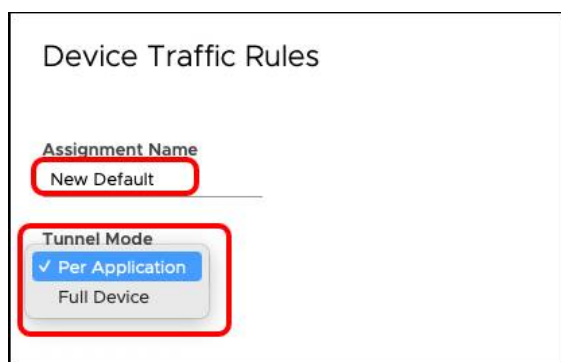
3. Edit Device Traffic Rule sets.
 - a. From within the Device Traffic Rules information block on the *Tunnel Configuration* page, click **Edit**.
4. Add or modify device traffic rule set.



Introduced in Workspace ONE UEM 2011, Device Traffic *Rule Sets* expand the functionality of device traffic rules allowing for granular assignment of rule sets to different groups of users and devices. Device Traffic Rule Sets are assigned when creating the per-app VPN profile in a later step.

To get started with Device Traffic Rule Sets, perform the following in the *Manage Traffic Assignments* screen:

- a. If no other Device Traffic Rule Sets exist (or a new rule set is required), click **Add** to create a new Device Traffic Rule Set.
- b. If modifications to an existing rule set are required, click the Device Traffic Rule Set name.
5. Set or modify device traffic rule name and tunnel mode.



- a. Enter a name for the Device Traffic Rule Set (or if necessary, modify the name of an existing rule set).
- b. Set the Tunnel Mode to Per Application.

This first tutorial on Windows shows you how to configure device traffic rules based on Per-Application Tunnel Mode. After completing the Windows tutorial return and switch the Tunnel Mode for this rule to Full Device. The Application fields will be removed and you will be required to specify only the actions and destination domains.

6. Click **Manage Applications**.
7. Click **Add**.
8. Define the application.

- a. Select Windows as the Platform.
 - b. Enter the friendly name of the application. The friendly name is displayed in the Device Traffic Rule.
 - c. Select the App Type, for example, Desktop App. The App Type can be a traditional Windows application or a Windows Store application.
 - d. Enter the App Identifier. For traditional Windows applications, use the File Path. For Store applications, you must enter the Package Family Name or PFN. You can use the PowerShell command `Get-AppxPackage` to find the PFN. For more information, see [Microsoft Docs: Find a package family name \(PFN\) for per-app VPN](#).
9. Add Chrome Web browser access.

- a. In this example, the Chrome application is defined under the Program Files (x86) path. The App Identifier value should contain the full path where the EXE file is located on the Windows machine.
 - b. The screenshot shows that the App Identifier used for Chrome is `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`
 - c. After you have entered the application details, click **Save**.
10. Add remote desktop (RDP) client.

Add Application

Add application details for setting app traffic policies.

Platform * Windows

Friendly Name * RDP

App Type * Desktop App

App Identifier * C:\Windows\System32\mstsc.exe ⓘ

CANCEL SAVE

- a. Next, add the Remote Desktop client. This allows end users to connect to Remote Desktop Hosts located behind the corporate firewall.
 - b. As the Remote Desktop Client is built into the Windows Operating system, the file path of the executable is different.
 - c. For example, in this screenshot, the App Identifier used for the RDP client is C:\Windows\System32\mstsc.exe
 - d. After you have entered the application details, click **Save**.
11. Add SMB for network drive and printer support.

Add Application

Add application details for setting app traffic policies.

Platform * Windows

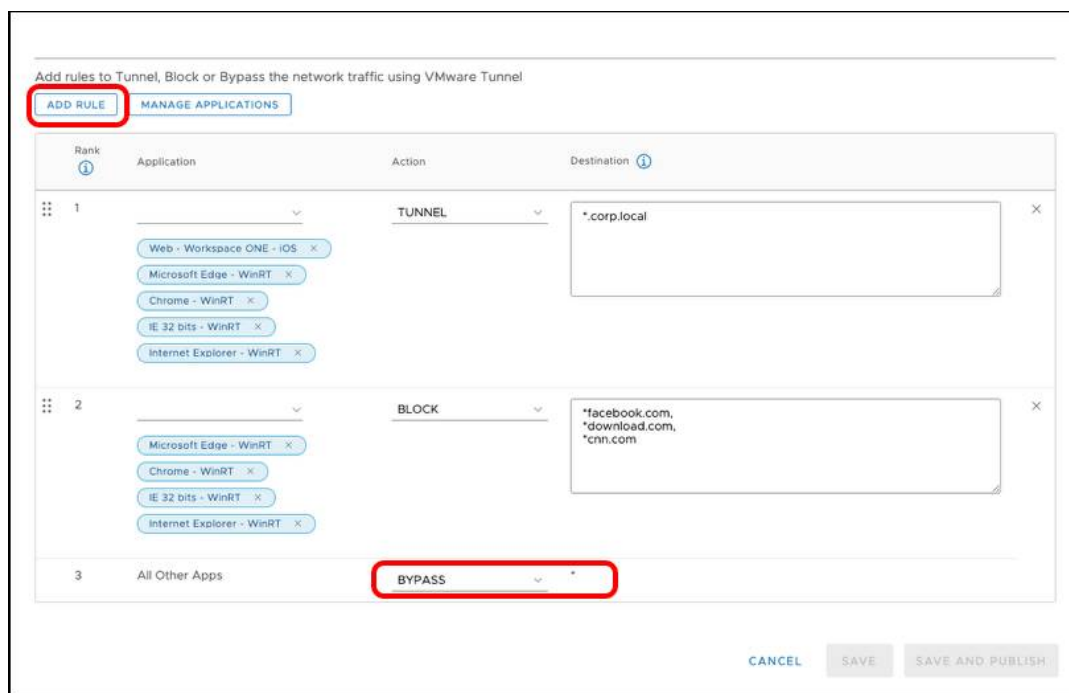
Friendly Name * System

App Type * Desktop App

App Identifier * System ⓘ

CANCEL SAVE

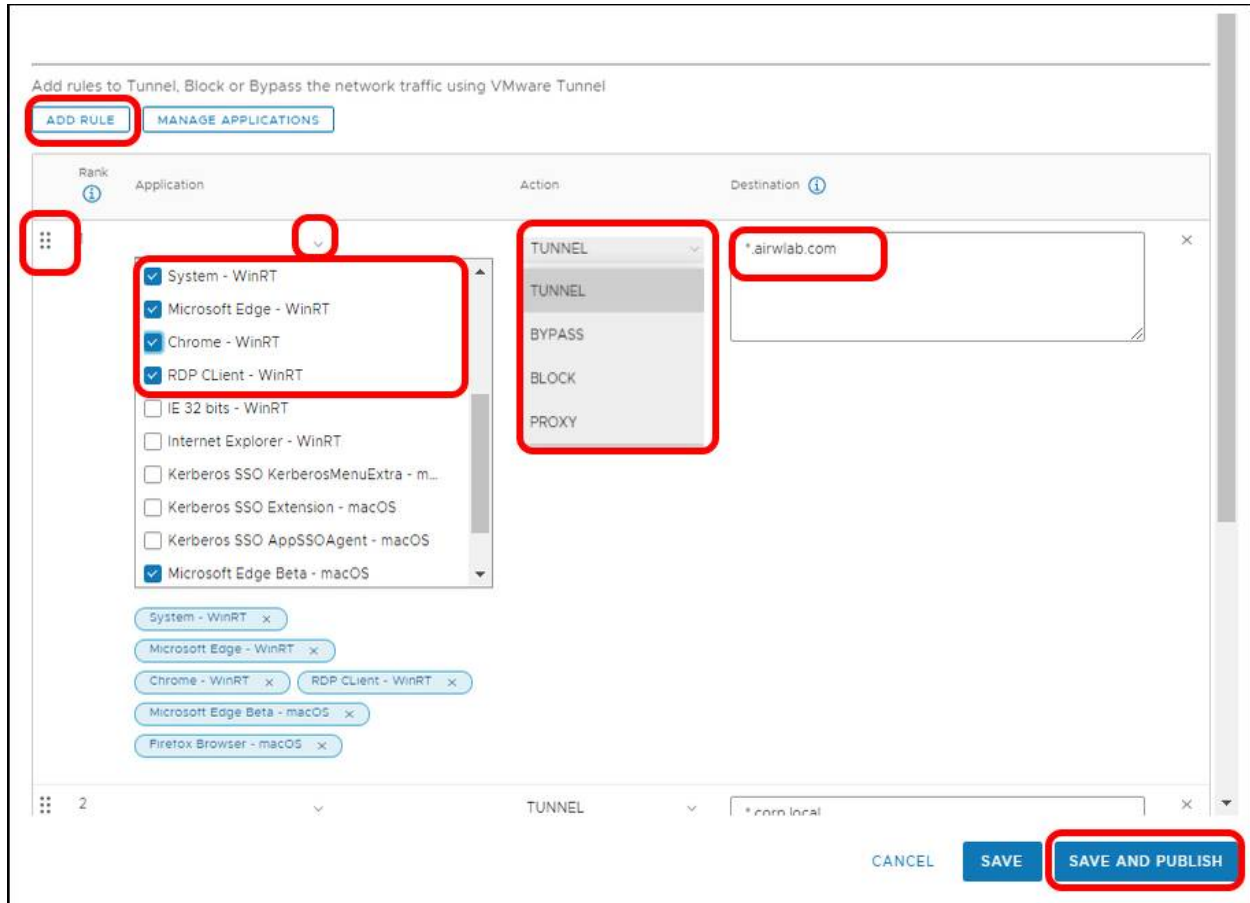
- a. Next, add support for tunneling SMB traffic from the system to allow users to map network shares and network printers. This allows end users to connect to file shares and printers that are located behind the corporate firewall.
 - b. As the SMB protocol is built into the Windows Operating system, the App Identifier is not an executable, instead, you define System as the App Identifier.
 - c. After you have entered the application details, click **Save**.
12. Add more applications to device traffic rules, if required.
- a. If more applications are needed for the ruleset, click Add and repeat starting at *Define the Application*.
 - b. If all the required applications have been defined, click X to close the Manage Applications window.
13. Add device traffic rule.



- a. Observe (and optionally modify) the default action which applies to all Windows applications.
 - i. Tunnel – All apps on the device configured for Per-App Tunnel send network traffic through the tunnel. For example, set the Default Action to Tunnel to ensure all configured apps without a defined traffic rule use the Workspace ONE Tunnel for internal communications.
 - ii. Block – Blocks all apps on the device configured for Per-App Tunnel from sending network traffic. For example, set the Default Action to Block to ensure that all configured apps without a defined traffic rule cannot send any network traffic regardless of destination.
 - iii. Bypass – All apps on the device configured for Per-App Tunnel bypass the tunnel and connect to the Internet directly. For example, set the Default Action to Bypass to ensure all configured apps without a defined traffic rule bypass the Workspace ONE Tunnel to access their destination directly.

b. Click Add Device Traffic Rule.

14. Build device traffic rule.

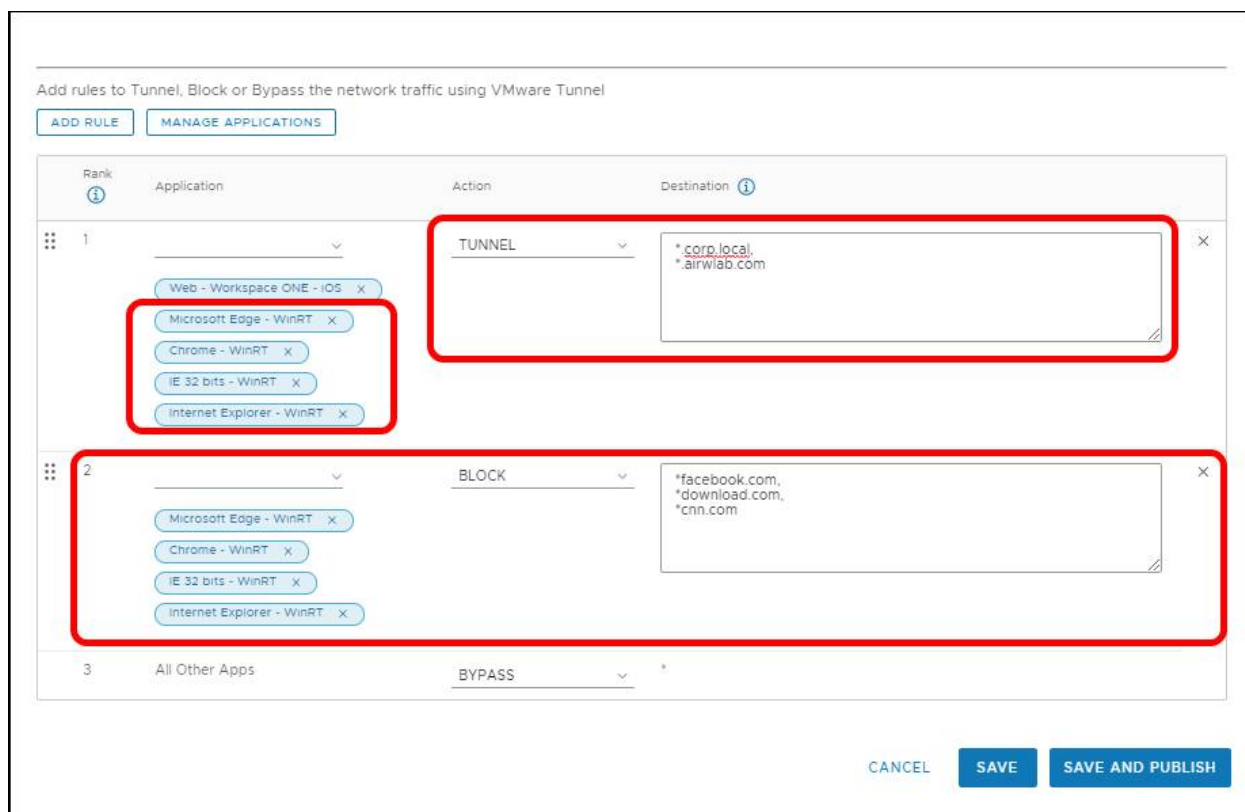


- a. In the newly created traffic rule, Click the down arrow to display the Application list.
- b. Select one or more triggering applications to control with this rule. All Applications not applicable to Windows.
- c. Select the Appropriate Action for Workspace ONE Tunnel to perform on traffic from the selected apps - For this exercise, select Tunnel.
 - i. Tunnel – Sends app network traffic for specified domains through the tunnel to your internal network.
 - ii. Block – Blocks all traffic sent to specified domains.
 - iii. Bypass – Bypasses the Workspace ONE Tunnel so the application accesses specified domains directly.
 - iv. Proxy – Redirect traffic to the specified HTTPS proxy for the listed domains. The proxy must be HTTPS and must follow the correct format: <https://example.com:port>.
 - v. Note: Proxy is not yet supported using the Workspace ONE Tunnel Desktop Application.
- d. Enter one or more comma-separated fully qualified domain names as destinations to which Workspace ONE Tunnel should apply the Device Traffic Rule. A single asterisk (*) can be used as a wild card for subdomains.
- e. If necessary, adjust the Device Traffic Rules rank in the list. Lower-numbered rank is the highest priority.
- f. If necessary, click Add Rule and repeat *Build Device Traffic Rule* until you have added all the necessary Device Traffic Rules for your organization.
- g. Click Save.

For more information on the formats (wildcards, IP, ports) allowed into the Destination field, see the *Device Traffic Rules Destination formats supported* chapter.

Note: For Windows Desktop devices, if Enhanced Domain Resolution is not enabled on the Per-App VPN profile, the domains added to the destination must also be added to the list of domains part of the DNS Resolution via Tunnel Gateway.

15. Review the summary of the device traffic rule configurations.



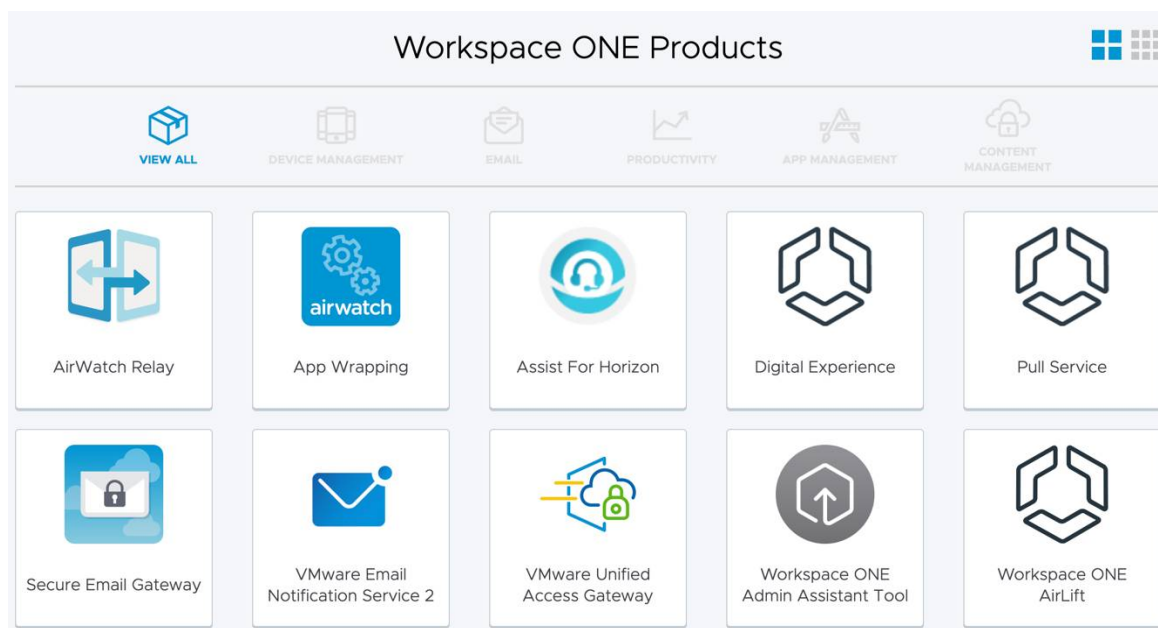
- a. The **Application** list contains triggering applications **Chrome**, **Remote Desktop**, and **System**.
 - i. The applications appear in the following format: **Application Friendly Name - UEM Organization Group - Platform**
 1. Google Chrome - ACME Corp - WinRT
 2. RDP - ACME Corp - WinRT
 3. System - ACME Corp - WinRT
- b. The Appropriate **Action** for Workspace ONE Tunnel to perform is **Tunnel**.
 - i. **Tunnel** - Sends app network traffic for specified domains through the tunnel to your internal network
 - ii. **Destination** - For this example, the domains are *.corp.local and *.airwlab.com
- c. **Optional** - You can also configure Device Traffic Rules to **Block**.
 - i. In this example, Chrome is set to block domains *.cnn.com, *.facebook.com, and *.match.com.

Distributing Workspace ONE Tunnel for Windows

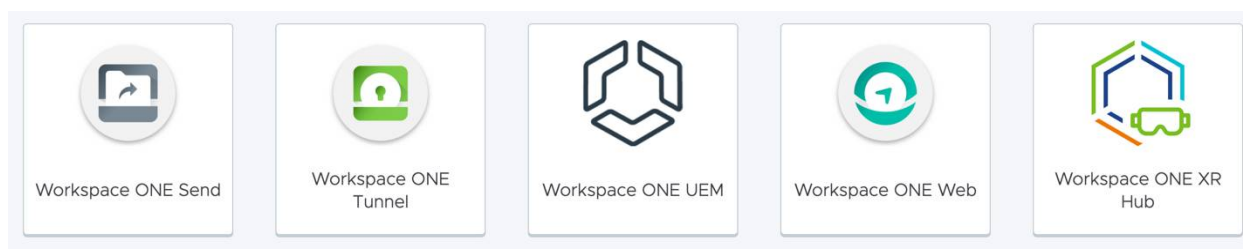
In this exercise, you deploy the Workspace ONE Tunnel Desktop Application on Windows 10 devices.

Note: The Per-App VPN profile should already be configured as part of the Prerequisites.

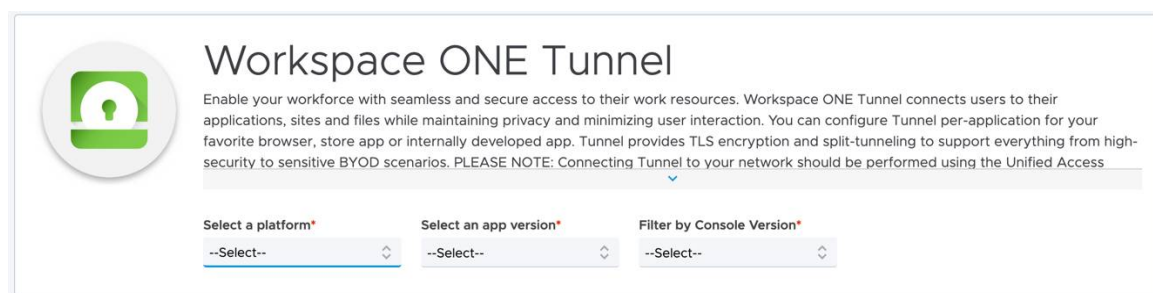
1. Download the Workspace ONE Tunnel desktop installer.



- a. Navigate to <https://my.workspaceone.com/products> and log in with your VMware Customer Connect credentials.
 - b. Click View All.
2. Scroll to the end of the page and select **Workspace ONE Tunnel**.



3. Select platform and version.



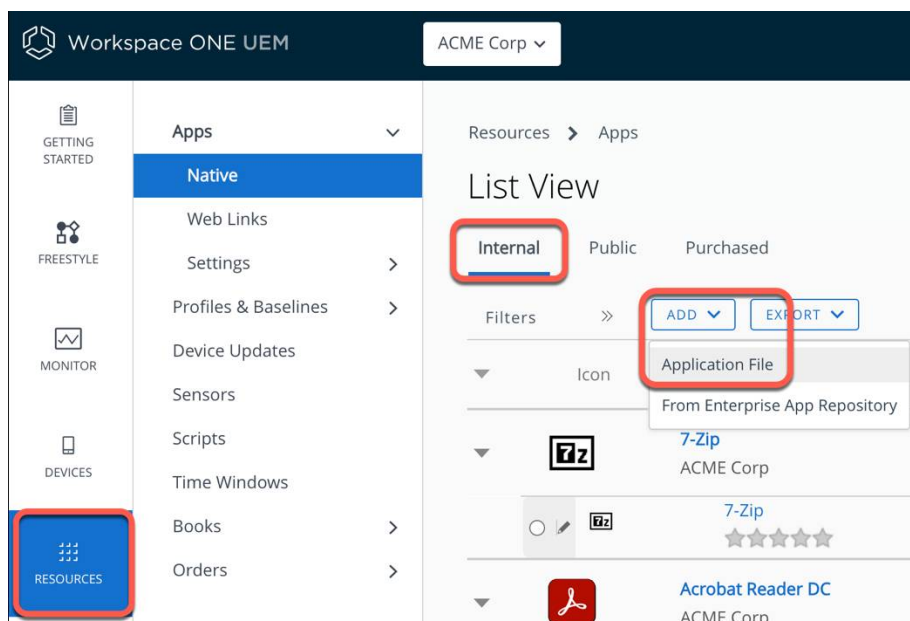
- a. Select Windows as the platform.
- b. Select the Latest version for the Workspace ONE Tunnel Desktop Application.
- c. Filter by console version.
- d. Select Install and Upgrades tab for a link to the download.

After you have Accepted the Terms of Use, the download should begin immediately.

Tip: It is helpful to have all Installation files pre-downloaded on your local machine, ready to upload into Workspace ONE UEM.

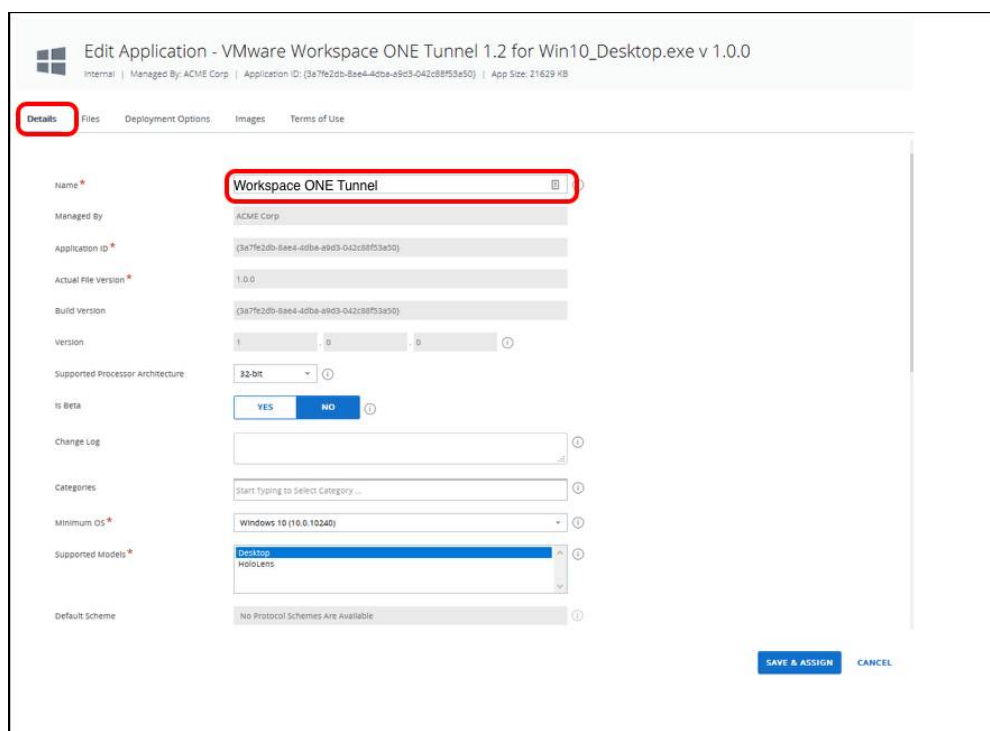
To improve user experience, have the application icons and screenshots of the application ready for the Application catalog.

4. Upload Tunnel application into Workspace ONE UEM.



- a. In the Workspace ONE UEM console, click **Resources**.
- b. Select Internal Application.
- c. Click Add > Application File and Upload.
- d. Browse for the Workspace ONE Tunnel EXE installer file and click Save.
- e. Select No for Is this a dependency app?.
- f. Click Continue.

5. On the Details tab, enter a name. For example, **Workspace ONE Tunnel**.



6. On the Files tab, Scroll down to find the **App Uninstall Process** section. For VMware Tunnel, enter VMware Workspace ONE Tunnel 1.2 for Win10_Desktop.exe /uninstall /Passive as the Uninstall Command.

Internal | Managed By: ACME Corp | Application ID: {3a7fe2db-8ae4-4dba-e9d3-042c88f53a50} | App Size: 21629 KB

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

Application File * VMware Workspace ONE Tunnel 1.2 for Win10_Desktop.exe

App Dependencies

No Dependencies files were found for this organization group. If you wish to deploy other applications before installing this app, please upload the dependent files as separate applications and come back to this page.

> App Transforms

> App Patches

App Uninstall Process

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

Custom Script Type *

Uninstall Command * VMware Workspace ONE Tunnel 1.2 for Win10_Desktop.exe /uninstall /Passive

7. Configure the Deployment Options tab.

Internal | Managed By: ACME Corp | Application ID: {3a7fe2db-8ae4-4dba-e9d3-042c88f53a50} | App Size: 21629 KB

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

When To Install

Data Contingencies ⓘ

Disk Space Required 0 KB ⓘ

Device Power Required 0 ⓘ

RAM Required 0 MB ⓘ

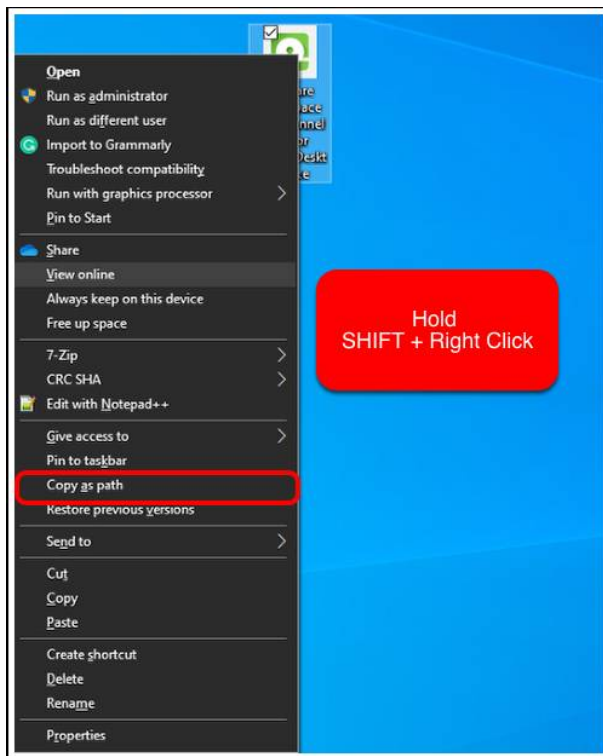
- a. Select the Deployment Options tab.
- b. Locate the When to Install section.
- c. Configure any minimum requirements for the following:
 - i. Data Contingencies - Use where criteria type needs to check for existing/non-existing Applications, Files or Registry Keys.
 - ii. Disk Space Required - Which specifies the amount of disk space the device must have available to install the application.
 - iii. Device Power Required - Which specifies the battery power, in percentage, that the device must have to install the application.
 - iv. RAM Required - Which specifies the amount of RAM the device must have to install the application.

8. Find the Install command options.

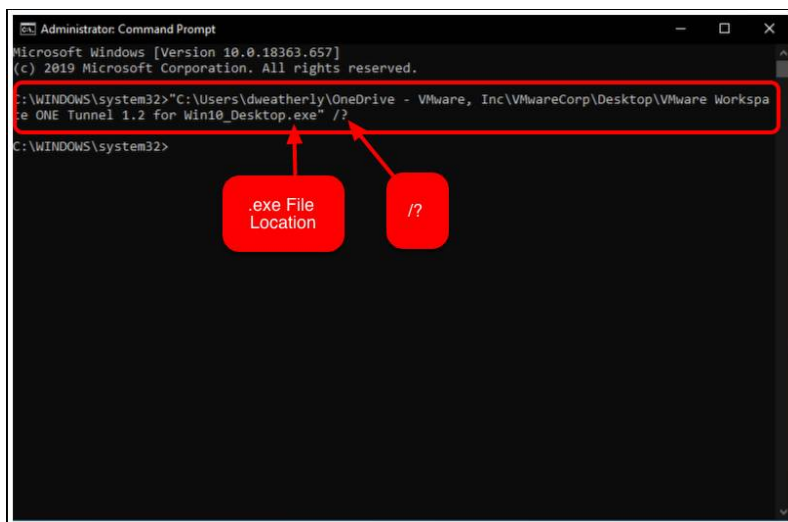
Some application installers may contain help options. Find help options by running the application file and adding /help or /? to the end of the file.

The following steps demonstrate how to run these commands.

- a. Find the installer file.



- b. Hold SHIFT + Right-click the installer file.
c. Hold Select Copy As Path.
d. Open Command Prompt.



- e. Paste in the installer file location, adding /help or /? to the end.
f. This should show a dialog box to show supported installation commands.

The results of running the command are shown in the screenshot. This example shows the supported Workspace ONE Tunnel Desktop Application Install parameters.

9. Define How to Install.

Edit Application - VMware Workspace ONE Tunnel 1.2 for Win10_Desktop.exe v 1.0.0
Internal | Managed By: ACME Corp | Application ID: (3a7fe20b-8ae4-4dba-e9d3-042c88f53e50) | App Size: 21629 KB

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

How To Install

Install Context: **DEVICE** **USER**

Install Command*: VMware Workspace ONE Tunnel 1.2 for Win10_Desktop.exe /install /Passive

Admin Privileges: **YES** **NO**

Device Restart: User Engaged Restart

Number of days after which device automatically reboots*: 7

Retry Count*: 3

Retry Interval*: 5

Install Timeout*: 60

Installer Reboot Exit Code: 3010

Installer Success Exit Code: 0

- Under Deployment Options tab, scroll down to find the How To Install section.
- For the Install Command, enter VMware Workspace ONE Tunnel 1.2 for Win10_Desktop.exe /Install /Passive.
- Ensure Admin Privileges is set to **Yes**.
- Change **Device Restart** if required. This example uses **User Engaged Restart**. This allows the user to reboot the machine to complete the install when the user is ready.
- For Installer Reboot Exit Code, the supported values are 3010 and 1641.
- For Installer Success Exit Code, the supported values are 0 and 3010.

Error Code	Value	Description
ERROR_SUCCESS	0	The action completed successfully.
ERROR_SUCCESS_REBOOT_INITIATED	1641	The installer has initiated a restart. This message indicates success.
ERROR_SUCCESS_REBOOT_REQUIRED	3010	A restart is required to complete the install. This message indicates success. This does not include installs where the ForceReboot action is run.

10. Define When to Call Install Complete.

When To Call Install Complete

Identify Application By*

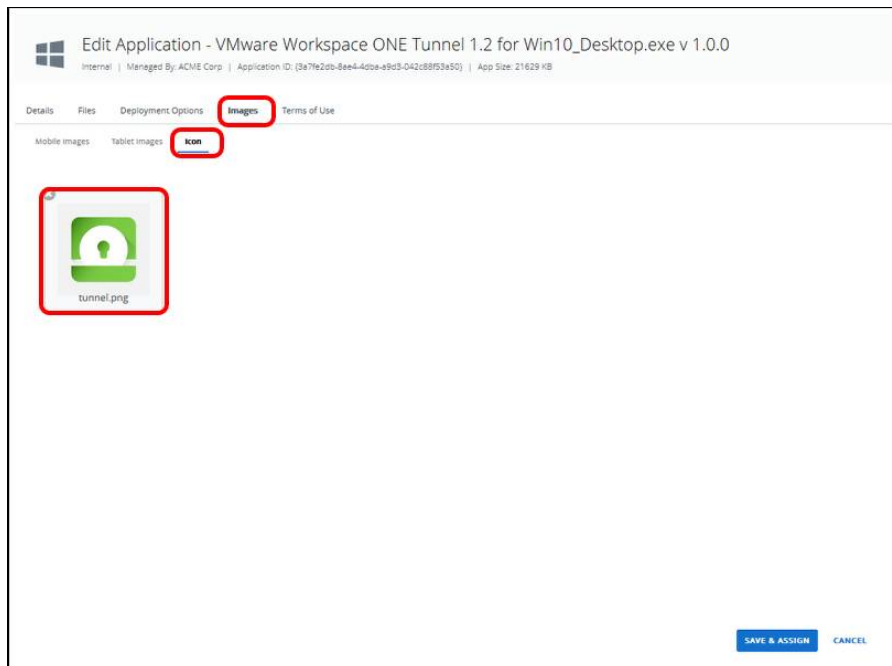
DEFINING CRITERIA **USING CUSTOM SCRIPT**

1. File exists - C:\Program Files\VMware\Workspace ONE Tunnel\VMwareTunnel.exe

SAVE & ASSIGN **CANCEL**

- Click **Add**.
- Select **File Exists** for the **Criteria Type**.
- Enter C:\Program Files\VMware\Workspace ONE Tunnel\VMwareTunnel.exe for the **Path**.
- Click **Add**.

11. Add the application icon.



- a. Select the Images tab.
- b. Select the Icon tab.
- c. Click the area labeled Click or drag files here.
- d. Navigate to the folder containing the Application logo, or download the provided image to use.

12. Set Terms of Use.

- a. Select the Terms of Use tab.
- b. If you decide to have a Terms of Use that your users must accept before installing applications, you can configure that here. For this exercise, select None.
- c. Click Save & Assign.

13. Select **Assignments** and click **Add Assignment**.

14. Configure the assignment.

15. Click **Add Assignment**.

16. Configure application distribution settings.

Workspace ONE - Tunnel - Assignment

Distribution

Restrictions

Name * ACME Corp

Description Assignment Description

Assignment Groups * To whom do you want to assign this app?
ACME Corp (ACME Corp) X

Deployment Begins * 01/28/2020 12:00 AM (GMT-05:00) Eastern Time (US & Canada)

App Delivery Method * ☐ Auto ☒ On Demand

Allow User Install Deferral ☐

Display in App Catalog ☒

CANCEL SAVE

- Give the application assignment a name.
 - Select the Select Assignment Groups search box and select an assignment group, for example, (Acme Corp).
 - Select On-Demand for the App Delivery Method.
 - Select Show for Display in App Catalog.
 - Navigate to the Restrictions Tab.
 - Enable for Make App MDM Managed if User Installed.
 - Select Save then click Save and Publish.
17. Confirm that the application appears in List View.

Resources > Apps

List View

Internal Public Purchased

Filters >> ADD EXPORT LAYOUT EXPORT Search List

Icon	Name	Version	Platform/OS/Model	Renewal Date	Install Status	Status	Source
7-Zip 19.00 (x64 edition)	ACME Corp	1 version(s)	Windows Desktop/Windows ...				
7-Zip 19.00 (x64 editio		19.0.0		Not Applicable	Assign	✓	Unknown
Workspace ONE - Tunnel	ACME Corp	1 version(s)	Windows Desktop/Windows ...				
Workspace ONE - Tun		1.0.0		Not Applicable	View	✓	Unknown
Workspace ONE Assist	ACME Corp	1 version(s)	Windows Desktop/Windows ...				
Workspace ONE Assis		5.2.0		Not Applicable	View	✓	Unknown

a. On the Internal applications List View, confirm that the Workspace ONE Tunnel Desktop Application is displayed. You have successfully added the Workspace ONE Tunnel Desktop Application to Workspace ONE UEM for deployment.

Creating Per-App VPN Profile for Windows Desktop

On Windows Desktop, VMware Tunnel can force selected applications to connect through your corporate VPN.

In this exercise, you configure the Windows Desktop profile which configures the tunnel client on the device to allow only designated applications to access content on internal servers.

Log in to the Workspace ONE UEM console to perform the next steps.

1. Click **Add** and click **Profile**.
2. Select **Windows**.
3. Select **Windows Desktop**.
4. Select **Device Profile**.
5. Configure the General settings.

Windows VPN Profile

Find Payload

General

Password

Wi-Fi

VPN

Credentials

Restrictions

Defender Exploit Guard

Data Protection

Windows Hello

Firewall (Legacy)

Firewall

Anti-Virus

Encryption

Windows Updates

Proxy

OEM Updates

SCEP

Application Control

Windows Licensing

BIOS

Kiosk

Personalization

Peer Distribution

Unified Write Filter

Custom Settings

General

Workflows that include this profile, use the assignment and deployment settings defined in that workflow.

Name * Windows VPN Profile

Version 25

Description

Deployment Managed

Assignment Type Auto

Allow Removal Always

Managed By ACME Corp

Smart Groups

- All Windows device (ACME Corp)
- Start typing to add a group

Exclusions

NO YES

VIEW DEVICE ASSIGNMENT

Additional Assignment Criteria

☐ Enable Scheduling and Install only during selected time periods

Removal Date M/D/YYYY

ADD VERSION SAVE AND PUBLISH CANCEL

- a. Select the **General** tab.
 - b. Enter a Name, for example, Per App VPN.
 - c. Select **Assignment type**. This example uses **Auto**, so devices automatically receive the policy.
 - d. Assign the policy to a **Smart Group(s)**.
6. Add and configure VPN payload.

VPN

Connection Info

Connection Name *

Connection Type *

Server *

Device Traffic Rules

Desktop Client ☒ ENABLE ☐ DISABLE ⓘ

Custom Configuration

Custom Configuration XML ⓘ

Trusted Network Detection ⓘ

DNS Resolution via Tunnel Gateway

Enhanced Domain Resolution ☒ ENABLE ☐ DISABLE ⓘ

SAVE AND PUBLISH **CANCEL**

- a. Select **VPN** from the payload menu and click **Configure**.
 - b. Enter a Connection Name for the policy, for example, Corp VPN.
 - c. Select Workspace ONE Tunnel from the Connection Type drop-down menu.
 - d. Choose the Device Traffic Rule Set (as configured in Configuring Device Traffic Rules for Windows 10) to be assigned via this Profile Payload.
 - e. Select Enable for Desktop Client - This enables the Workspace ONE Tunnel Desktop Application, otherwise it will use the Windows UWP client, no longer recommended.
 - f. Configure Custom Configuration XML as needed. Refer to *Custom Configuration XML for Windows Desktop* for additional details on the list of Custom Configuration parameters available.
 - g. Select Enable for the Enhanced Domain Resolution located under DNS Resolution via Tunnel Gateway.
 - h. Click Save & Publish.
7. Click **Publish** to publish the VPN profile.

Custom Configuration XML for Windows Desktop

Custom Configuration allows the administrator to determine the behavior of the Tunnel Client on the device, from initialization process, UI elements and network behaviour.

As example, the following XML configuration allows the end user to turn on/off (ToggleTunnelFeature) the Tunnel from the tray icon, and change the Tunnel connection (OnDemand) from an on-demand basis to always connected.

```
<?xml version="1.0" encoding="utf-16"?>
<CustomConfiguration>
  <ToggleTunnelFeature>true</ToggleTunnelFeature>
  <OnDemand>>false</OnDemand>
</CustomConfiguration>
```

The result of this XML configuration reflects on the UI of the Tunnel Windows Client showing an option to enable/disable the Tunnel

Client, and for the OnDemand connection it determine the Tunnel internal behaviour as always be connected.

Several other parameters that can be customized to change the Tunnel behavior, the following table list the custom configuration parameters supported and their respective Tunnel Mode. For additional information visit the [Configure Tunnel Profile for Windows Desktop Client](#) in the VMware documentation.

Custom Configuration XML tag syntax	Description	Tunnel Mode
Format <ServerCertSN>{Subject CN Name}</ServerCertSN> For Wildcard Certificate <ServerCertSN>*.airwlab.com</ServerCertSN> For SAN Certificates mention the complete Subject Alternate Name <ServerCertSN>tunnel.airwlab.com</ServerCertSN>	Required when using Third-Party SSL certificate for the Tunnel Server Certificate. This applies only to SAN Certificate and Wildcard certificate. To retrieve the subject CN name: 1. Open the certificate on a Windows machine. 2. Select the Details tab. 3. The Subject row contains the CN of the cert.	Per-App and Full Device
<DnsSearchDomain>domain.com</DnsSearchDomain>	List of DNS search domains in comma-separated values	Per-App and Full Device
<TrustedNetworkProbeUrl>https://probeurl, http://probeurl2</TrustedNetworkProbeUrl>	List of probe URLs used by the Desktop client to consider if it is connected to a trusted network based on the reachability. Supported schemes: http:// & https:// or IP Addresses http://10.0.0.1	Per-App and Full Device
<ExcludeFQDN>host1.com,host2.com</ExcludeFQDN>	Comma separated list of hostnames whose resolution should not be tunneled	Per-App
<ToggleTunnelFeature>true/false</ToggleTunnelFeature>	Default is false. When set to true, users will be given an option to Enable and Disable tunnel client service OnDemand from the system tray icon. The Tunnel Client Service will be up when the user deactivates from the tray icon, but the Tunnel client will not intercept any traffic. When the user enables the Tunnel Client from the tray icon the tunnel client will be ready to intercept the traffic and tunnel the requests.	Per-App and Full Device
<OnDemand>true/false</OnDemand>	Default is true. When set to true, Tunnel Client will connect when required based on incoming requests from the apps, like user trying to browser. If there is not traffic for 5 minutes, Tunnel Client will disconnect automatically. When set to false, Tunnel Client will be always connected.	Per-App and Full Device
<StartTunnelPreLogon>true/false</StartTunnelPreLogon>	Default is false. Use this attribute to enable the Tunnel service to start before you login. This parameter is useful for specific domain authentication scenarios, such as dropship provision where Tunnel needs to start before the user logon.	Per-App and Full Device
<PreferExternalDNS>true/false</PreferExternalDNS>	Use this attribute to prefer external DNS response over internal DNS response when DNS response is received from both.	Per-App and Full Device Note: Use the PreferInternalDNS or PreferExternalDNS XML code in the Configuration XML. If both the XML codes are used in the Configuration XML, then the PreferInternalDNS XML code takes precedence.
<PreferInternalDNS>true/false</PreferInternalDNS>	Use this attribute to prefer internal DNS response over external DNS response when DNS response is received from both.	

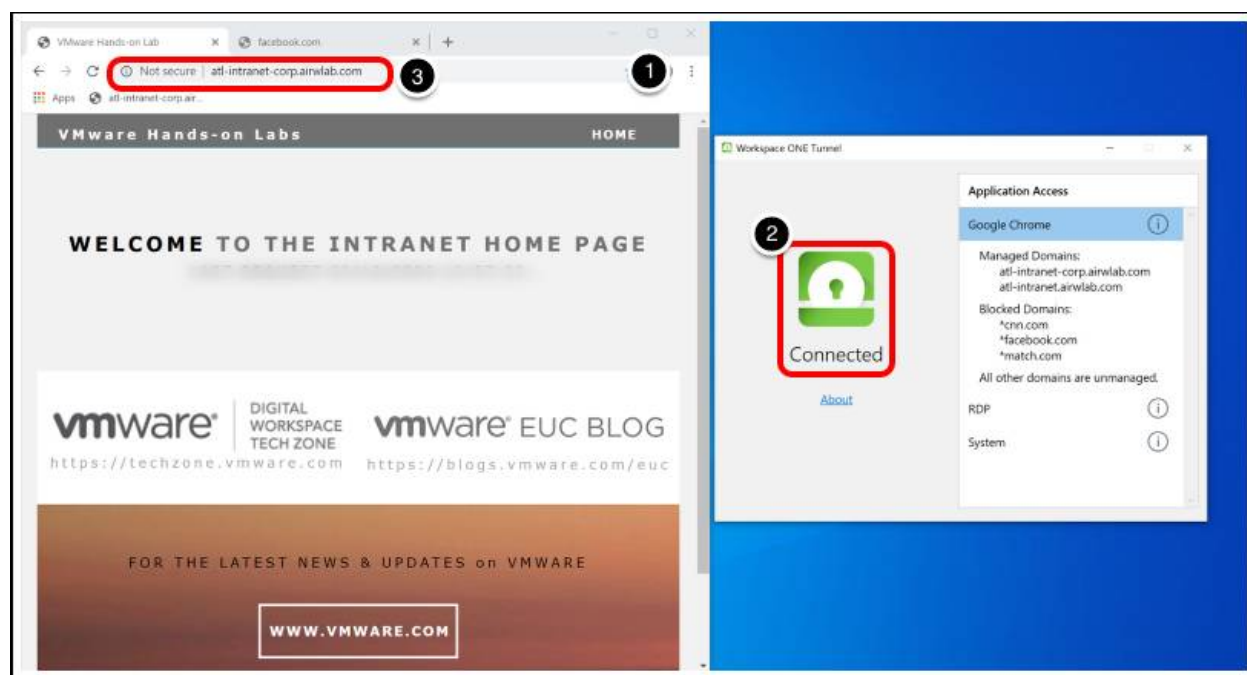
Testing Per-App Tunnel on Windows

Now that the enrolled device has received the settings configured in the Workspace ONE UEM Console, you are ready to begin testing the Per-App VPN functionality. The Workspace ONE Tunnel Desktop Application should be installed on your device.

In this exercise, you learn how to:

1. Launch an internal website with an authorized application.
2. Launch an internal website with an unauthorized application.
3. Launch a defined application and demonstrate blocked domains.
4. Launch an RDP session and connect to the machine on the internal network.
5. Connect to an SMB share to access file shares inside the corporate network.

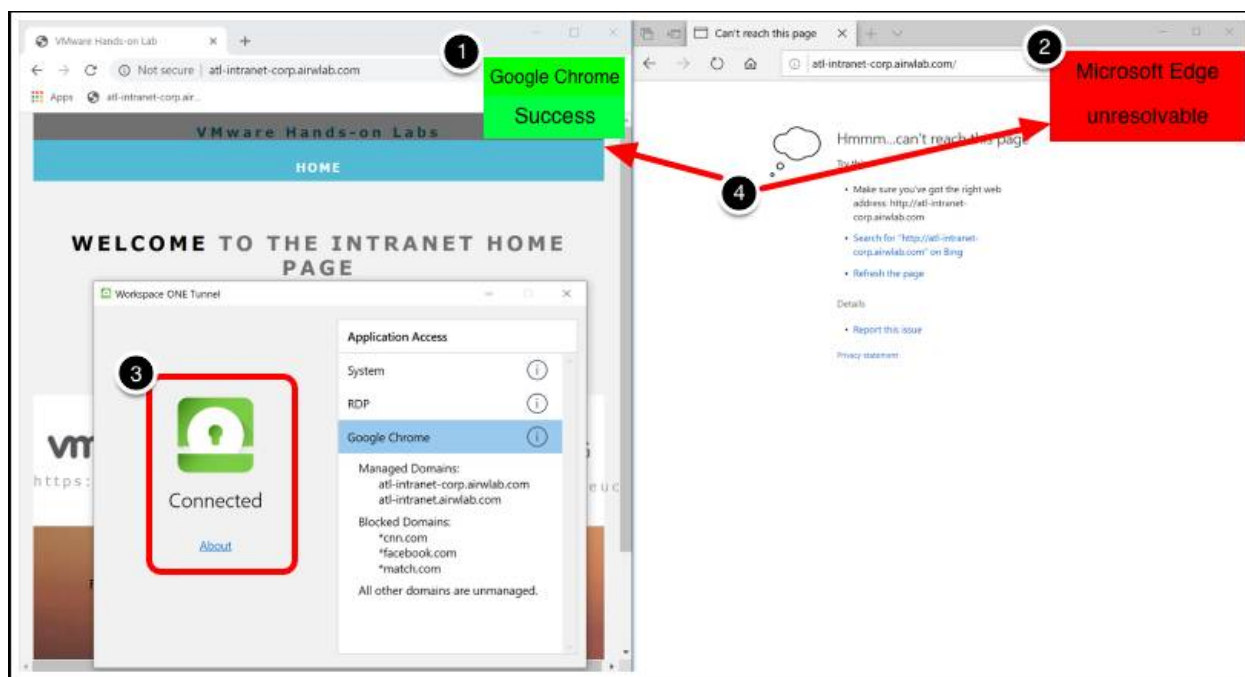
Launch Internal Website with an Authorized Application



1. Launch **Chrome** as a browser. Chrome was the application specified to Tunnel traffic.
2. The *Workspace ONE Tunnel Desktop Application* is connected and an internal web page is displayed.
3. The address used - atl-intranet-corp.airwlab.com - is specified in the Device Traffic Rules in the previous exercise. This web page is accessible only to applications (in this use case, Chrome) defined in the policy.

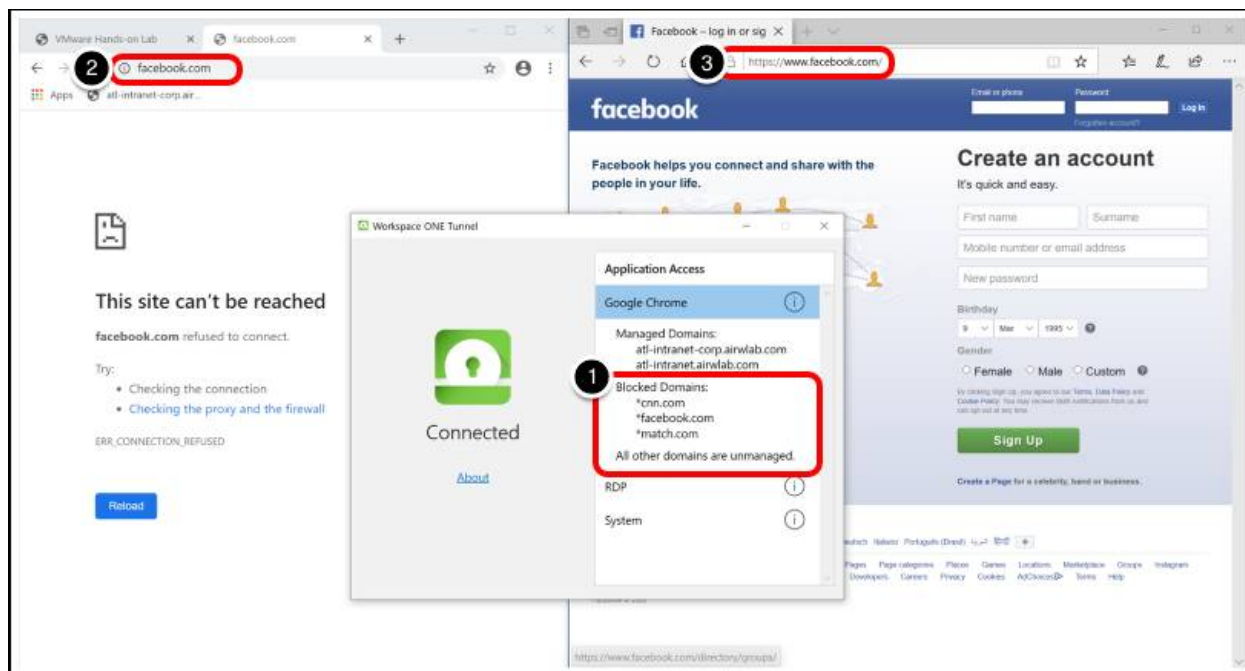
Launch Internal Website with an Unauthorized Application

Next, open another web browser, such as Microsoft Edge, and navigate to an internal web page. For example, atl-intranet-corp.airwlab.com.



1. Launch **Chrome** - this is the authorized application.
2. Launch another browser - for example, **Microsoft Edge**.
3. The **Workspace ONE Tunnel Desktop Application** is connected and an internal web page is displayed.
4. The address `atl-intranet-corp.airwlab.com` can be resolved in Chrome, but *not* in Microsoft Edge.

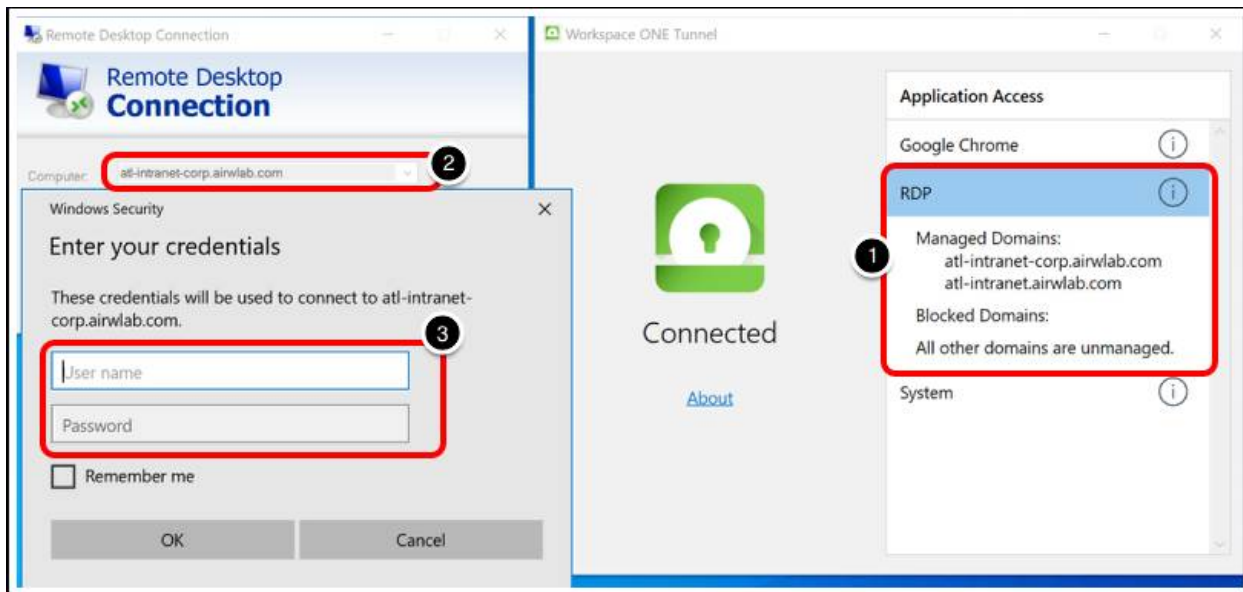
Launch a Defined Application to Demonstrate Blocked Domains



1. In the Application access rules, *certain websites are blocked*. These were listed in the Device Traffic Rules.
 - a. Websites blocked are `cnn.com`, `facebook.com`, and `match.com`.
2. Open **Chrome** and navigate to one of these websites. This example uses `facebook.com`.
 - a. When trying to resolve the DNS name, the browser displays an error as this website is blocked.
3. Launch **another browser**, in this case, Microsoft Edge. Facebook.com is accessible, as the policy is configured for Chrome only.

Test RDP Connections

Sometimes, you may need to RDP into desktop sessions that are located back in the office.

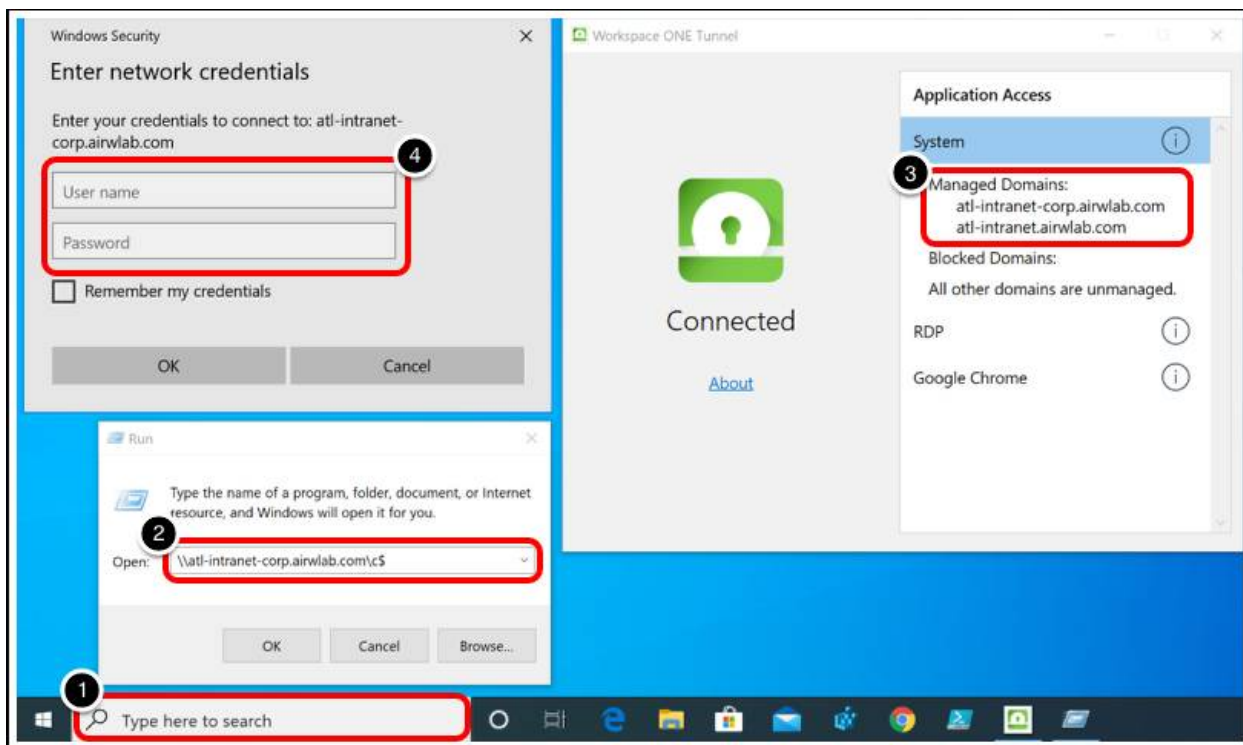


1. In the Application access rules, confirm the domain configuration for Remote Desktop Client access.
Note: The RDP application is not from the Windows Store.
2. Launch the RDP application and enter the machine name. In this example, you connect to the machine `atl-intranet-corp` on the domain `airwlab.com`.
3. Workspace ONE Tunnel Desktop Application resolves this address, and you should be prompted for authentication.

Test SMB Share Connections

Workspace ONE Tunnel Desktop Application allows remote Windows users to connect to file shares located behind the corporate firewall. This can be team shares, individual shares, or connecting to a specific machines' C drive, for example.

This example uses the host **atl-intranet-corp** and connects to its **C: drive**.



1. In the search bar, enter **Run** and press the return key.
2. Enter the address of the **file share** you would like to connect to. For example, `\\atl-intranet-corp.airwlab.com\\c$`.
3. In the Application access rules, confirm the domain configuration for System resource access.
4. Launch the SMB share. VMware Tunnel will resolve this address, and you should be prompted for authentication to the SMB share.

Troubleshooting Workspace ONE Tunnel on Windows

If a Per-App Tunnel problem occurs on Windows Desktop, you can check a number of places to troubleshoot. This section of the operational tutorial covers where to troubleshoot on Windows Desktop at a high level. Depending on the problem, there may be steps that should be performed on the Unified Access Gateway. However, troubleshooting the Unified Access Gateway is outside the scope of this tutorial. Workspace ONE UEM administrators should contact VMware Support for assistance when troubleshooting Per-App Tunnel, Workspace ONE Tunnel, or the Unified Access Gateway.

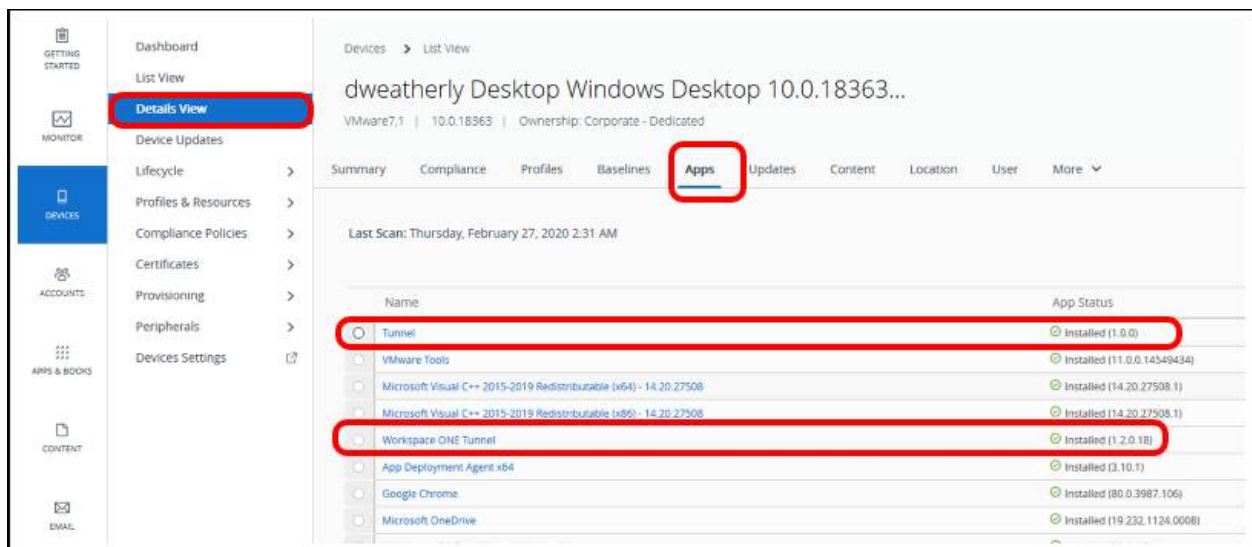
This section is divided into two and covers the following high-level set of initial troubleshooting steps.

1. Workspace ONE Tunnel Desktop Application Installation Troubleshooting.
 - a. Checking Workspace ONE UEM console for application install status.
 - b. Locating Workspace ONE Tunnel desktop application installer logs.
 - c. Checking device registry for Workspace ONE Tunnel desktop application install status.
 - d. Checking Workspace ONE UEM console for Policy install status.
 - e. Checking device registry for Per-App VPN Profile.
2. Workspace ONE Tunnel Desktop Application Connectivity Troubleshooting.
 - a. Confirming the Workspace ONE Tunnel status when Tunnel is connected.
 - b. Confirming the Workspace ONE Tunnel status when Profile is not installed.
 - c. Confirming Application Access and Tunnel Service.
 - d. Checking the Workspace ONE Tunnel certificate.
 - e. Enabling Workspace ONE Tunnel debug logging.
 - f. Locating Workspace ONE Tunnel logs.
 - g. Confirming Workspace ONE Tunnel DNS Resolution.

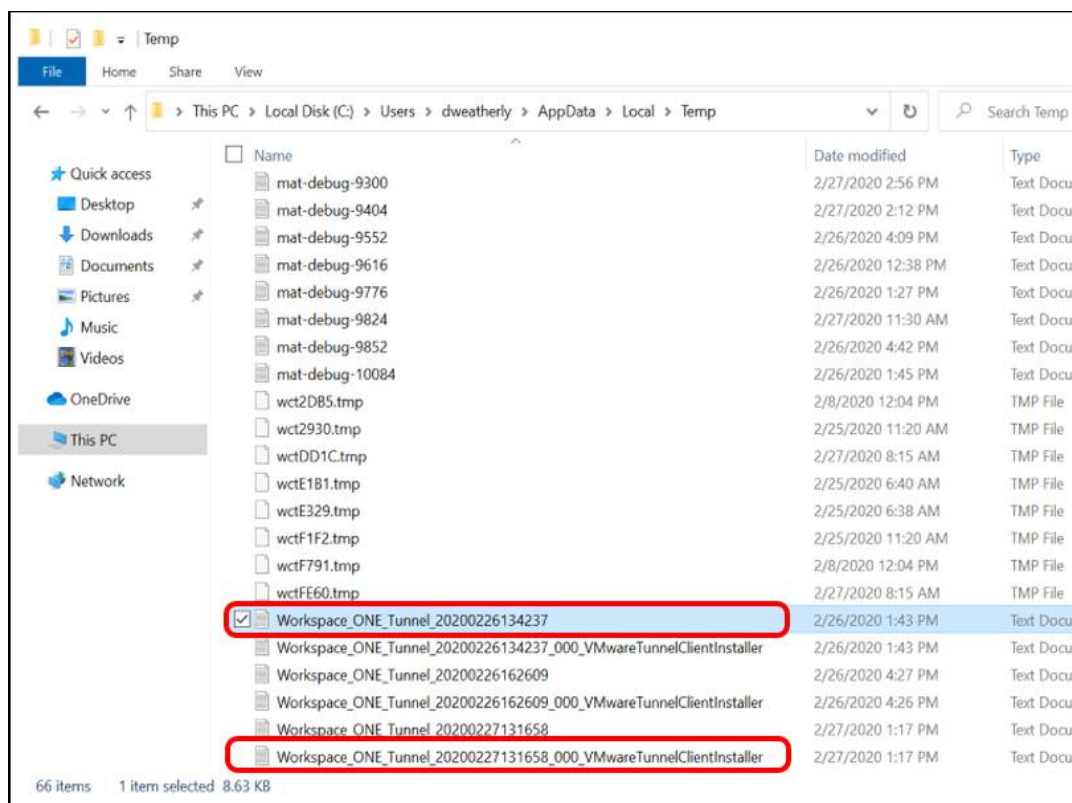
Troubleshoot Workspace ONE Tunnel Installation

In this section, check issues that may arise from the Workspace ONE Tunnel desktop client application installation.

1. Check Workspace ONE UEM console for application install status.



- a. Navigate to the Details view of the device.
 - b. Select the Apps tab.
 - c. Confirm that the App Status for the Tunnel Installer is Installed.
 - d. Confirm that the App Status for Workspace ONE Tunnel shows the correct version. In this example, Workspace ONE Tunnel 1.2.0.18 is installed.
2. Locate Workspace ONE Tunnel desktop application installer logs.



By default, the Workspace ONE Tunnel Desktop Application Installer logs are found in %TEMP%.

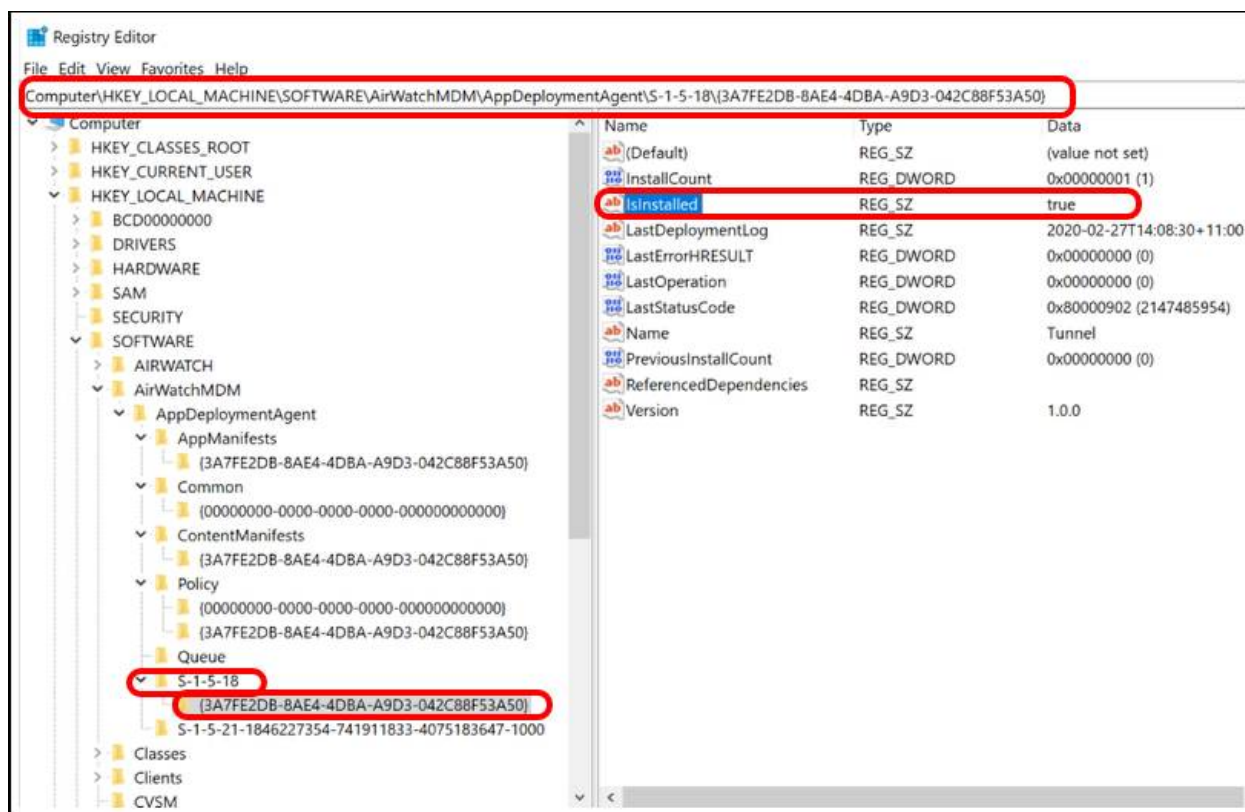
Two logs should exist:

- a. Workspace_ONE_Tunnel_<date>.log
 - i. This is the Bootstrapper log which usually does not yield very important errors unless any dependency programs fail on install, for example, .NET.
- b. Workspace_ONE_Tunnel_<date>_000_VMwareTunnelClientInstaller.log
 - i. This is the Tunnel Installer log which shows any failures during the Workspace ONE Tunnel desktop application installation.

3. Check device registry for Workspace ONE Tunnel install status.

Check the location of the registry installation settings for the Workspace ONE Tunnel desktop application. These values should match the values in the Workspace ONE UEM console.

On the computer that should have the Workspace ONE Tunnel desktop application installed, open the **Windows Registry** or run `regedit.msc`.



- Navigate to **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > AirWatchMDM > AppDeploymentAgent > S-1-5-18**.
- Click the GUID of the application. For example, {3A7FE2DB-8AE4-4DBA-A9D3-042C88F53A50}.
- Click the Registry key to show **IsInstalled**.

Tip: The Application GUID should match the value in the Workspace ONE UEM Console.

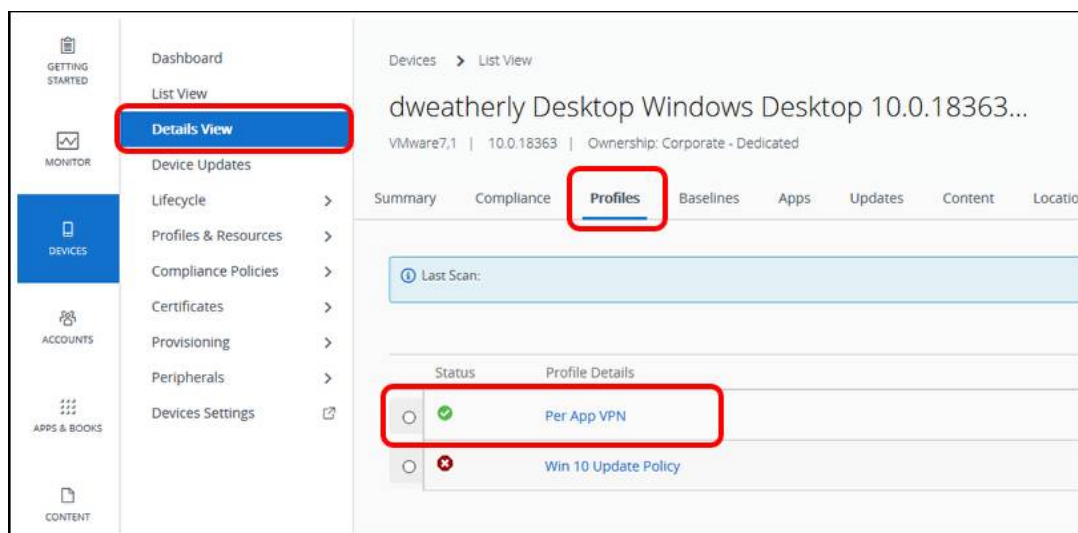
- Confirm application ID in the Workspace ONE UEM console.



- In the Workspace ONE UEM console, navigate to Resources > and select the Workspace ONE Tunnel Application from List View.
- In the App Details View, the Application ID (GUID) should match the registry value in the previous screenshot.

For more information on troubleshooting Windows Applications, see [Troubleshooting Windows Devices: Workspace ONE Operational Tutorial](#).

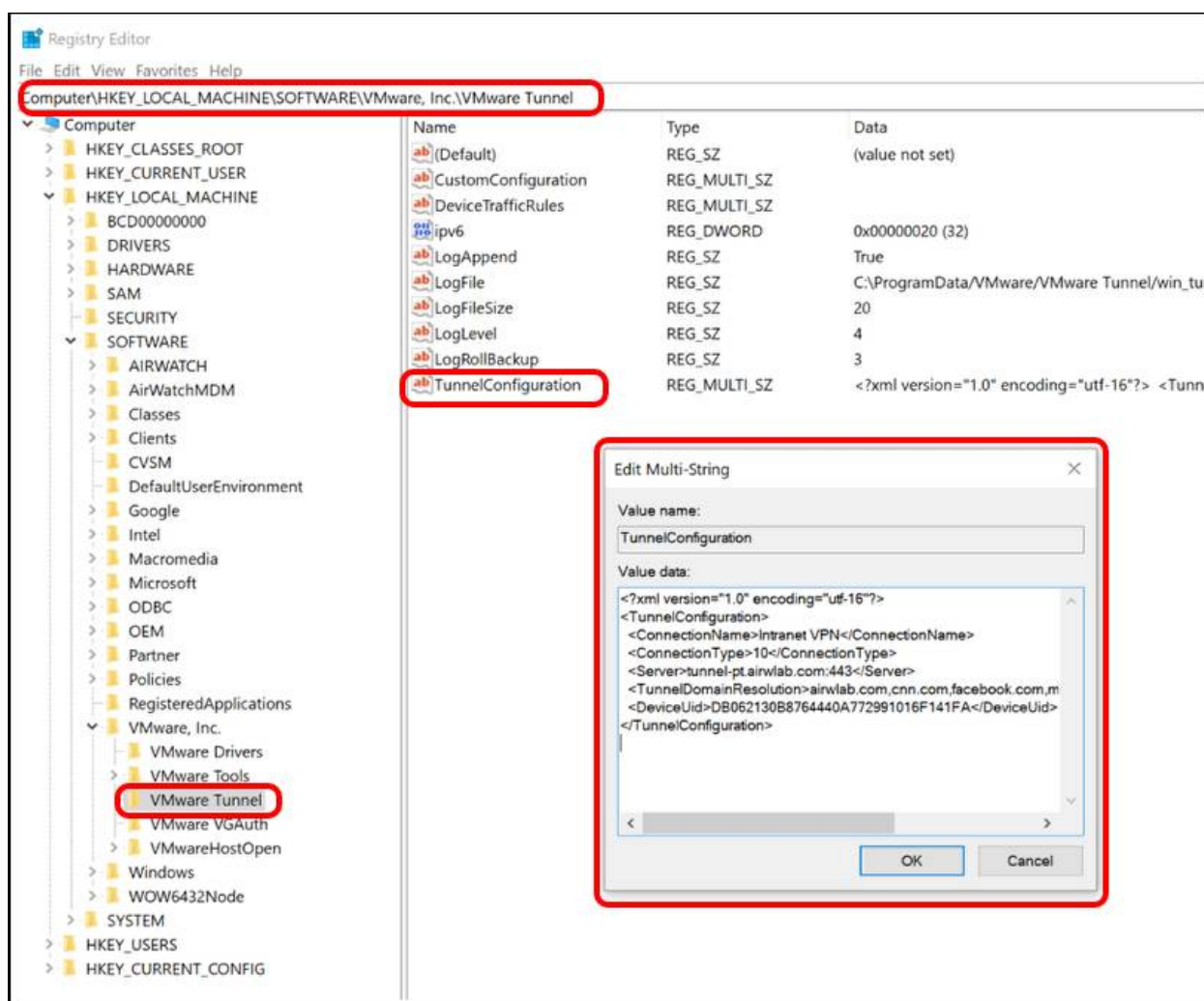
- Check Workspace ONE UEM console for policy install status.



After you have confirmed that the application is installed, make sure the policy is installed on the device.

- a. In the Workspace ONE UEM console, navigate to the Details View of that device.
 - b. Select the Profiles tab.
 - c. Confirm that the Status of the Per App VPN Profile is successful.
6. Check device registry for per-app VPN profile.

On the computer that should have the Tunnel policy installed, open the **Windows Registry** or run `regedit.msc`.



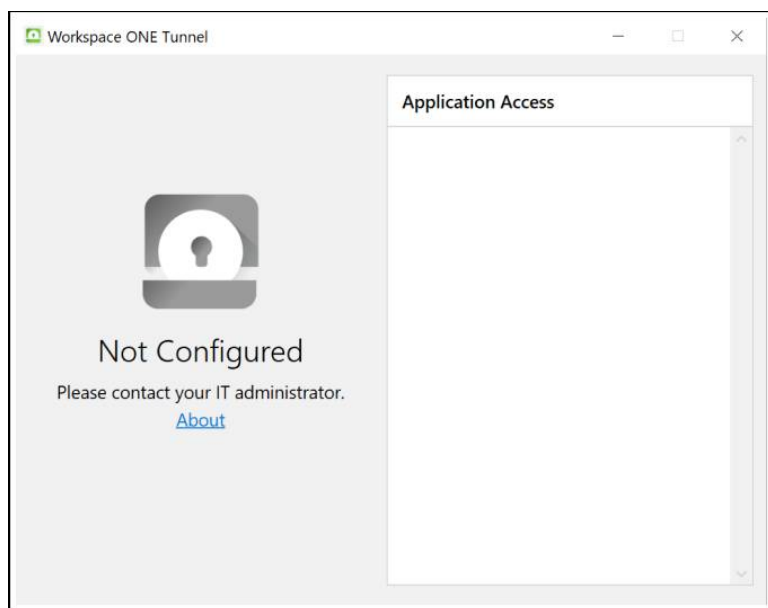
- a. Navigate to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Tunnel.
- b. Click **TunnelConfiguration**.
- c. This displays the Tunnel Policy applied to that machine.

Tip: If no policy is shown in the registry, re-push the policy from the Workspace ONE UEM console and perform a Device Query on that device from the Workspace ONE UEM console.

Troubleshoot Workspace ONE Tunnel Client Connectivity

After you have successfully installed the Workspace ONE Tunnel, the next step is to test the Per-App Tunnel connectivity by attempting to access one of the internal resources through the domains defined on the Device Traffic Rules.

1. Confirm the Workspace ONE Tunnel status when Tunnel is connected.
 - a. When the Tunnel Client has reached a successful connection, the Tunnel Client UI displays Connected.
2. Confirm Workspace ONE Tunnel status when profile is not installed.

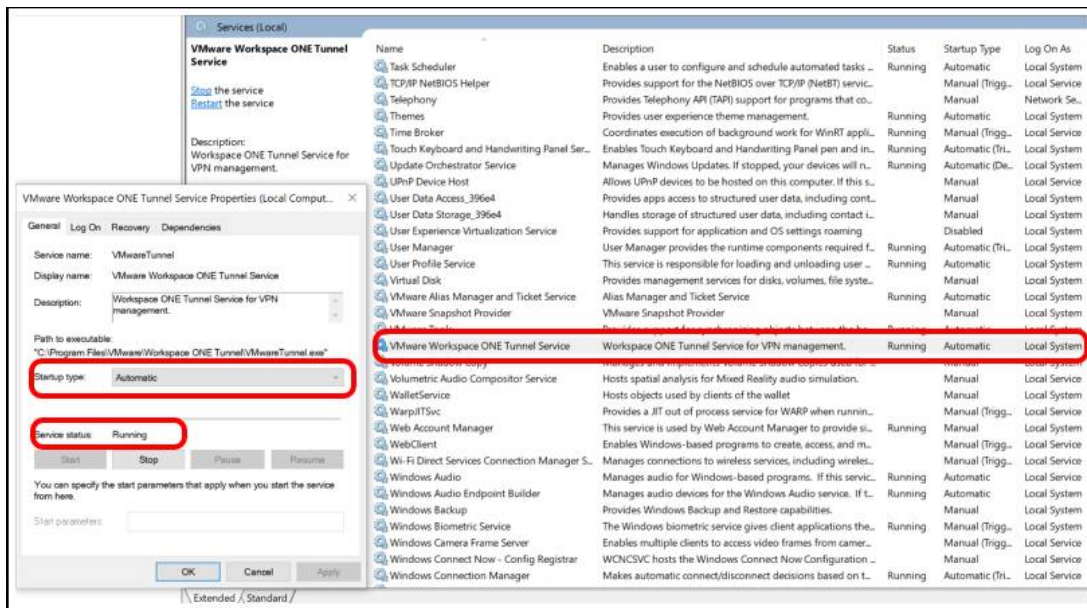


- a. If the Workspace ONE Tunnel Client has installed, but the configuration settings have not, the Tunnel client status is Not Configured.

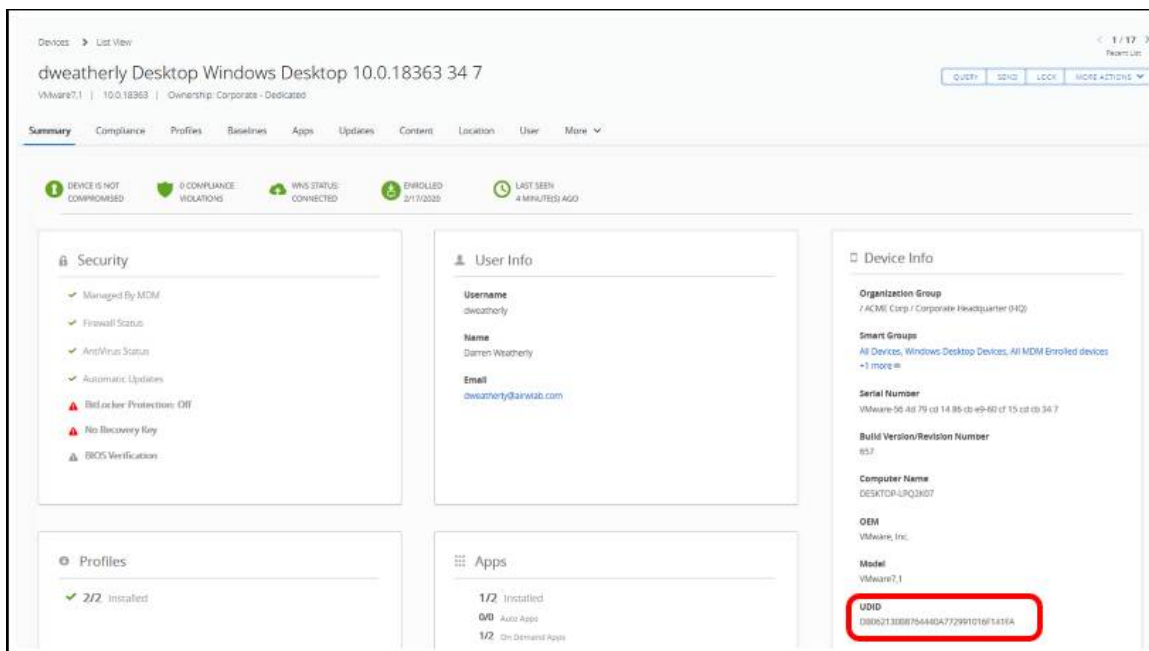
Tip: To resolve, ensure the Per-App VPN profile is assigned to the device, and ensure it is successfully installed.

3. Confirm application access and Tunnel service.
 - **Problem:** The Workspace ONE Tunnel Client status is Disconnected.
 - **Solution:** Confirm that the Application is defined in Application Access and that the application is running.
 - **Problem:** The Workspace ONE Tunnel Client status is Disconnected.
 - **Solution:** Confirm that the VMware Workspace ONE Tunnel Service is running in Windows Services. If the service is not started, start the service.

To check the Tunnel service:



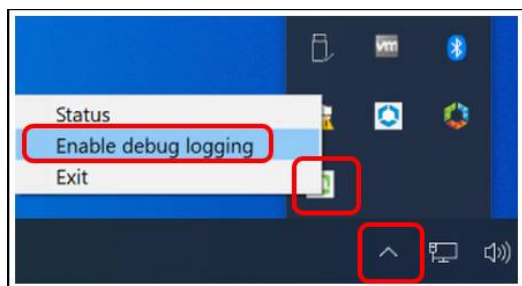
- a. On the Windows machine, open Services and locate the VMware Workspace ONE Tunnel Service.
 - b. Ensure that the Startup type is set to Automatic.
 - c. Ensure that the Service is running.
4. Check the Workspace ONE Tunnel desktop application certificate.
 - Authentication for the Tunnel Client can be configured to use Enterprise Certificates or internally-signed certificates. If no certificate is present, the Tunnel UI status displays Not Configured - Authentication Certificates are not present.
 - If there is no certificate present, you may want to re-push the policy again to the device. By re-pushing the policy, the Tunnel certificate should be installed.



To check the certificates:

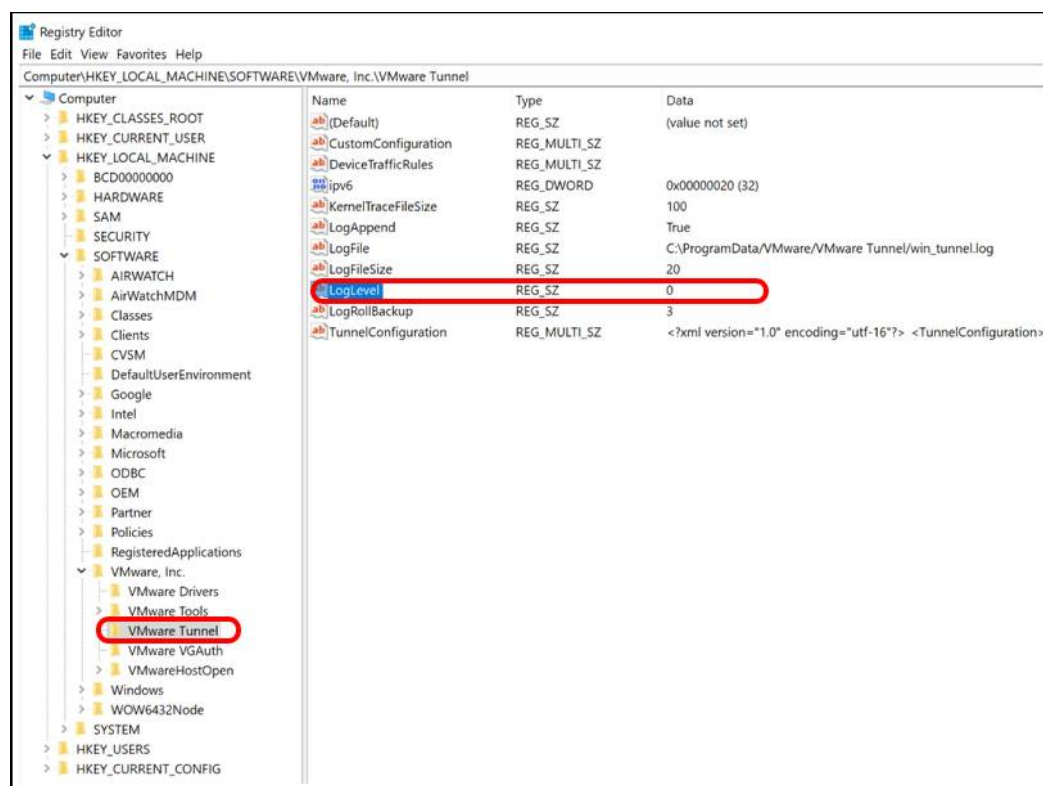
- On the Windows machine, search MMC, and open the Certificates snap in.
- Navigate to Local Computer > Personal > Certificates.
- Confirm that the certificate for certificate authentication to the Tunnel service is listed.
- Retrieve the device UDID from the Workspace ONE UEM console.
- Navigate to Devices > List View > Summary and confirm that the device UDID matches the Certificate request as shown in the previous screenshot.

5. Enable Workspace ONE Tunnel debug logging.



- On the Windows machine, navigate to the system tray. You should see the Tunnel icon.
- Right-click the Tunnel client.
- Select Enable debug logging.
- Debug logging levels are from 0-4 - Enabling debug logging will set the log level to 4.

You can also check the Workspace ONE Tunnel log level in the device registry.

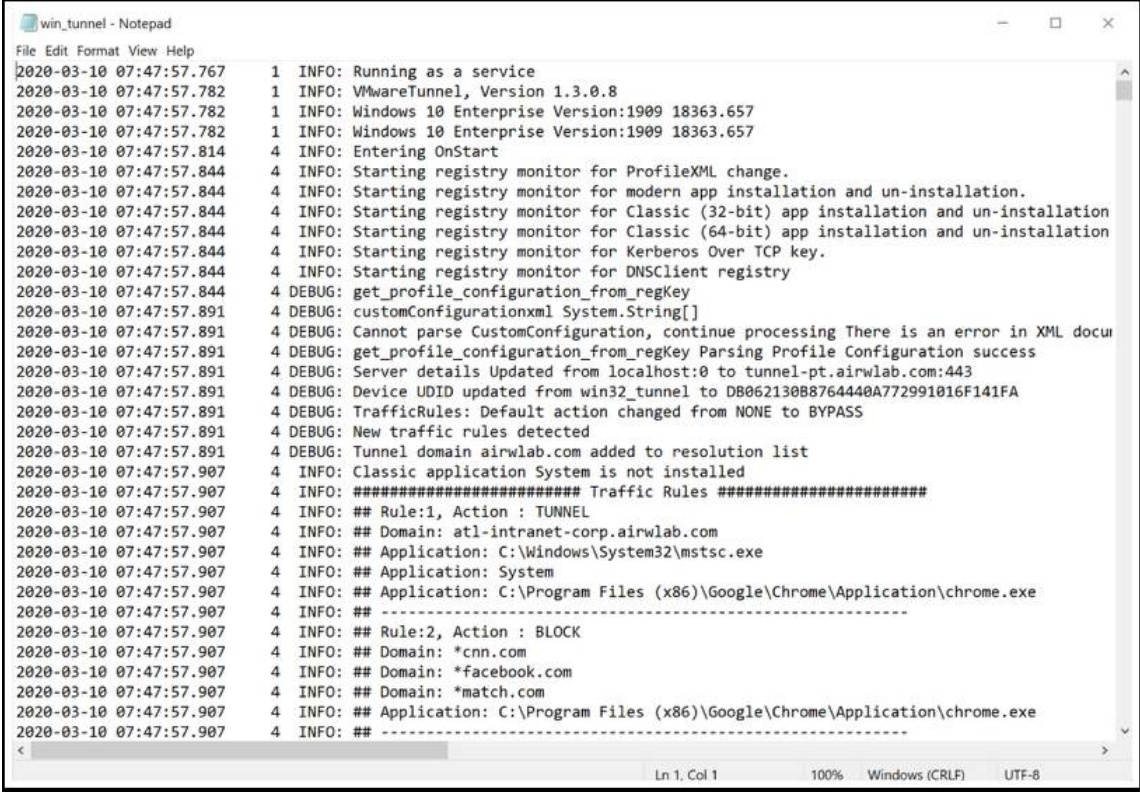


- On the computer that should have the Tunnel installed, open the **Windows Registry** or run `regedit.msc`.
- Navigate to **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Tunnel**.
- Under the **LogLevel** entry, you should see a value from 0-4. In this example, the value is 0.
- You cannot change the value in the registry. You must follow the steps to *Enable Workspace ONE Tunnel Debug Logging*.

6. Locate Workspace ONE Tunnel logs.

a. By default, the Workspace ONE Tunnel Client Installer logs are located in `C:\ProgramData\VMware\VMware Tunnel`. Two logs should exist:

- win_tunnel** – This log file shows connectivity issues with the Workspace ONE Tunnel desktop application.

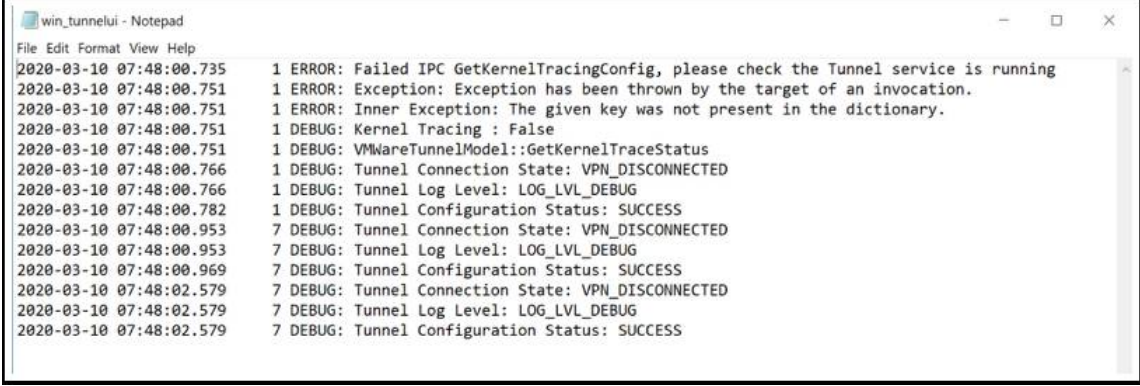


```

win_tunnel - Notepad
File Edit Format View Help
2020-03-10 07:47:57.767 1 INFO: Running as a service
2020-03-10 07:47:57.782 1 INFO: VMwareTunnel, Version 1.3.0.8
2020-03-10 07:47:57.782 1 INFO: Windows 10 Enterprise Version:1909 18363.657
2020-03-10 07:47:57.782 1 INFO: Windows 10 Enterprise Version:1909 18363.657
2020-03-10 07:47:57.814 4 INFO: Entering OnStart
2020-03-10 07:47:57.844 4 INFO: Starting registry monitor for ProfileXML change.
2020-03-10 07:47:57.844 4 INFO: Starting registry monitor for modern app installation and un-installation.
2020-03-10 07:47:57.844 4 INFO: Starting registry monitor for Classic (32-bit) app installation and un-installation
2020-03-10 07:47:57.844 4 INFO: Starting registry monitor for Classic (64-bit) app installation and un-installation
2020-03-10 07:47:57.844 4 INFO: Starting registry monitor for Kerberos Over TCP key.
2020-03-10 07:47:57.844 4 INFO: Starting registry monitor for DNSClient registry
2020-03-10 07:47:57.844 4 DEBUG: get_profile_configuration_from_regKey
2020-03-10 07:47:57.891 4 DEBUG: customConfigurationxml System.String[]
2020-03-10 07:47:57.891 4 DEBUG: Cannot parse CustomConfiguration, continue processing There is an error in XML docu
2020-03-10 07:47:57.891 4 DEBUG: get_profile_configuration_from_regKey Parsing Profile Configuration success
2020-03-10 07:47:57.891 4 DEBUG: Server details Updated from localhost:0 to tunnel-pt.airwlab.com:443
2020-03-10 07:47:57.891 4 DEBUG: Device UDID updated from win32_tunnel to DB062130B8764440A772991016F141FA
2020-03-10 07:47:57.891 4 DEBUG: TrafficRules: Default action changed from NONE to BYPASS
2020-03-10 07:47:57.891 4 DEBUG: New traffic rules detected
2020-03-10 07:47:57.891 4 DEBUG: Tunnel domain airwlab.com added to resolution list
2020-03-10 07:47:57.907 4 INFO: Classic application System is not installed
2020-03-10 07:47:57.907 4 INFO: ##### Traffic Rules #####
2020-03-10 07:47:57.907 4 INFO: ## Rule:1, Action : TUNNEL
2020-03-10 07:47:57.907 4 INFO: ## Domain: atl-intranet-corp.airwlab.com
2020-03-10 07:47:57.907 4 INFO: ## Application: C:\Windows\System32\mstsc.exe
2020-03-10 07:47:57.907 4 INFO: ## Application: System
2020-03-10 07:47:57.907 4 INFO: ## Application: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
2020-03-10 07:47:57.907 4 INFO: ## -----
2020-03-10 07:47:57.907 4 INFO: ## Rule:2, Action : BLOCK
2020-03-10 07:47:57.907 4 INFO: ## Domain: *cnn.com
2020-03-10 07:47:57.907 4 INFO: ## Domain: *facebook.com
2020-03-10 07:47:57.907 4 INFO: ## Domain: *match.com
2020-03-10 07:47:57.907 4 INFO: ## Application: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
2020-03-10 07:47:57.907 4 INFO: ## -----
Ln 1, Col 1 100% Windows (CRLF) UTF-8

```

- ii. **win_tunnelui** – This log file shows User Interface changes within the Workspace ONE Tunnel desktop application.



```

win_tunnelui - Notepad
File Edit Format View Help
2020-03-10 07:48:00.735 1 ERROR: Failed IPC GetKernelTracingConfig, please check the Tunnel service is running
2020-03-10 07:48:00.751 1 ERROR: Exception: Exception has been thrown by the target of an invocation.
2020-03-10 07:48:00.751 1 ERROR: Inner Exception: The given key was not present in the dictionary.
2020-03-10 07:48:00.751 1 DEBUG: Kernel Tracing : False
2020-03-10 07:48:00.751 1 DEBUG: VMwareTunnelModel::GetKernelTraceStatus
2020-03-10 07:48:00.766 1 DEBUG: Tunnel Connection State: VPN_DISCONNECTED
2020-03-10 07:48:00.766 1 DEBUG: Tunnel Log Level: LOG_LVL_DEBUG
2020-03-10 07:48:00.782 1 DEBUG: Tunnel Configuration Status: SUCCESS
2020-03-10 07:48:00.953 7 DEBUG: Tunnel Connection State: VPN_DISCONNECTED
2020-03-10 07:48:00.953 7 DEBUG: Tunnel Log Level: LOG_LVL_DEBUG
2020-03-10 07:48:00.969 7 DEBUG: Tunnel Configuration Status: SUCCESS
2020-03-10 07:48:02.579 7 DEBUG: Tunnel Connection State: VPN_DISCONNECTED
2020-03-10 07:48:02.579 7 DEBUG: Tunnel Log Level: LOG_LVL_DEBUG
2020-03-10 07:48:02.579 7 DEBUG: Tunnel Configuration Status: SUCCESS
Ln 1, Col 1 100% Windows (CRLF) UTF-8

```

7. Confirm Workspace ONE Tunnel desktop application DNS resolution.

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\dweatherly> Get-DnsClientNrptRule

Name                           : {73B72B82-4377-4025-B75B-51613CAE7E9C}
Version                         : 1
Namespace                       : {cnn.com}
IPsecCARestriction              :
DirectAccessDnsServers          :
DirectAccessEnabled             : False
DirectAccessProxyType           :
DirectAccessProxyName           :
DirectAccessQueryIPsecEncryption :
DirectAccessQueryIPsecRequired  :
NameServers                     : 127.0.0.1
DnsSecEnabled                   : True
DnsSecQueryIPsecEncryption      :
DnsSecQueryIPsecRequired        : False
DnsSecValidationRequired        : False
NameEncoding                    : Disable
DisplayName                     : VMware Tunnel NRPT
Comment                         : NRPT by VMware Tunnel

Name                           : {79CE20A4-F746-4E7A-9257-DD2D903ECD50}
Version                         : 1
Namespace                       : {tunnel-pt.airwlab.com}
IPsecCARestriction              :
DirectAccessDnsServers          :
DirectAccessEnabled             : False
DirectAccessProxyType           :
DirectAccessProxyName           :
DirectAccessQueryIPsecEncryption :
DirectAccessQueryIPsecRequired  :
NameServers                     : 192.168.174.2
DnsSecEnabled                   : True
DnsSecQueryIPsecEncryption      :
DnsSecQueryIPsecRequired        : False
DnsSecValidationRequired        : False
NameEncoding                    : Disable
DisplayName                     : VMware Tunnel NRPT
Comment                         : NRPT by VMware Tunnel

Name                           : {7B07211A-CBE6-4608-BB8E-F19128B42992}
Version                         : 1
Namespace                       : {.facebook.com}
IPsecCARestriction              :

```

After you have confirmed Tunnel connectivity, check the DNS resolution.

Sometimes, the Workspace ONE Tunnel Client may be in good working order. For example, the profile is installed, the application is installed, the service is running, and the status is Connected. But the DNS resolution is still failing. In this case, general networking troubleshooting can assist greatly.

You can check the Name Resolution Policy Table (NRPT).

On the Windows machine, open PowerShell and enter `Get-DnsClientNrptRule`. This command retrieves the Name Resolution Policy Table (NRPT) for the device. For more information, see [Microsoft PowerShell Docs - Get-DnsClientNrptRule](#).

Deploying Workspace ONE Tunnel for Android

Per-App Tunneling helps users to access critical information using applications on their devices from their devices. Mobile flows help users perform business-critical tasks from a single app — streamlining the user experience.

Leveraging Per-App Tunnel allows you to control which applications are on a device and what internal resources the applications have access to by automatically activating or deactivating Per-App VPN access, based on which applications are active. By enabling remote access, you no longer need to provide a device-wide VPN on your devices, which can allow unintended or unauthorized apps or processes to access your VPN. In this tutorial, you configure and deploy VMware Workspace ONE Tunnel to enable the Per-App Tunnel component on managed devices.

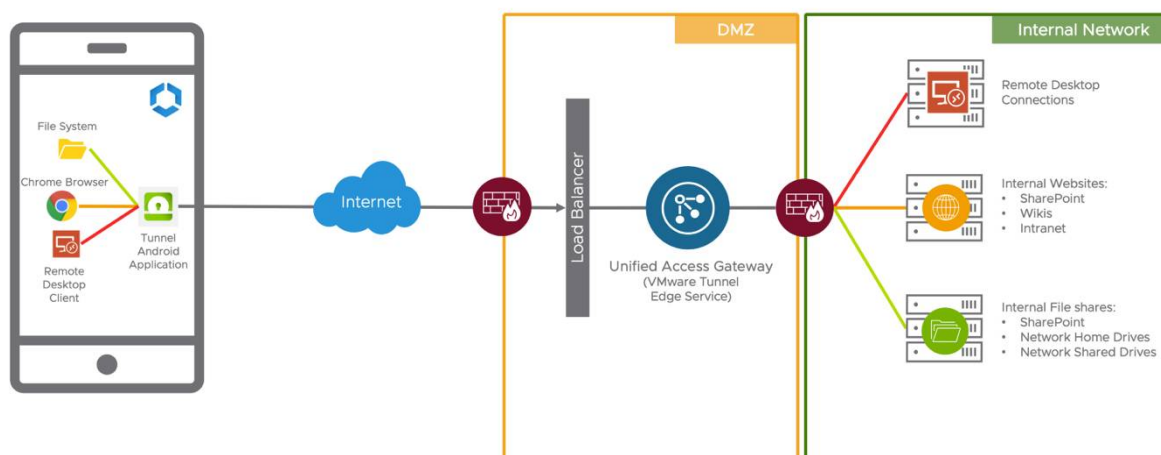
These exercises involve the following components:

- **Workspace ONE Tunnel** – The app used on the device to securely connect to the Unified Access Gateway to provide Per-App Tunnel functionality, also referred to as Tunnel Client.
- **Unified Access Gateway** – The virtual appliance where the VMware Tunnel edge service is installed, and to which the tunnel client connects.
- **Per-App Tunnel** – Component of VMware Tunnel edge service for connecting to a secure tunnel channel on a per-application basis, which is controlled and configured by the VPN profile payload and Device Traffic Rules.
- **Per-App VPN Profile and Device Traffic Rules** – The Workspace ONE UEM configuration is pushed to the device that contains the Per-App Tunnel configurations. Every time a specified application is opened, the Workspace ONE Tunnel client evaluates the Device Traffic Rules assigned to it before making any routing decisions and establishes a Per-App tunnel connection with the Unified Access Gateway based on the Per-App VPN Profile configuration.

High-Level Architecture

Workspace ONE Tunnel Android Application

Example of Per-App VPN Remote Access



The device contains the applications required by the end-user to perform their daily job. Some applications require access to internal resources to function. Those applications, based on Per-App VPN configuration, use Workspace ONE Tunnel which communicates with the Tunnel Service on Unified Access Gateway hosted on the DMZ, to validate if the device requesting access is in compliance or not before authorizing access through the internal resource.

Prerequisites

Before you can perform the steps in this exercise, you must have the following components installed and configured:

- Workspace ONE UEM version 2203 and later
- Android 10.0+ enrolled in Workspace ONE UEM
- The latest version of Workspace ONE Tunnel app from Google Play Store
 - Deploy Workspace ONE Tunnel using Android Enterprise

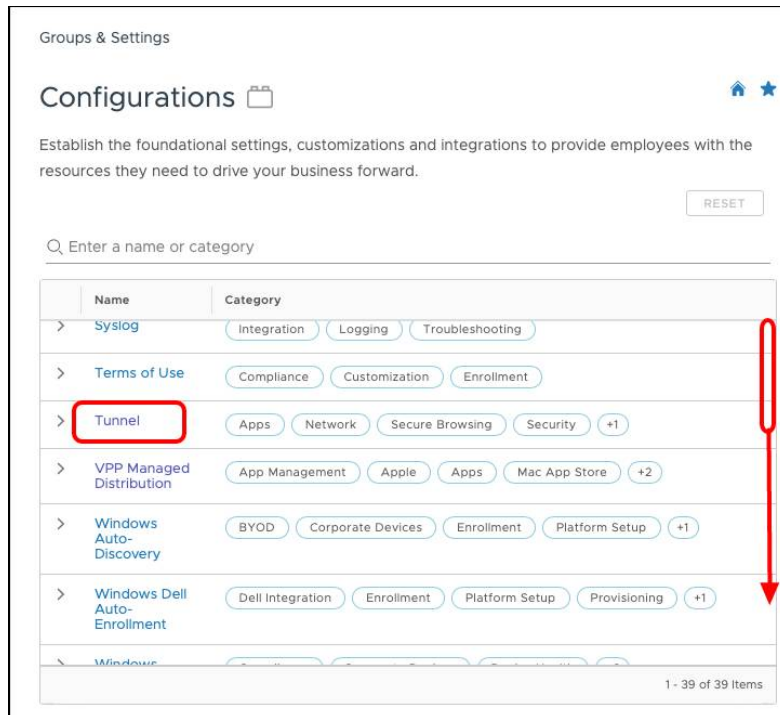
Configuring Device Traffic Rules for Android

In this exercise, you configure device traffic rules for Android.

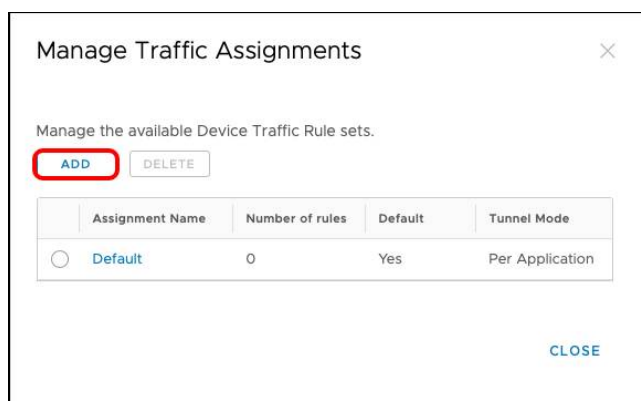
Note: Domain values used in this section are examples only. Your values will differ.

In the Workspace ONE UEM console:

1. Navigate to **Groups & Settings > Configurations**.
2. Select **Tunnel**.



3. From the Device Traffic Rules tile, click **Edit**.
4. Click **Add** or the **Default** assignment to manage the device traffic rules.



Administrators can create multiple Device Traffic Rules that will be assigned to the Per-APP VPN profile and will deploy to the devices based on the smart group assigned to the Profile. The first device traffic rule assignment created will be set as default.

5. Observe the default device traffic rule.

Device Traffic Rules

Assignment Name
Default

Tunnel Mode
Per Application

Add rules to Tunnel, Block or Bypass the network traffic using VMware Tunnel

ADD RULE **MANAGE APPLICATIONS**

Rank	Application	Action	Destination
1	All Other Apps	BYPASS	*

CANCEL **SAVE** **SAVE AND PUBLISH**

1. Update the Assignment Name with the name of your choice.
2. Observe (or modify) the default action which applies to all Android applications selected to use Per-App VPN:
 - i. **Tunnel** - All apps, on the device configured for Per-App Tunnel send network traffic through the tunnel. For example, set the Default Action to Tunnel to ensure all configured apps without a defined traffic rule use the Workspace ONE Tunnel for internal communications.
 - ii. **Block** - Blocks all apps, on the device configured for Per-App Tunnel from sending network traffic. For example, set the Default Action to Block to ensure that all configured apps without a defined traffic rule cannot send any network traffic regardless of destination.
 - iii. **Bypass** - All apps, except Safari, on the device configured for Per-App Tunnel bypass the tunnel and connect to the Internet directly. For example, set the Default Action to Bypass to ensure all configured apps without a defined traffic rule bypass the Workspace ONE Tunnel to access their destination directly.
3. Click **ADD RULE**.
6. Build the device traffic rule.

Add rules to Tunnel, Block or Bypass the network traffic using VMware Tunnel

ADD RULE **MANAGE APPLICATIONS**

Rank	Application	Action	Destination
1	<input type="checkbox"/> Safari - iOS <input type="checkbox"/> Safari - macOS <input type="checkbox"/> AirWatch Container - iOS <input type="checkbox"/> AirWatch Learn - iOS <input type="checkbox"/> Web - Workspace ONE - iOS <input type="checkbox"/> Android workspace - Android <input type="checkbox"/> AirWatch Secure Browser - And... <input type="checkbox"/> AirWatch Email Client - Android <input checked="" type="checkbox"/> All Applications	BLOCK	*.facebook.com *.tinder.com *.utorrent.com
2	All Other Apps	BYPASS	*

CANCEL **SAVE** **SAVE AND PUBLISH**

1. Click **ADD RULE**.
2. Click the down arrow to display the Application list.
3. Select one or more triggering applications to control with this rule. Alternatively, on the drop-down select **All Applications** to apply the rule to all Android applications listed in the drop-down, which are the ones that you assigned the Per-App VPN profile.
4. Enter one or more comma-separated fully qualified domain names as destinations to which Workspace ONE Tunnel should apply the Device Traffic Rule. A single asterisk (*) can be used as a wildcard for subdomains.
5. Select the Appropriate Action for Workspace ONE Tunnel to perform on traffic from the selected apps:
 - i. **Tunnel** - Sends app network traffic for specified domains through the tunnel to your internal network.
 - ii. **Block** - Blocks all traffic sent to specified domains.
 - iii. **Bypass** - Bypasses the Workspace ONE Tunnel so the application accesses specified domains directly.
 - iv. **Proxy** - Redirect traffic to the specified HTTPS proxy for the listed domains. The proxy must be HTTPS and must follow the correct format: <https://example.com:port>.
6. If necessary, adjust the Device Traffic Rules rank in the list. Lower-numbered rank is the highest priority.
7. Click **Save**.

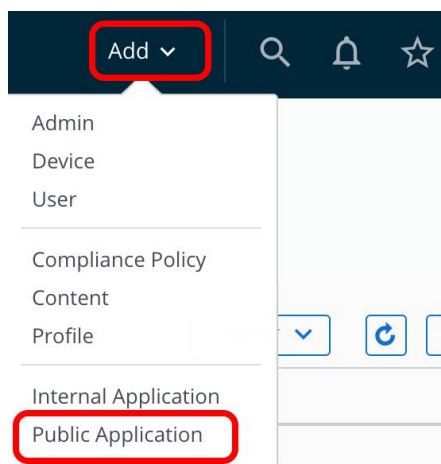
The example shown blocks access to Facebook, Tinder, and Utorrent domains for all applications available on the Android device.

For more information on the formats (wildcards, IP, ports) allowed into the Destination field, see the *Device Traffic Rules Destination formats supported* chapter.

Distributing Workspace ONE Tunnel for Android

In this exercise, you deploy an application configured to use the Per-App VPN tunnel on Android.

1. Click **Add** and click **Public Application**.



2. Search for Workspace ONE Tunnel.

Add Application



Managed By

Platform* Android ▼

Source SEARCH APP STORE ENTER URL IMPORT FROM PLAY

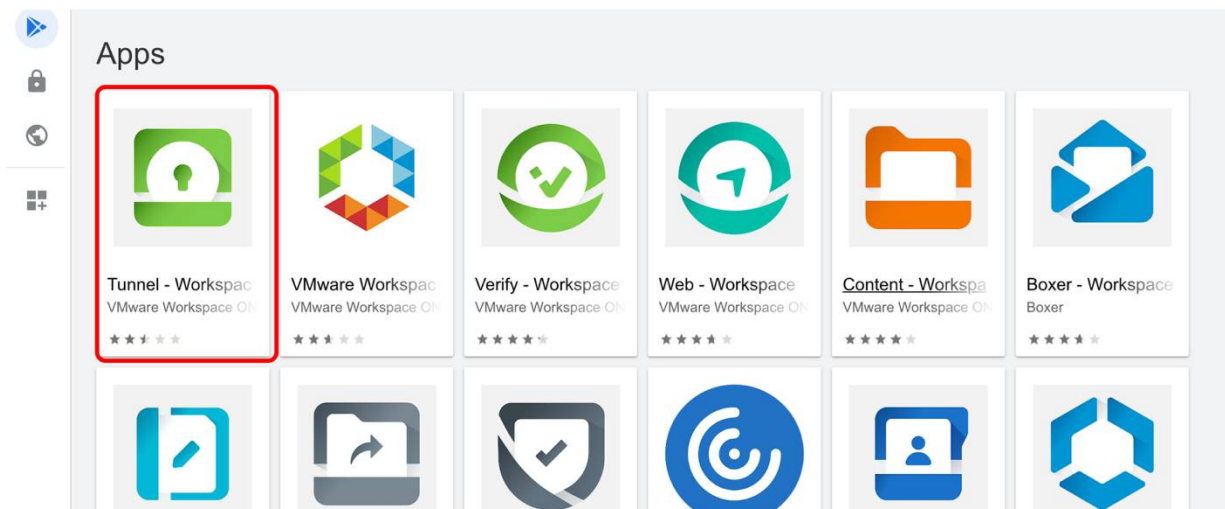
Name* Workspace ONE Tunnel

NEXT[CANCEL](#)

- a. Select **Android** for the **Platform**.
- b. Enter an application **Name**. For example, Workspace ONE Tunnel.
- c. Click **Next**.

3. Select **Tunnel - Workspace ONE Tunnel**.

Add Application



4. Click **Approve** for the Workspace ONE Tunnel app and for any following requests.
5. Click **Save and Assign**.
6. Click **Add Assignment**.
7. Configure Assignment settings.

Tunnel - Workspace ONE - Add Assignment

Assignment Groups *

App Delivery Method * ☒ Auto ☐ On Demand

- a. Click the **Selected Assignment Groups** field to display the list of created Assignment Groups. Enter All Devices, and select the **All Devices (your@email.shown.here)** group.
 - b. Select **Auto** for the **App Delivery Method**.
8. Configure Policies.

Adaptive Management Level : Managed Access

Apply policies that give users access to apps based on administrative management of devices.

Data Loss Prevention [Configure](#)

DLP policies provide controlled exchange of data between managed and unmanaged applications on the device. To prevent data loss on this application, make it "Managed Access" and create "Restriction" profile policies for desired device types.

Managed Access ☒

Pre-release Version *

Application Configuration [CONFIGURE](#)

[CANCEL](#) [ADD](#)

- a. Scroll down to find the Policies section.
 - b. Select Enabled for Managed Access.
 - c. Click Add.
9. Confirm that your assignment is displayed and click **Save and Publish**.

Tunnel - Workspace ONE - Update Assignment ×Assignments Exclusions

Devices will receive application based on the below configuration.

In the case where devices belong to multiple groups, they will receive policies from the grouping with highest priority (0 being highest priority).

ADD ASSIGNMENT
EDIT
DELETE
MOVE UP
MOVE DOWN
↺

	Name	Priority	App Delivery Method	Managed Access	VPN Access	Send Configuration	Pre-release Version
<input type="radio"/> ▼	All Devices	0	Auto	✓ Enabled	⊘ Disabled	⊘ Disabled	⊘ Disabled

CANCEL

SAVE AND PUBLISH

10. Preview your assigned devices and click **Publish**.

Android Considerations

Note the following for Workspace ONE Tunnel on Android:

- After installing VMware Workspace ONE Tunnel for Android, end users must run the application at least once and accept the connection request.
- The key icon in the notification center displays on the device because there is an application installed that uses the Per-App Tunnel functionality. This icon does not indicate an active connection or session with the VMware Tunnel Service. The key icon displays even if you are not actively browsing.
- Certain Android devices allow end users to disable the VPN on an OS level. This prevents the VMware Tunnel from working on the device.


Creating Per-App VPN Profile for Android

Per-App VPN profile allows you to force selected applications to connect through your corporate VPN. Your VPN provider must support this feature, and you must publish the applications as managed applications.

In this exercise, you create the Android profile which configures the Workspace ONE Tunnel client on the device to allow only designated applications to access content on internal servers.

Log in to the Workspace ONE UEM console to perform the next steps.

1. Click **Add** and click **Profile**.
2. Select **Android**.
3. Configure the General settings.

 Per App VPN Android

Find Payload

General

Passcode

Chrome Browser Settings

Restrictions

Exchange ActiveSync

Public App Auto Update

Credentials

Custom Messages

Application Control

Proxy Settings

System Updates

Wi-Fi

VPN

Permissions

Single App Mode

Launcher

Enterprise Factory Reset Protection

Custom Settings

General

Name *

Version

Description

OEM Settings

Profile Scope

Assignment Type

Allow Removal

Managed By

Smart Groups

Exclusions

- a. Select the **General** tab.
 - b. Enter a Name, for example, Per App VPN.
 - c. Select the name of your device's assignment group, and select that group. For example, select All MDM Enrolled Devices (ACME Corp) as the Assigned Smart Group.
4. Add and configure VPN payload.

Add a New Android Profile

Find Payload

General

Passcode

Restrictions

Wi-Fi

VPN

Email Settings

Exchange ActiveSync

Application Control

Bookmarks

Credentials

Workspace ONE Launcher

Global Proxy

Date/Time

VPN

All VPN Options Below Are Supported By:

Connection Info

Connection Type * **Workspace ONE Tunnel**

Connection Name * VPN Configuration

Server * TCP://tunnel.airwatch.com:443

Per-App VPN Rules ☒

Device Traffic Rule Sets **Default - Default**

Authentication

Identity Certificate Certificate

SAVE AND PUBLISH

- Select **VPN** from the payload menu and click **Configure**.
- Select Workspace ONE Tunnel from the Connection Type drop-down menu.
- Select the Default traffic rule previously created for Device Traffic Rule Sets.
- Click Save & Publish.

5. Click **Publish** to publish the VPN profile.

Configuring Workspace ONE Web for Per-App Tunnel

Workspace ONE Web is part of the secure productivity app suite from VMware. Administrators can deploy Workspace ONE Web when data loss and copy/paste restrictions are critical to the business use case.

In this exercise, you distribute and configure Workspace ONE Web for Per-App Tunnel on Android.

- Add application.

Workspace ONE UEM ACME Corp

GETTING STARTED

Apps

Native

Web Links

Settings

Profiles & Baselines

Device Updates

Sensors

Scripts

Time Windows

Books

Orders

Resources

Resources > Apps

List View

Internal **Public** Purchased

Filters >> **ADD APPLICATION**

Icon	Name
	Boeing Toolbox Mobile L Airwatch Internal ★★★★★
	Calculator & Math Solver Airwatch Internal ★★★★★

- In the Workspace ONE UEM console, click **Resources**.
- Select **Native** under Apps.
- Select **Public** and click **Add Application**.

2. Search for Workspace ONE Web on Google Play Store.

Add Application



Managed By

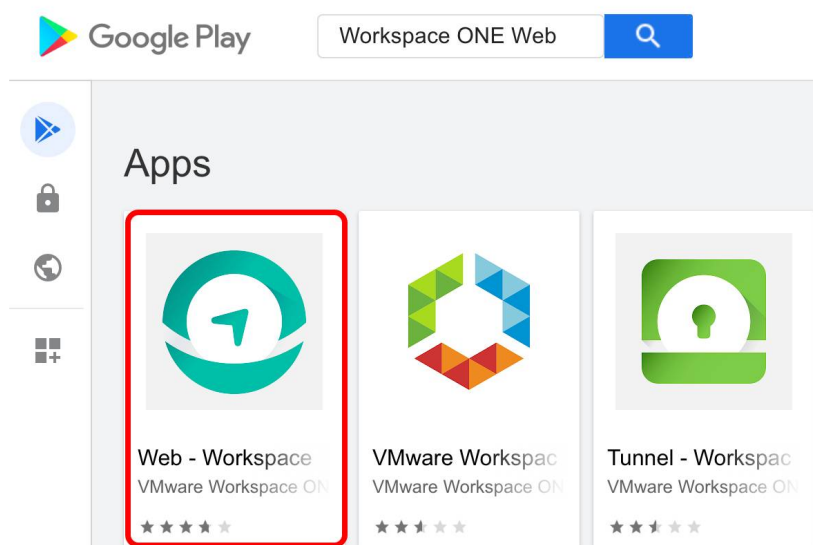
Platform*

Source

Name*

- a. Select **Android** for the **Platform**.
 - b. Enter an application **Name**. For example, Workspace ONE Web.
 - c. Click **Next**.
3. Select **Workspace ONE Web** app and approve.

Add Application



4. Click **Save and Assign**.
5. Click **Add Assignment**.
6. Assign Per-App VPN profile to Workspace ONE Web.

Web - Workspace ONE - Add Assignment



Assignment Groups *

All Devices

Start typing to add a group

App Delivery Method *

☒ Auto ☐ On Demand

Adaptive Management Level : Managed Access

Apply policies that give users access to apps based on administrative management of devices.

Data Loss Prevention

DLP policies provide controlled exchange of data between managed and unmanaged applications on the device. To prevent data loss on this application, make it "Managed Access" and create "Restriction" profile policies for desired device types.

[Configure](#)

Managed Access



App Tunneling



Android Legacy *

None

Android *

Per App VPN Android @ ACME Corp

Pre-release Version *

None

CANCEL

ADD

- Select **All Devices** on Assignment Groups.
- Select **Auto** for App Delivery Method.
- Enable **Managed Access**.
- Enable **App Tunneling**.
- On Android, select the Per-App VPN Profile that you previous created.
- Click **Add**.

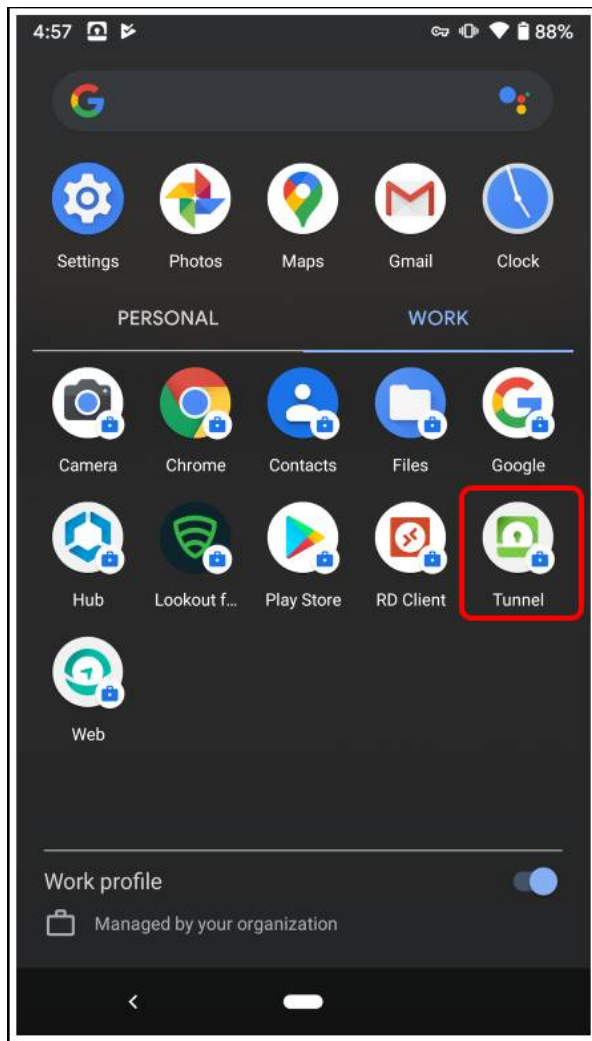
7. Click **Save and Publish**.

Testing Per-App Tunnel on Android

Now that the enrolled device has received the settings configured in the Workspace ONE UEM Console, you are ready to begin testing the Per-App Tunnel functionality. The applications assigned in the previous exercises should push down during enrollment. The VMware Tunnel and Workspace ONE Web applications should be installed on your device.

In this exercise, launch Workspace ONE Web and access the internal website. Then verify that, although the VPN connection is active, other applications on the device are not able to access the tunnel or internal resources.

- Open Workspace ONE Tunnel.



Press the Home button on your device to return to the Launchpad. Swipe right to see the downloaded applications, if needed.

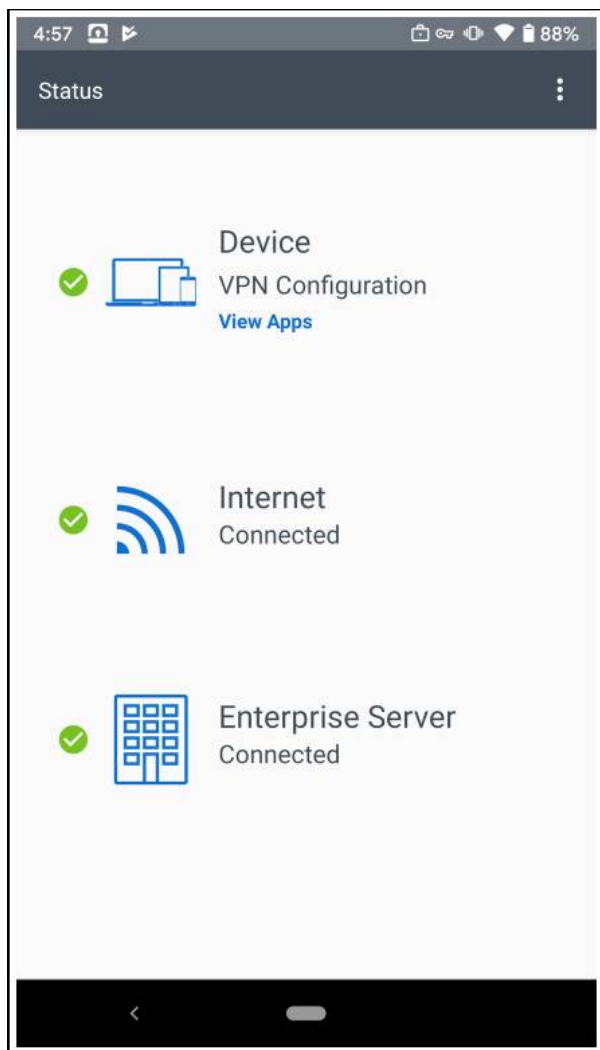
Tap the Workspace ONE Tunnel icon to launch the application. If prompted, select OK to allow Workspace ONE Web to send your device push notifications.

After the application has been opened, accept the privacy prompts and tap **Continue**.

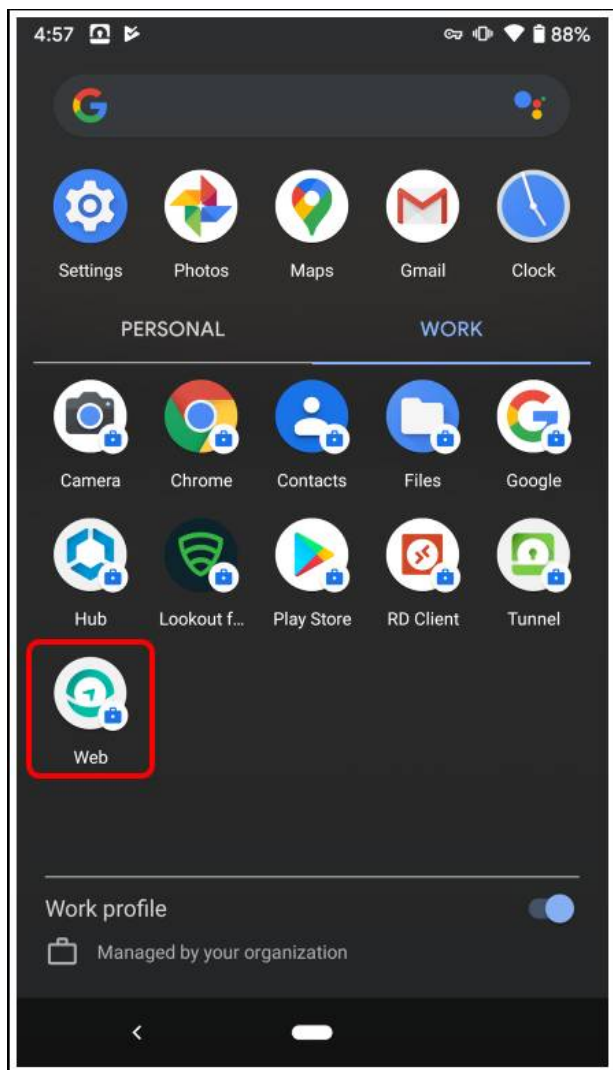
Note: On Android, the Workspace ONE Tunnel Client must be launched once to silently route traffic for future occurrences.

2. Tap **I Understand** to accept the Privacy Prompt.
3. Tap **I agree** to accept the Data Sharing Prompt.
4. Confirm Tunnel connectivity.

After the Tunnel Client has been opened, you can see three areas.



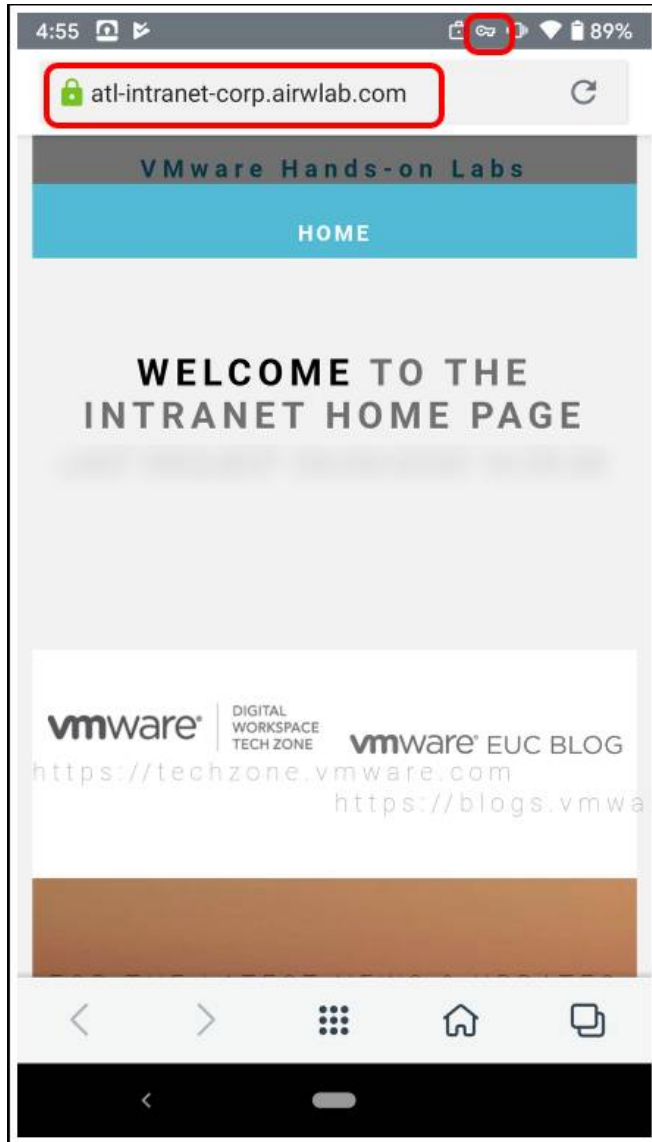
- a. Device VPN Configuration
 - i. The Profile or Policy that is delivered from Workspace ONE UEM. It shows a list of apps that will use the VPN Tunnel.
 - b. Internet
 - i. Displays whether the device has internet connectivity or not.
 - c. Enterprise Server
 - i. Displays whether the device has connectivity to the VMware Tunnel edge service.
5. Launch Workspace ONE Web.



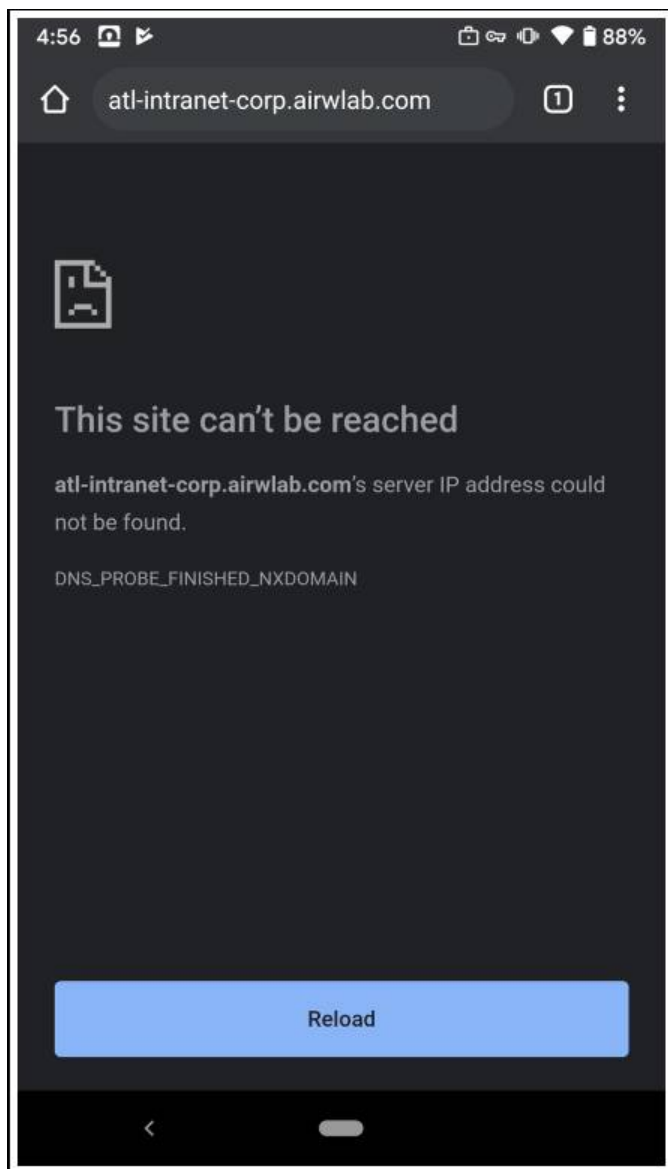
Press the Home button on your device to return to the Launchpad. Swipe right to see the downloaded applications, if needed.

Tap the Workspace ONE Web icon to launch the application. If prompted, tap OK to allow the Web to send your device push notifications.

6. Access the internal website with Workspace ONE Web.



- a. After the application launches, enter the URL for your intranet website, such as <https://atl-intranet-corp.airwlab.com>.
 - b. Confirm that the VPN icon appears, indicating the connection is active. The application now connects to Workspace ONE UEM and retrieves the settings for your Organization Group.
 - c. The website should load. In this example, it displays a Welcome message.
 - d. Select and copy the internal URL. In the next step, you test entering this URL into another browser.
7. Paste the URL into another browser.



- a. Open another browser, such as Chrome.
- b. Copy and paste the URL from the previous step.
- c. Confirm that only the defined applications can access internal resources.

Note: This example used a Work Managed Device. Work Managed devices provide separation from personal and corporate data. With Per-App Tunnel, you can isolate traffic to only those applications that need it rather than all corporate resources. This example shows Chrome inside the Work Profile attempting to access internal resources.

Troubleshooting Workspace ONE Tunnel on Android

If a Per-App Tunnel problem occurs on Android, you can check a number of places to troubleshoot. This section of the operational tutorial covers where to troubleshoot the Workspace ONE Tunnel client for Android at a high level.

Depending on the problem, there may be steps that should be performed on the Unified Access Gateway. However, troubleshooting the Unified Access Gateway is outside the scope of this tutorial.

Workspace ONE UEM administrators should contact VMware Support for assistance when troubleshooting Per-App VPN, Workspace ONE Tunnel, or the Unified Access Gateway.

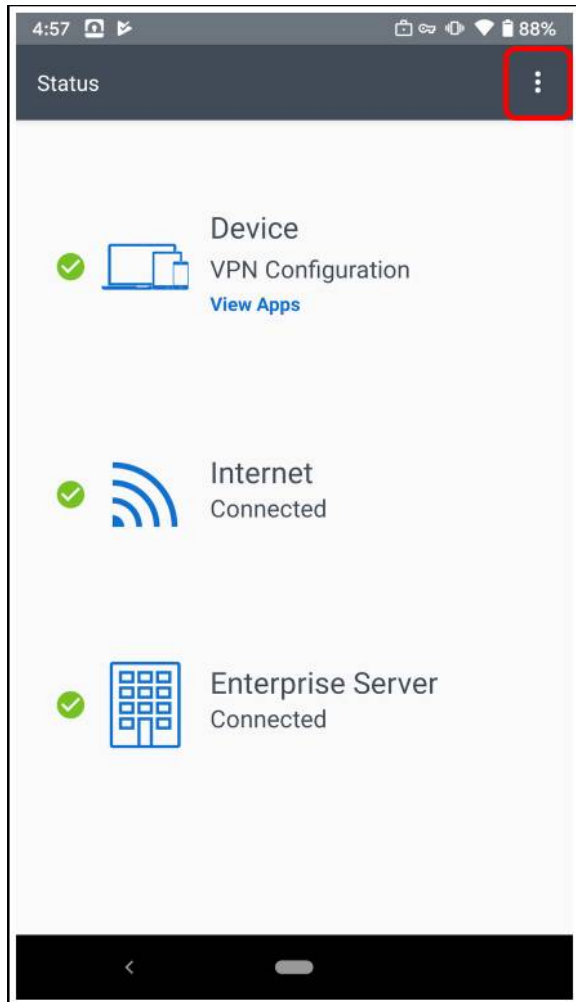
This section is divided into three parts and guides you through high-level steps to troubleshoot the Workspace ONE Tunnel installation and connectivity.

1. Troubleshooting Device Connectivity
 - a. This section displays where to search for Tunnel Client connectivity issues.
2. Collecting logs automatically

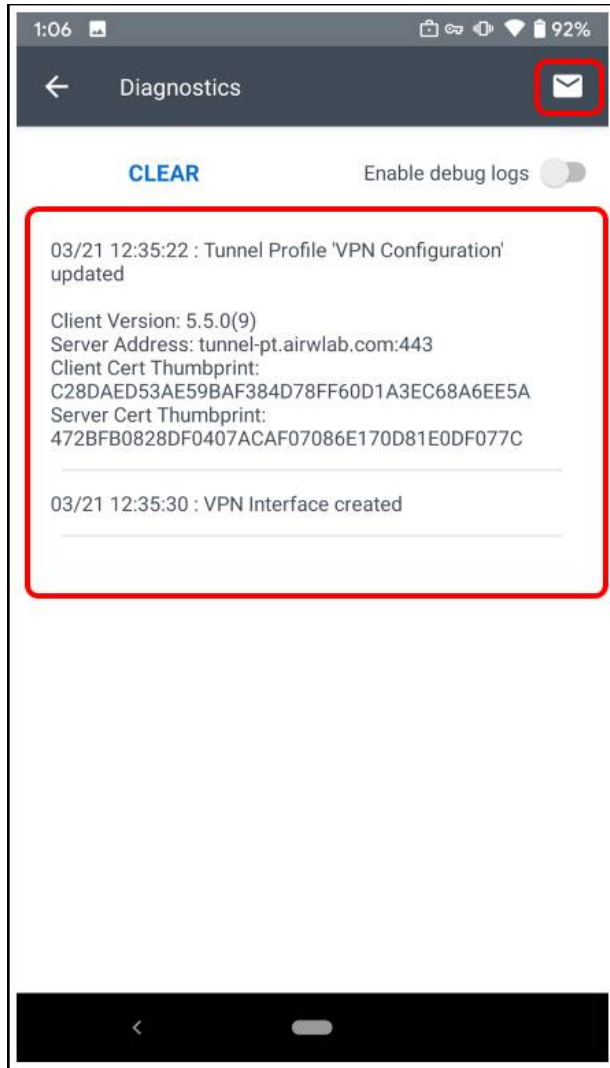
- a. This step is useful for recreating issues and retrieving the Workspace ONE Tunnel Client log file.
3. Advanced: Collecting logs manually on an Android Device
 - a. This step is for advanced cases where you may need to see how the devices VPN stack is behaving. This step should be used only for test devices; it is not recommended to leave Developer Options turned on.

Troubleshoot Device Connectivity

1. Open the Tunnel Application and tap the Diagnostics menu option.



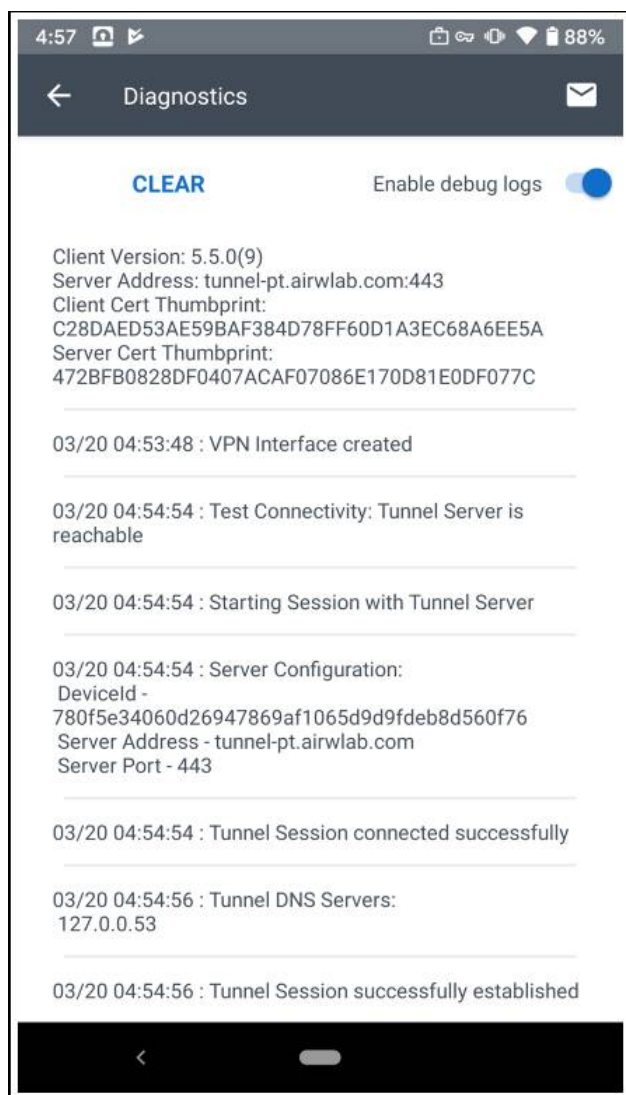
2. Any issues related to connectivity issues with the Tunnel server or a Proxy server are shown on the UI.



3. Tap the email option in the upper-right corner to send these logs to your administrator.

Collect Logs Automatically

1. Open the Tunnel Application and tap the Diagnostics menu option.
2. Activate the Enable debug logs toggle.



3. After the issue is reproduced, go to your internal storage and open the AirWatchLogs folder.
4. This folder contains a set of log files that, if required, can be shared with the Workspace ONE support teams.

Advanced: Collect Logs Manually on Android

1. To collect logs manually, you must **enable developer options** on the mobile device.
 - a. Navigate to **Settings > About** page on the device and tap the build number more than 7 times to enable developer options.
2. **Enable USB debugging** in the **Settings > Developer Options**.
3. Connect the device via USB cable to a laptop and install the device drivers.
 - a. Check whether the device is getting detected in the laptop by running `adb devices` in the command prompt. The device should be listed with a Unique id.
 - b. `adb` is a tool part of the android-sdk which you must download from <http://developer.android.com>.
4. After the device is detected (keep the device connected) run `adb logcat -v threadtime > TunnelLogs.log`. Logs will continuously dump to the file.
5. After the issue is reproduced, logging can be stopped either by disconnecting the device or using **Ctrl + c** command.
6. If required, share the `TunnelLogs.log` with the Workspace ONE support teams.

Summary and Additional Resources

This operational tutorial provided steps to leverage native Per-App Tunnel capabilities across mobile platforms, Android and iOS, and desktop platforms, macOS and Windows.

By publishing Per-App VPN profiles to your devices, you can ensure that only authorized apps are accessing authorized applications through the Tunnel. This eliminates the user requirement to manually start and end a network connection like traditional VPN solutions based on the apps they are accessing.

It also provides an extra layer of security to your corporate resources by ensuring that non-authorized apps are unable to connect to your VPN, creating the beginnings of a Zero Trust model for application access.

Additional Resources

For more information about Workspace ONE, explore the [VMware Workspace ONE Activity Path](#). The activity path provides step-by-step guidance to help you level-up in your Workspace ONE knowledge. You will find everything from beginner to advanced curated assets in the form of articles, videos, and labs.

Additionally, you can check out the [VMware Workspace ONE and VMware Horizon Reference Architecture](#) which provides a framework and guidance for architecting an integrated digital workspace using VMware Workspace ONE and VMware Horizon.

Changelog

The following updates were made to this guide:

Date	Description of Changes
2023-09-07	<ul style="list-style-type: none"> Updated requirements for Workspace ONE UEM Referenced new documentation links
2023-3-28	<ul style="list-style-type: none"> Updated supported platform matrix for Workspace ONE Tunnel Updated list of Custom XML Configuration for Windows Desktop Updated requirements for Windows deployment Added Windows 11 support
2022-12-05	<ul style="list-style-type: none"> Updated the Trust Network Detection chapter: added DNS resolution details when Trust Network Detection is enabled. Updated platform support and features availability matrix. Added details on the new Device Traffic Rules sync process for Android.
2021-07-09	<ul style="list-style-type: none"> Updated the Device Traffic Rules chapter adding a detailed explanation of default action rule per platform. Added supported custom configuration parameters for Windows 10. Added details for Trusted Network Detection based on probe URL.
2021-06-30	<ul style="list-style-type: none"> Updated Device Traffic Rules with an explanation about the new Full Device Tunnel Mode. Added Device Traffic Rules Guidelines for use of the asterisk, IP, and port range. Added steps to deploy Workspace ONE Tunnel for iOS as Public App (App Store) using Workspace ONE UEM.
2020-11-13	<ul style="list-style-type: none"> Added Trusted Network Detection chapter. Updated Device Traffic Rules topic, adding support to manage traffic assignments based on multiple Device Traffic Rules sets. Update Profile configuration for all platforms to support device traffic rule configuration via profile.
2020-3-26	<ul style="list-style-type: none"> Added Windows, Android, and macOS Platforms. Edited iOS Platform.

About the Author and Contributors

This tutorial was written by:

- [Andreano Lanusse](#), End-User-Computing Staff Architect, Technical Marketing, VMware.
- [Darren Weatherly](#), End-User-Computing Senior Architect, Technical Marketing, VMware.
- [Robert Terakedis](#), VMware alumni.

Feedback

Your feedback is valuable.

To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.



Copyright © 2023 VMware, Inc. All rights reserved. VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001

VMware and the VMware logo are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. Item No: vmw-wp-tech-temp-uslet-word-2021 8/21