

VMware Tunnel Guide

Deploying the VMware Tunnel for your Workspace ONE UEM environment

Workspace ONE UEM v1810

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

Chapter 1: VMware Tunnel	4
Supported Platforms for VMware Tunnel	5
Chapter 2: Key Concepts	8
App Tunnel and Secure Browsing	8
Per-App Tunnel Component	8
Proxy Component	9
VMware Tunnel and Unified Access Gateway	9
Load Balancing	9
App Certificate Authentication and Encryption	9
Chapter 3: VMware Tunnel Architecture and Deployment Model	10
Per-App Tunnel Architecture	10
Proxy (SDK/Browser) Architecture	10
Managing VMware Tunnel Certificates	11
VMware Tunnel Deployment Model	12
Chapter 4: VMware Tunnel Core Configuration	16
Configure AWCM Server and Enable API Access	16
Configure VMware Tunnel	17
Chapter 5: VMware Tunnel Advanced Configuration	21
Configure Advanced Settings for VMware Tunnel	21
Configure Network Traffic Rules for the Per-App Tunnel Component	21
Configure Outbound Proxy for the Proxy and Per-App Tunnel Component	21
SSL Offloading the Proxy Component	22
Configure Advanced Settings for the Per-App Tunnel Component	22
Configure Outbound Proxy for the Per-App Tunnel Component	23
Configure Network Traffic Rules for the Per-App Tunnel Component	25
Configure Advanced Settings for the Proxy Component	29
Configure Outbound Proxy for the Proxy Component	31
SSL Offloading the Proxy Component	33

Chapter 6: VMware Tunnel Deployment with Unified Access Gateway	37
System Requirements for Deploying VMware Tunnel with Unified Access Gateway	37
Installing VMware Tunnel with Unified Access Gateway	42
Configure VMware Tunnel Settings in the Unified Access Gateway UI	53
Upgrade VMware Tunnel deployed with Unified Access Gateway	55
Chapter 7: VMware Tunnel Deployment on a Linux Server	56
System Requirements for Deploying VMware Tunnel on a Linux Sever	56
Single-Tier VMware Tunnel Installation	61
Multi-Tier VMware Tunnel Installation	63
Upgrade VMware Tunnel Deployed on a Linux Server	69
Uninstalling VMware Tunnel	70
Chapter 8: VMware Tunnel Management	71
Deploying Per-App Tunnel to devices	71
VMware Tunnel SSL Certificate Life Cycle Management	76
Integrating VMware Proxy Tunnel with RSA	77
Using VMware Browser for VMware Tunnel	79
Chapter 9: Health and Monitoring	81
Access Logs and Syslog Integration	81
Monitor and Analyze VPN Report	81
Chapter 10: VMware Tunnel Troubleshooting and Support	84
Troubleshooting using the Tunnel_snap Utility	84
Upgrade Java Without Reinstalling Tunnel Proxy	85
Troubleshooting Per-App Component	85
Troubleshooting Proxy Component	86

Chapter 1:

VMware Tunnel

VMware Tunnel provides a secure and effective method for individual applications to access corporate resources. VMware Tunnel authenticates and encrypts traffic from individual applications on compliant devices to the back-end system they are trying to reach. VMware Tunnel serves as a relay between your mobile devices and enterprise systems by authenticating and encrypting traffic from individual applications to back-end systems.

Supported Platforms for Tunnel App

VMware Tunnel app is supported by iOS, macOS, Android and Windows 10. To know the supported platforms, requirements and considerations, see [Supported Platforms for VMware Tunnel on page 5](#).

Key Concepts

When configuring and deploying the VMware Tunnel, you must learn the VMware Tunnel terminology. Understanding the functionality that these components reference will aid your comprehension of this product. For more information, see [Key Concepts on page 8](#).

Architecture and Deployment Model

The VMware Tunnel is a product you can install on physical or virtual servers that reside in either the DMZ or a secured internal network zone. VMware Tunnel comprises two separate components, proxy and Per-App Tunneling, each with their own architecture and security features. For more information, see [VMware Tunnel Architecture and Deployment Model on page 10](#).

VMware Tunnel offers two architecture models for deployment, that is single-tier and multi-tier. For more information on deployment models and components, see [VMware Tunnel Deployment Model on page 12](#).

VMware Tunnel Pre-Deployment Configuration

Preparing for your VMware Tunnel installation ensures a smooth installation process. Installation includes performing preliminary steps in the Workspace ONE UEM console, and setting up a server that meets the listed hardware, software, and network requirements. For more information, see [VMware Tunnel Core Configuration on page 16](#).

Deploy VMware Tunnel on Unified Access Gateway

VMware offers a hardened virtual appliance (Unified Access Gateway) that hosts Workspace ONE services like Per-app Tunnel, and is the preferred method for deployment. Deploying Tunnel on Unified Access Gateway can be done from either vSphere or Hyper-V and can be automated using PowerShell.

From an architecture and networking perspective, Unified Access Gateway and the stand-alone Linux installer are the same. The Tunnel service on Unified Access Gateway is same as what the Linux installer provides. For more information, see [VMware Tunnel Deployment with Unified Access Gateway on page 37](#).

Deploy VMware Tunnel on Linux Server

For customers who do not want to use the Unified Access Gateway deployment, Workspace ONE UEM offers the Linux installer so you can configure, download, and install VMware Tunnel onto a server. The Linux installer has different prerequisites than the Unified Access Gateway method. To run the Linux installer, you must meet specific hardware, software, and general requirements before you can begin installation. For information see, [VMware Tunnel Deployment on a Linux Server on page 56](#).

VMware Tunnel Management

Consider configuring additional functionality to enhance your VMware Tunnel deployment. These features allow you more control over device access and networking support. For more information, see [VMware Tunnel Management on page 71](#).

VMware Tunnel Troubleshooting

The VMware Tunnel supports troubleshooting logs to aid in diagnosing issues in your deployment. For more information, see [VMware Tunnel Troubleshooting and Support on page 84](#).

Supported Platforms for VMware Tunnel

Read through the following section to know more about the supported platforms and considerations of each of the platforms.

Supported Console Versions

VMware Tunnel works with all the supported versions of VMware Workspace ONE UEM.

Supported Platforms

VMware Tunnel supports iOS, macOS, Android, and Windows 10. The following table outlines the requirements for each of the supported platforms.

Platform	Requirements
iOS	<ul style="list-style-type: none"> • VMware Tunnel for iOS <ul style="list-style-type: none"> ◦ iOS 9.3+ • AirWatch Tunnel for iOS <ul style="list-style-type: none"> ◦ iOS 8.0+ ◦ Consider using VMware Tunnel if your devices run 9.3+.
macOS	macOS 10.12+
Android	Workspace ONE Intelligent Hub v5.3+ for Android Android 4.4+
Windows 10	Windows 10 Build 14393+

Android Considerations

- After installing VMware Tunnel for Android, end users must run the app 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 VPN functionality. This icon does not indicate an active connection or session with the VMware Tunnel server. The key icon displays even if you are not actively browsing.
- If you are using Per-App Tunnel with Android devices in a cascade mode, then ensure that your internal DNS is exposed to the VMware Tunnel front-end server in the DMZ. For basic endpoint setups, ensure that your internal DNS is exposed to the VMware Tunnel server in the DMZ. For more information, see the knowledge base article, [Configure Per-App Tunnel DNS entries for Android and Windows 10 devices](#).
- Certain Android devices allow end users to disable the VPN on an OS level. This prevents the VMware Tunnel from working on the device.
- If you are adding an internal application, Per-App VPN Profile tunneling currently supports only the Android (Legacy) devices. However, Android Work Profile and the Work Managed devices do not support Per-App VPN Profile tunneling for all the internal applications.

Windows 10 Considerations

- After installing VMware Tunnel for Windows 10, end users must accept an alert the first time they start an application that triggers VMware Tunnel.
- When using Windows 10 devices, ensure that your DNS server does not use 192.168.x.x IP as this address is used by the VMware Tunnel Server to assign the IPs to clients (mobile devices). This setting is a configurable setting in server.conf.
- The VMware Tunnel displays as Connected whenever an end user opens a managed app that you configured to use the App Tunnel profile.

Note: VMware Tunnel for Windows 10 does not support VMware Browser for Windows.

iOS and macOS Considerations

End users who are using the Tunnel App on iOS and macOS must download and install VMware Tunnel from the App Store. After installing it, end users have to run it at least once and accept the User Permission prompt.

Important: VMware Tunnel must be present on devices before assigning the VPN profile. For more information on migrating to VMware Tunnel, see [VMware Tunnel client to replace AirWatch Tunnel client on iOS](#)

Chapter 2:

Key Concepts

Understanding the key concepts that are used throughout VMware Tunnel helps you make most of your enterprise mobility experience with enhanced security architecture, simplified management and a greater emphasis on the end-user VPN connectivity experience. Read through the key concepts to get familiar with the VMware Tunnel technologies and features.

App Tunnel and Secure Browsing

App tunnel is a generic term used to describe the act of creating a secure "tunnel" through which traffic can pass between an end-user device and a secure internal resource, such as a website or file server.

By using the VMware Tunnel with VMware Browser, you can provide secure internal browsing to any intranet site and web application that resides within your network. Because VMware Browser is designed with application tunneling capabilities, all it takes to enable mobile access to your internal websites is to enable a setting from the Workspace ONE UEM console. By doing so, VMware Browser establishes a trust with VMware Tunnel using a Workspace ONE UEM issued certificate and accesses internal websites by proxying traffic through the VMware Tunnel over SSL encrypted HTTPS. IT can not only provide greater levels of access to their mobile users, but also remain confident that security is not compromised by encrypting traffic, remembering history, disabling copy/paste, defining cookie acceptance, and more.

Per-App Tunnel Component

It is considered to be a best practice to use the Per-App Tunnel component as it provides the most functionality with easier installation and maintenance. Per-App Tunnel uses the native platform (Apple, Google, Microsoft) APIs to provide a seamless experience for users. The Per-App Tunnel provides most of the same functionality of the Proxy component without the need for additional configuration that Proxy requires.

The Per App Tunnel component and VMware Tunnel apps for iOS, Android, Windows Desktop, and macOS allow both internal and public applications to access corporate resources that reside in your secure internal network. They allow this functionality using per app tunneling capabilities. Per app tunneling lets certain applications access internal resources on an app-by-app basis. This restriction means that you can enable some apps to access internal resources while you leave others unable to communicate with your back-end systems.

Proxy Component

Proxy is the VMware Tunnel component that handles securing traffic between an end-user device and a website through the VMware Browser mobile application. VMware Tunnel Proxy is also available on Windows. To use an internal application with VMware Tunnel Proxy, then ensure the VMware AirWatch® Software Development Kit™ is embedded in your application, which gives you tunneling capabilities with this component.

VMware Tunnel and Unified Access Gateway

VMware offers a hardened virtual appliance deployment known as Unified Access Gateway that hosts Workspace ONE services like Per-App Tunnel, and is the preferred method for deployment. Deploying VMware Tunnel on Unified Access Gateway can be done from either vSphere or Hyper-V and can be automated using PowerShell.

From an architecture and networking perspective, Unified Access Gateway and the stand-alone Linux installer are the same. The Tunnel service on Unified Access Gateway is same as what the Linux installer provides.

Load Balancing

The VMware Tunnel can be load balanced for improved performance and faster availability. Using a load balancer requires additional considerations.

The Per-App Tunnel component requires authentication of each client after a connection is established. Once connected, a session is created for the client and stored in memory. The same session is then used for each piece of client data so the data can be encrypted and decrypted using the same key. When designing a load balancing solution, the load balancer must be configured with an IP or session-based persistence enabled. The load balancer sends data from a client to the same server for all its traffic during the connection. An alternative solution might be to – on the client side – use a DNS round robin, which means the client can select a different server for each connection.

The Proxy component authenticates devices based on HTTP header information in the request. Ensure that the load balancer is configured to Send Original HTTP Headers so that these headers are not removed when going through the load balancer to VMware Tunnel.

For more information on load balancing with Unified Access Gateway appliances, see Unified Access Gateway Load Balancing Topologies in the [Unified Access Gateway Documentation](#).

App Certificate Authentication and Encryption

When you whitelist an application for corporate access through the VMware Tunnel, Workspace ONE UEM automatically deploys a unique X.509 certificate to enrolled devices. This certificate can then be used for mutual authentication and encryption between the application and the VMware Tunnel. Unlike other certificates used for Wi-Fi, VPN, and email authentication, this certificate resides within the application sandbox and can only be used within the specific app itself. By using this certificate, the VMware Tunnel can identify and allow only approved, recognized apps to communicate with corporate systems over HTTP(S), or, for Per-App Tunneling, TCP and HTTP(S).

Chapter 3:

VMware Tunnel Architecture and Deployment Model

The VMware Tunnel is a product you can install on physical or virtual servers that reside in either the DMZ or a secured internal network zone. VMware Tunnel comprises two separate components, Proxy and Per-App tunneling, each with their own features.

Consider using the Per-App Tunnel component as it provides the most functionality with easier installation and maintenance. Per-App Tunnel uses the native platform (Apple, Google, Microsoft) APIs to provide a seamless experience for users.

The Proxy component provides most of the same functionality of Per-App Tunnel with the need for additional configuration.

VMware Tunnel offers single-tier and multi-tier deployment models. Both the configurations support load-balancing for faster availability. The Proxy component supports SSL offloading, while Per-App tunneling cannot be SSL-offloaded.

Per-App Tunnel Architecture

The per app tunneling solution implements app-level access controls to your network. Traffic from apps is routed through the native framework and arrives at the VMware Tunnel client as data streams. The data streams pass through the same channel as a full-device VPN does and arrive at the Tunnel server. On the server side, the server opens a TCP connection for each data stream and the data is sent to the destination host through the data stream. Once a connection is made, data can continuously flow between the client and host until either side drops the connection.

Proxy (SDK/Browser) Architecture

The VMware Tunnel Proxy component uses HTTPS tunneling to use a single port to filter traffic through an encrypted HTTPS tunnel for connecting to internal sites such as SharePoint or a wiki.

When accessing an end site, such as SharePoint, an intranet, or wiki site, traffic is sent through an HTTPS tunnel, regardless of whether the end site is HTTP or HTTPS. For example, if a user accesses a wiki site, whether it is **http://<internalsite>.wiki.com** or **https://<internalsite>.wiki.com**, the traffic is encrypted in an HTTPS tunnel and sent

over the port you have configured. This connection ends once it reaches the VMware Tunnel and is sent over to the internal resource as either HTTP or HTTPS.

HTTPS Tunneling is enabled by default. Enter your desired port for the **Default HTTPS Port** during VMware Tunnel configuration, as described in VMware Tunnel Configuration.

The current authentication scheme requires the use of a chunk aggregator of fixed size. A low value puts restrictions on the amount of data that is sent from the devices in a single HTTP request. By contrast, a faster value causes extra memory to be allocated for this operation. Workspace ONE UEM uses a default optimum value of 1 MB, which you can configure based on your maximum expected size of upload data. Configure this value in the proxy.properties file on the VMware Tunnel Proxy server in the **/conf** directory.

Managing VMware Tunnel Certificates

VMware Tunnel uses certificates to authenticate communication among the Workspace ONE UEM console, VMware Tunnel, and end-user devices. The following workflows show the initial setup process and certificate integration cycle.

Initial Setup Workflow

1. VMware Tunnel connects to the Workspace ONE UEM API and authenticates with an **API Key** and a **Certificate**.
 - Traffic requests are SSL encrypted using HTTPS.
 - Setup authorization is restricted to admin accounts with a role enabled for an VMware Tunnel setup role (see preliminary steps).
2. Workspace ONE UEM generates a unique identity certificate pair for both the Workspace ONE UEM and VMware Tunnel environments.
 - The Workspace ONE UEM certificate is unique to the group selected in the Workspace ONE UEM console.
 - Both certificates are generated from a trusted Workspace ONE UEM root.
3. Workspace ONE UEM sends the unique certificates and trust configuration back to the VMware Tunnel server over HTTPS.

The VMware Tunnel configuration trusts only messages signed from the Workspace ONE UEM environment. This trust is unique per group.

Any additional VMware Tunnel servers set up in the same Workspace ONE UEM group as part of a highly available (HA) load-balanced configuration are issued the same unique VMware Tunnel certificate.

For more information about high availability, refer to the **VMware Workspace ONE UEM Recommended Architecture Guide**.

Certificate Integration Cycle

1. Workspace ONE UEM generates Device Root Certificates that are unique to every instance during the installation process.
 - For Proxy:** The Device Root Certificate is used to generate client certificates for each of the applications and devices.
 - For Per-App Tunnel:** The Device Root Certificate is used to generate client certificates for each of the devices.
2. **For Proxy:** The certificate an application uses to authenticate with the VMware Tunnel is only provided after the

application attempts to authenticate with the Workspace ONE UEM enrollment credentials for the first time.

For Per-App Tunnel: The certificate is generated at the time of profile delivery.

3. VMware Tunnel gets the chain during installation. The VMware Tunnel installer is dynamically packaged and picks these certificates at the time of download.
4. Communication between the VMware Tunnel and device-side applications (includes VMware Browser and wrapped applications using app tunneling) is secured by using the identity certificates generated during installation. These identity certs are child certificates of the Secure Channel Root certificate.
5. VMware Tunnel makes an outbound call to the AWCM/API server to receive updated details on the device and certificates. The following details are exchanged during this process: *DeviceUid*, *CertThumbprint*, *applicationBundleId*, *EnrollmentStatus*, *complianceStatus*.
6. VMware Tunnel maintains a list of devices and certificates and only authenticates the communication if it sees a certificate it recognizes.
X.509 (version 3) digitally signed client certificates are used for authentication.

VMware Tunnel Deployment Model

The VMware Tunnel supports deploying a single-tier model and a multi-tier model. Both SaaS and on-premises Workspace ONE environments support the single-tier and multi-tier models. You can use the deployment model that best fits your needs.

Single-Tier Deployment Model

Single-tier models have a single instance of VMware Tunnel configured with a public DNS. In the Workspace ONE UEM console and the installer, this deployment model uses the basic-endpoint model.

Multi-Tier Deployment Model

Multi-tier networks have a separation between servers with firewalls between the tier. Typical Workspace ONE multi-tier deployments have a DMZ that separates the Internet from the internal network. VMware Tunnel supports deploying a front-end server in the DMZ that communicates with a back-end server in the internal network. The multi-tier deployment model includes two instances of the VMware Tunnel with separate roles. The VMware Tunnel front-end server resides in the DMZ and can be accessed from public DNS over the configured ports. The servers in this deployment model communicate with your API and AWCM servers. For SaaS deployments, Workspace ONE hosts the API and AWCM components in the cloud. For an on-premises environment, the AWCM component is typically installed in the DMZ with the API.

The cascade deployment model architecture includes two instances of the VMware Tunnel with separate roles. In cascade mode, the front-end server resides in the DMZ and communicates to the back-end server in your internal network.

If you are using a multi-tier deployment model and the Proxy component of the VMware tunnel, use the relay-endpoint deployment mode. The relay-endpoint deployment mode architecture includes two instances of the VMware Tunnel with separate roles. The VMware Tunnel relay server resides in the DMZ and can be accessed from public DNS over the configured ports.

Single-Tier Deployment Model

If you are using the single-tier deployment model, use the basic-endpoint mode. The basic endpoint deployment model of VMware Tunnel is a single instance of the product installed on a server with a publicly available DNS.

Basic VMware Tunnel is typically installed in the internal network behind a load balancer in the DMZ that forwards traffic on the configured ports to the VMware Tunnel, which then connects directly to your internal Web applications. All deployment configurations support load balancing and reverse proxy.

The basic endpoint Tunnel server communicates with API and AWCM to receive a whitelist of clients allowed to access VMware Tunnel. Both proxy and Per-App Tunnel components support using an outbound proxy to communicate with API/AWCM in this deployment model. When a device connects to VMware Tunnel, it is authenticated based on unique X.509 certificates issued by Workspace ONE UEM. Once a device is authenticated, the VMware Tunnel (basic endpoint) forwards the request to the internal network.

If the basic endpoint is installed in the DMZ, the proper network changes must be made to allow the VMware Tunnel to access various internal resources over the necessary ports. Installing this component behind a load balancer in the DMZ minimizes the number of network changes to implement the VMware Tunnel and provides a layer of security because the public DNS is not pointed directly to the server that hosts the VMware Tunnel.

Cascade Mode Deployment

The cascade deployment model architecture includes two instances of the VMware Tunnel with separate roles. In cascade mode, the front-end server resides in the DMZ and communicates to the back-end server in your internal network.

Only the Per-App Tunnel component supports the cascade deployment model. Cascade mode supports a relay-endpoint service if you use the Per-App component and the Proxy component in combination. If you use only the Proxy component, you must use the Relay-Endpoint model. For more information, see [Relay-Endpoint Deployment on page 14](#).

Devices access the front-end server for cascade mode using a configured hostname over configured ports. The default port for accessing the front-end server is port 8443. The back-end server for cascade mode is installed in the internal network hosting your intranet sites and web applications. This deployment model separates the publicly available front-end server from the back-end server that connects directly to internal resources, providing an extra layer of security.

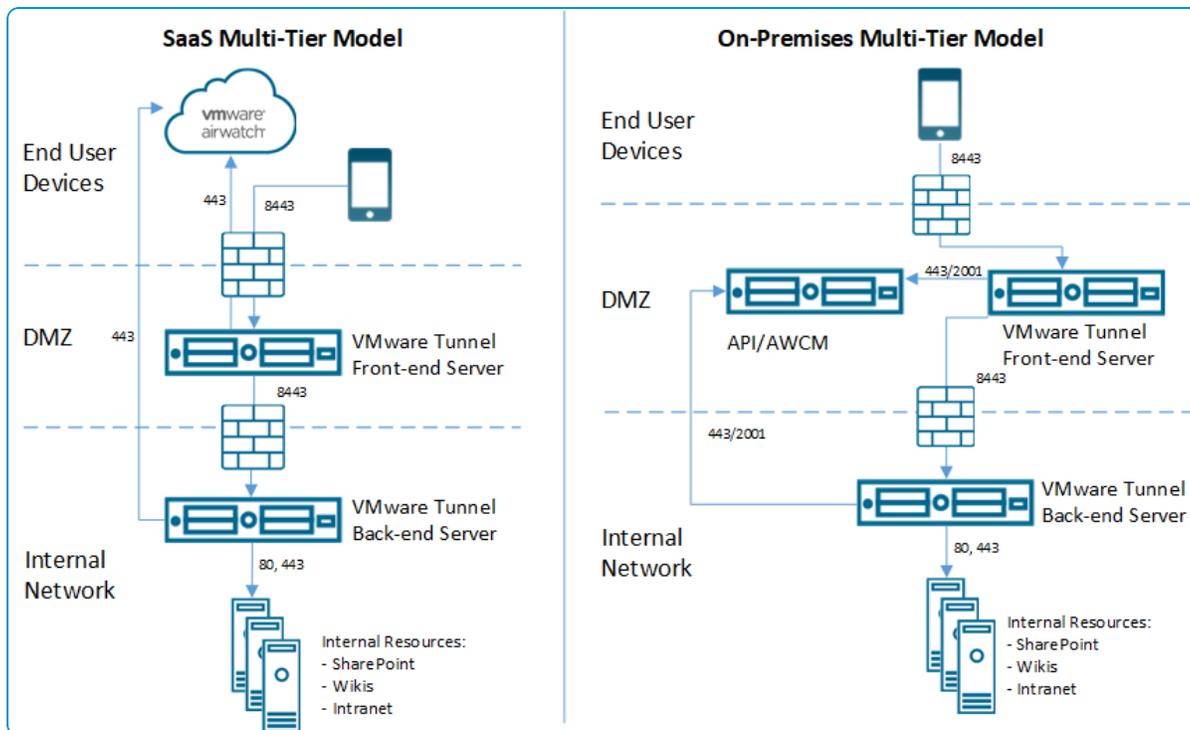
The front-end server facilitates authentication of devices by connecting to AWCM when requests are made to the VMware Tunnel. When a device makes a request to the VMware Tunnel, the front-end server determines if the device is authorized to access the service. Once authenticated, the request is forwarded securely using TLS over a single port to the back-end server.

The back-end server connects to the internal DNS or IP requested by the device.

Cascade mode communicates using TLS connection (or optional DTLS connection). You can host as many front-end and back-end servers as you like. Each front-end server acts independently when searching for an active back-end server to connect devices to the internal network. Each back-end server must share the same hostname. You can set up multiple DNS entries in a DNS lookup table to allow load balancing.

Both the front-end and back-end servers communicate with the Workspace ONE UEM API server and AWCM. The API server delivers the VMware Tunnel configuration and the AWCM delivers device authentication, whitelisting, and traffic rules. The front-end and back-end server communicates with API/AWCM through direct TLS connections unless you enable outbound proxy calls. Use this connection if the front-end server cannot reach the API/AWCM servers. If enabled, front-end servers connect through the back-end server to the API/AWCM servers. This traffic, and the back-end traffic, route using server-side traffic rules. For more information, see [Configure Network Traffic Rules for the Per-App Tunnel Component on page 25](#)

The following diagram illustrates the Multi-Tier deployment for the Per-App Tunnel component in cascade mode:



Relay-Endpoint Deployment

If you are using a multi-tier deployment model and the Proxy component of the VMware tunnel, use the relay-endpoint deployment mode. The relay-endpoint deployment mode architecture includes two instances of the VMware Tunnel with separate roles. The VMware Tunnel relay server resides in the DMZ and can be accessed from public DNS over the configured ports.

If you are only using the Per-App Tunnel component, consider using a cascade mode deployment. For more information, see [Cascade Mode Deployment on page 13](#).

The ports for accessing the public DNS are by default port 8443 for Per-App Tunnel and port 2020 for proxy. The VMware Tunnel endpoint server is installed in the internal network hosting intranet sites and Web applications. This server must have an internal DNS record that is resolved by the relay server. This deployment model separates the publicly available server from the server that connects directly to internal resources, providing an added layer of security.

The relay server role includes communicating with the API and AWCM components and authenticating devices when requests are made to VMware Tunnel. In this deployment model, VMware Tunnel supports an outbound proxy for communicating with API and AWCM from the relay. The Per-App Tunnel service must communicate with API and AWCM directly. When a device makes a request to the VMware Tunnel, the relay server determines if the device is authorized to access the service. Once authenticated, the request is forwarded securely using HTTPS over a single port (the default port is 2010) to the VMware Tunnel endpoint server.

The role of the endpoint server is to connect to the internal DNS or IP requested by the device. The endpoint server does not communicate with the API or AWCM unless **Enable API and AWCM outbound calls via proxy** is set to **Enabled** in the VMware Tunnel settings in the Workspace ONE UEM console. The relay server performs health checks at a regular interval to ensure that the endpoint is active and available.

These components can be installed on shared or dedicated servers. Install VMware Tunnel on dedicated Linux servers to ensure that performance is not impacted by other applications running on the same server. For a relay-endpoint

deployment, the proxy and Per-App Tunnel components are installed on the same relay server. Only the Proxy component is installed on the endpoint server. The Per-App Tunnel relay component uses the proxy endpoint to connect to internal applications, so the components share a relay-endpoint port and the same endpoint hostname.

Chapter 4:

VMware Tunnel Core Configuration

Preparing for your VMware Tunnel installation ensures a smooth installation process. Installation includes performing preliminary steps in the Workspace ONE UEM console, and setting up a server that meets the listed hardware, software, and network requirements.

Before deploying the VMware Tunnel, you must complete the following pre-deployment configurations:

1. Before you begin installing VMware Tunnel, you have to ensure that the API and AWCM are installed correctly, running, and communicating with the Workspace ONE UEM without any errors. For more information, see [Configure AWCM Server and Enable API Access on page 16](#).
2. After completing AWCM Server configuration, you can configure VMware Tunnel settings per your deployment's configuration and functionality needs in the Workspace ONE UEM console. For more information, see [Configure VMware Tunnel on page 17](#).
3. After you complete the VMware Tunnel configuration, you also must configure various settings to enable the VMware Browser and Per-App Tunnel-enabled apps to use VMware Tunnel. Doing so ensures all HTTP(S) and TCP traffic for the specified applications is routed through the VMware Tunnel. For more information, see [Enable and Configure Kerberos Proxy Settings for the Proxy component on page 30](#).
4. The **Advanced** tab under **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration** lets you configure more settings that are optional for an VMware Tunnel deployment. Except where noted, you can configure these settings before or after installation. For more information, see [Configure Advanced Settings for the Proxy Component on page 29](#).

Configure AWCM Server and Enable API Access

Before you begin installing VMware Tunnel, you have to ensure that the API and AWCM are installed correctly, running, and communicating with the Workspace ONE UEM without any errors. Read through the following topic to configure the AWCM server.

Important: If you are an on-premises customer, do not configure VMware Tunnel at the Global organization group level. Configure VMware Tunnel at the Company level or Customer type organization group. The REST API key can only be generated at a Customer type organization group.

To configure the AWCM Server and to enable the API access, perform the following steps:

1. Navigate to **Groups & Settings > All Settings > System > Advanced > Site URLs** in the Workspace ONE UEM console.
2. Validate the following URLs in Site URLs:

Setting	Description
REST API URL	Enter in the format of "https://<url>/api". SaaS customers must contact Workspace ONE UEM support to get their REST API URL.
AWCM Server External URL –	Enter in the format of "server.acme.com" and <u>do not</u> include a protocol such as https.
AWCM Service Internal URL –	Enter in the format of "https://server.acme.com". For on-premises customers, the default port for AWCM is 2001. For SaaS customers, AWCM and API use port 443.

3. Select **Save**.
4. Navigate to **Groups & Settings > All Settings > System > Advanced > API > REST API** and select the **Override** radio button.
5. Ensure that the **Enable API Access** check box is selected and an API Key is displayed in the text box.
6. Select **Save**.

Configure VMware Tunnel

Configure the VMware Tunnel installer in the UEM console under **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel**. The wizard walks you through the installer configuration step-by-step. The options configured in the wizard are packaged in the installer, which you can download from the UEM console and move to your Tunnel servers. Changing the details in this wizard typically requires a reinstall of the VMware Tunnel with the new configuration.

To configure the VMware Tunnel, you need the details of the server where you plan to install. Before configuration, determine the deployment model, one or more hostnames and ports, and which features of VMware Tunnel to implement, such as access log integration, NSX integration, SSL offloading, enterprise certificate authority integration, and so on. Because the wizard dynamically displays the appropriate options based on your selections, the configuration screens may display different text boxes and options.

To configure the VMware Tunnel, perform the following steps:

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration**.
If this is your first time configuring VMware Tunnel, then select **Configure** and follow the configuration wizard screens. Otherwise, select **Override**, then select the **Enable VMware Tunnel** check box, and then select **Configure**.
2. On the **Configuration Type** screen, select the components that you want to configure.
Your options are **Proxy** and **Per-App Tunnel**. Depending on your selections, the following screens may display different text boxes and options. In the drop-down menus that display, select whether you are configuring a **Cascade**, **Relay-Endpoint**, or **Basic** deployment for each component. Select the information icon to see an example for the selected type.

3. Select **Next**.
4. On the **Details** screen, configure the following settings:

Setting	Description
PROXY (APP WRAPPING / BROWSER / SDK) CONFIGURATION	
Relay Host Name	(Relay-Endpoint Only). Enter the FQDN of the public host name for the Tunnel relay server, for example, tunnel.acmemdm.com. This hostname must be publicly available as it is the DNS that devices connect to from the Internet.
Endpoint Host Name	The internal DNS of the Tunnel endpoint server. This value is the hostname that the relay server connects to on the relay-endpoint port. If you plan to install the VMware Tunnel on an SSL offloaded server, enter the name of that server in place of the Host Name . When you enter the Host Name , do not include a protocol, such as http://, https://, etc.
Relay Port (HTTPS)	The proxy service is installed on this port. Devices connect to the <relayhostname>:<port> to use the VMware Tunnel proxy feature. The default value is 2020.
Relay-Endpoint Port	(Relay-Endpoint only). This value is the port used for communication between the VMware Tunnel relay and VMware Tunnel endpoint. The default value is 2010. If you are using a combination of Proxy and Per-App Tunnel, the relay endpoint installs as part of the Front-End Server for Cascade mode. The ports should be different values.
Advanced Proxy Configuration Details	
Use Kerberos Proxy	Enable Kerberos proxy support to allow access to Kerberos authentication for your target back end Web services. This feature does not currently support Kerberos Constrained Delegation (KCD). For more information, see Enable and Configure Kerberos Proxy Settings for the Proxy component on page 30 . The Endpoint server must be on the same domain as KDC for the Kerberos Proxy to communicate successfully with the KDC.
Realm	Enter the domain of the KDC server. This text box only displays if you enable Use Kerberos Proxy .
PER - APP TUNNELING CONFIGURATION	
Basic Mode	
Hostname	Enter the FQDN of the public host name for the Tunnel server, for example, tunnel.acmemdm.com. This hostname must be publicly available as it is the DNS that devices connect to from the Internet.
Port	Enter the port number assigned for communication with the VMware Tunnel component. The default value is 8443.
Cascade Mode	
Front-end Hostname	Enter the FQDN of the public host name for the Tunnel relay server, for example, tunnel.acmemdm.com. This hostname must be publicly available as it is the DNS that devices connect to from the Internet.

Setting	Description
Front-end Port	Enter the port number assigned for communication with the VMware Tunnel component. The default value is 8443.
Back-end Hostname	Enter the hostname of the back-end server. When entering the hostname, do not include protocol (http://, https://, and so on).
Back-end Port	Enter the port used for communication between the VMware Tunnel relay and the Per-App Tunnel endpoint. The default value is 8443.

- Select **Next**.
- On the **SSL** screen, configure the following settings to select the certificates that secure client-server communication from enabled application on a device to the VMware Tunnel.

Setting	Description
PROXY (APP WRAPPING / BROWSER / SDK) SSL CERTIFICATE	
Default	By default, this setup uses a Workspace ONE UEM certificate for secure server-client communication. Workspace ONE UEM issues a certificate for the hostname configured on the Details screen.
Use Public SSL Certificate	Enable this option if you prefer to use a third-party SSL certificate for encryption between VMware Browser or SDK-enabled apps and the VMware Tunnel server. Upload a .PFX or .P12 certificate file and enter the password. This file must contain both your public and private key pair. CER and CRT files are not supported.
PER - APP TUNNELING SSL CERTIFICATE	
Default	By default, this setup uses a Workspace ONE UEM certificate for secure server-client communication. Workspace ONE UEM issues a unique certificate for the hostname configured on the Details screen. To use the Default option, select Next , and certificates are generated automatically.
Use Public SSL Certificate	Enable this option if you prefer to use a third-party SSL certificate for encryption between VMware Browser or SDK-enabled apps and the VMware Tunnel server. Upload a .PFX or .P12 certificate file and enter the password. This file must contain both your public and private key pair. CER and CRT files are not supported. SAN certificates are not currently supported. Certificates must be either issued to the VMware Tunnel Hostname or a valid wildcard certificate for the corresponding domain. The Tunnel Device Root Certificate is automatically generated when you select Next to continue to the Authentication section.

- Select **Next**.
- On the **Authentication** screen, configure the following settings to select the certificates that devices use to authenticate to the VMware Tunnel.

Proxy Authentication / Per-App Tunnel Authentication – By default, all the components use Workspace ONE UEM issued certificates. To use Enterprise CA certificates for client-server authentication, select the Enterprise CA option.

- Select **Default** to use Workspace ONE UEM issued certificates. The default Workspace ONE UEM issued client certificate does not automatically renew. To renew these certificates, re-publish the VPN profile to devices that have an expiring or expired client certificate. View the certificate status for a device by navigating to **Devices > Device Details > More > Certificates**.
- Select **Enterprise CA** in place of Workspace ONE UEM-issued certificates for authentication between the VMware Browser, Per-App Tunnel-enabled apps, or SDK-enabled apps and the VMware Tunnel requires that a certificate authority and certificate template are set up in your Workspace ONE UEM environment before configuring VMware Tunnel.
 - Select the certificate authority and certificate template that are used to request a certificate from the CA.
 - Upload the full chain of the public key of your certificate authority to the configuration wizard.

The CA template must contain *CN=UDID* in the subject name. Supported CAs are ADCS, RSA, and SCEP.

Certificates auto-renew based on your CA template settings.

9. Select **Next**.
10. On the **Miscellaneous** screen, you can enable access logs for the proxy or Per-App Tunnel components. If you intend to use this feature you must configure it now as part of the configuration, as it cannot be enabled later without reconfiguring Tunnel and rerunning the installer. For more information on these settings, see [Access Logs and Syslog Integration on page 81](#) and [Configure Advanced Settings for the Proxy Component on page 29](#).
For Per-App Tunneling, you can also configure NSX Communication, which is the integration between Workspace ONE UEM and VMware NSX to achieve micro-segmentation. For more information on this integration, refer to the **VMware AirWatch and VMware NSX Integration Guide**.
11. Select **Next**, review the summary of your configuration, confirm that all hostnames, ports and settings are correct, and select **Save**. The installer is now ready to download on the VMware Tunnel configuration screen.
12. If you plan to use SSL offloading for the VMware Tunnel Proxy component, select the Advanced tab on the Tunnel Configuration screen and select **Export Proxy Certificate**. Then, import this certificate on the server performing SSL offloading. (This server can be a load balancer or reverse proxy.)
13. Select the **General** tab and then select the **Download Unified Access Gateway Appliance** hyperlink. This button downloads the OVA or vhd file. The download file also includes the PowerShell script and .ini template file for the PowerShell deployment method.
For legacy installer methods, select Download Linux Installer. This button downloads a single TAR file used for deploying the relay and endpoints. You must also confirm a certificate password that is used during installation. The password must contain a minimum of six characters.
14. Select **Save**.

Chapter 5:

VMware Tunnel Advanced Configuration

After you complete the pre-deployment configuration, you can configure advanced settings for VMware Tunnel that are optional for VMware Tunnel deployment. Except where noted, you can configure these settings before or after installation.

Configure Advanced Settings for VMware Tunnel

The Advanced settings tab in VMware Tunnel lets you configure more settings that are optional for an VMware Tunnel deployment. For example, you can configure RSA Adaptive Auth Integration, Kerberos Proxy Port, API and AWCN outbound calls via proxy and so on. All the advanced configuration, except where noted, can be completed before or after installation.

Configure Network Traffic Rules for the Per-App Tunnel Component

Network traffic rules allow you to set granular control over how the VMware Tunnel directs traffic from devices. Device traffic rules forces VMware Tunnel to send traffic through the tunnel, block all the traffic to specified domains, bypass the internal network straight to the Internet, or send traffic to an HTTPS proxy site. Server traffic rules enable you to manage the network traffic when you have third-party proxies configured in your network.

Configure Outbound Proxy for the Proxy and Per-App Tunnel Component

Many organizations use outbound proxies to control the flow of traffic to and from their network. Outbound proxies can also be used for performing traffic filtering, inspection, and analysis.

It is not mandatory to use outbound proxies with VMware Tunnel, but your organization may choose to deploy them behind one or more VMware Tunnel servers based on recommendations from your security and network teams. For VMware Tunnel on Linux, Workspace ONE UEM supports outbound proxies for the two VMware Tunnel components: Proxy and Per-App Tunnel. For VMware Tunnel on Windows, Workspace ONE UEM supports outbound proxies for the Proxy component.

SSL Offloading the Proxy Component

You can configure SSL Offloading to ease the burden of encrypting and decrypting traffic from the VMware Tunnel server. Only the VMware Tunnel Proxy component supports SSL Offloading. You can perform SSL offloading with products such as F5's BIG-IP Local Traffic Manager (LTM), or Microsoft's Unified Access Gateway, Threat Management Gateway (TMG) or Internet Security and Acceleration Server (ISA) solutions. VMware Tunnel Proxy is compatible with general SSL offloading solutions if the solution supports the HTTP CONNECT method.

Configure Advanced Settings for the Per-App Tunnel Component

The Advanced settings tab lets you configure more settings that are optional for the Per-App component. Except where noted, you can configure these settings before or after installation.

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration** and select the **Advanced** tab.
2. Configure the following VMware Tunnel Proxy component settings. Any changes to the Per-App Tunneling settings after installation of the VMware Tunnel server do not require restarting or re-installation of the service. Changes automatically apply to the server.

Setting	Description
Log Level	Select the level of logging for the Per-App Tunnel component.
Access Logs	<p>Enable this setting to tell VMware Tunnel to write access logs to syslog for any of your own purposes. These logs are not stored locally. They are pushed to the syslog host over the port you define. Communication to the syslog server occurs over UDP, so ensure that UDP traffic is allowed over this port.</p> <p>In relay-endpoint deployments, the relay server writes the access logs, in a cascade deployment, the back-end server writes the access logs and in a basic deployment, the basic server writes the access logs.</p> <p>There is no correlation between this syslog integration and the integration accessed on Groups & Settings > All Settings > System > Enterprise Integration > Syslog.</p> <p>This feature can be enabled during initial configuration or after installation in the Advanced settings tab in the Workspace ONE UEM console. If configured after installation, the automatic configuration logic updates the tunnel server config with the updated access log settings and restarts the service.</p> <p>Syslog Hostname: Enter the URL of your syslog host. This setting displays after you enable Access Logs.</p> <p>Port: Enter the port over which you want to communicate with the syslog host. This setting displays after you enable Access Logs.</p>
API and AWCM outbound calls via proxy	Enable this option if the communication for initialization between the VMware Tunnel and Workspace ONE UEM API or AWCM is through an outbound proxy.

Setting	Description
Authentication	Maintain your SSL certificates <ul style="list-style-type: none"> If you are using AirWatch SSL, select Regenerate to regenerate the certificates If you are using public SSL certificates and you need to add a new certificate, consider using Public SSL Certificate Rotation.

3. Select **Save**.

Configure Outbound Proxy for the Per-App Tunnel Component

Many organizations use outbound proxies to control the flow of traffic to and from their network. Outbound proxies can also be used for performing traffic filtering, inspection, and analysis.

It is not mandatory to use outbound proxies with VMware Tunnel, but your organization may choose to deploy them behind one or more VMware Tunnel servers based on recommendations from your security and network teams. For VMware Tunnel on Linux, Workspace ONE UEM supports outbound proxies for the two VMware Tunnel components: Proxy and Per-App Tunnel.

Only the basic and cascade deployment models support outbound proxies for the Per-App Tunnel component through server traffic rules.

The following table illustrates outbound proxy support for the VMware Tunnel Per-App Tunnel component on Linux:

Proxy Configuration	Supported?
Outbound Proxy with no auth	✓
Outbound Proxy with basic auth	✓
Outbound Proxy with NTLM auth	✓
Multiple Outbound Proxies	✓
PAC Support	✓

Configure the rules for sending traffic to your outbound proxies using the server traffic rules. For more information, see [Create Server Traffic Rules on page 28](#).

If you want to send the requests to the API/AWCM servers through your outbound proxy as well, then you must enable the **Enable API and AWCM outbound calls via proxy** setting on the **VMware Tunnel > Advanced** settings page. Once enabled, add the respective web proxies for API/AWCM hostnames on the server traffic rules page.

VMware Tunnel PAC Utility

The VMware Tunnel PAC Utility allows you to use PAC files to configure outbound proxies for the Per-App Tunnel component.

Download the PAC utility bundle from the [Workspace ONE UEM Resources Portal](#). Install the PAC utility on any Linux server such as your VMware Tunnel server. Installation requires extracting the PAC utility and running the install script.

The PAC Utility only supports Linux servers currently.

The PAC utility does not support the following rules:

- Nested `if` statements
Try to put the inner logic above the outer logic. This change makes the outer logic lower ranked than the inner logic.
- `Else-if` statements
Try to convert these rules to `if` statements.
- Regex
- `myapaddress()`
- generic use of the AND operator

The PAC utility also supports only limited use of variable declaration and use.

Important: If the PAC file contains DNS resolution rules such as `dnsresolve()` or `isInNet()`, change the value of `traffic_rule_post_dns` in `server.conf` to `1` on your VMware Tunnel server.

Install the VMware Tunnel PAC Utility

Install the VMware Tunnel PAC Utility to use PAC files to configure your outbound proxies for the Per-App Tunnel component.

Prerequisites

You must meet the following network requirements:

- Access to the Workspace ONE UEM API server
The PAC utility requires access to the Workspace ONE UEM API server. The server is typically accessed over port 443. Consider installing the PAC utility on your VMware Tunnel server as the server already has access to the Workspace ONE UEM API server.
- Access to the PAC file
If you are hosting your PAC file on a Web server, the PAC utility must have access to that server.
- Python 2.7 installed on the server
- RHEL 6 and 7 as the server OS

Procedure

To install the PAC utility:

1. On the Linux server, extract the PAC utility bundle from the [Workspace ONE UEM Resources Portal](#).
The extract also creates the `pacreader` folder.
2. Open the `pacreader` folder.
3. To install the PAC utility in the `pacreader` folder, run the install script:

```
sudo ./install.sh
```

4. Configure the necessary properties in the `pacreader.properties` file:

Property	Description
API_SERVER_URL	Enter the API server URL.
API_KEY	Enter the API key for the API server. Find this key by navigating to Groups & Settings > All Settings > System > Advanced > API > REST API > API Key .
OG_ID	Enter the Organization Group ID for the OG in which the VMware Tunnel is configured.
PAC_LINK	Enter the URL of the PAC file if you host it on a Web server. If you configure PAC_LINK, do not configure PAC_PATH.
PAC_PATH	Enter the file path to the PAC file on the server. If you configure PAC_PATH, do not configure PAC_LINK.

5. Start the PAC utility:

```
./pacreader.sh start
```

Configure Network Traffic Rules for the Per-App Tunnel Component

Network traffic rules allow you to set granular control over how the VMware Tunnel directs traffic from devices. Using the Per-App Tunnel component of VMware Tunnel, create device traffic rules to control how devices handle traffic from specified applications and server traffic rules to manage network traffic when you have third-party proxies configured.

Device traffic rules force VMware Tunnel to send traffic through the tunnel, block all traffic to specified domains, bypass the internal network straight to the Internet, or send traffic to an HTTPS proxy site. The device traffic rules are created and ranked to give an order of execution. Every time a specified app is opened, VMware Tunnel checks the list of rules to determine which rule applies to the situation. If no set rules match the situation, VMware Tunnel applies the default action. The default action, set for all applications except for safari, applies to domains not mentioned in a rule. If no rules are specified, the default action applies to all domains. The device traffic rules created apply to all VPN VMware Tunnel profiles in the organization group the rules are created in.

Server traffic rules enable you to manage the network traffic when you have third-party proxies configured in your network. These rules apply to traffic originating from the VMware Tunnel. The rules force the VMware Tunnel to send traffic for specified destinations to either use the proxy or bypass it.

Supported Platforms

VMware Tunnel supports Network Traffic rules for the following platforms:

- iOS devices with VMware Tunnel for iOS
- macOS devices with VMware Tunnel for macOS
VMware Tunnel only supports network traffic rules for the Safari app for macOS devices.
- Android devices with VMware Tunnel for Android

VMware Tunnel supports enforcing the Per-App VPN rules configured in the Windows Desktop and Windows Phone VPN profiles.

 Looking for information on Single Sign-On? For information on implementing Android mobile single sign-on for Workspace ONE, see the Workspace ONE Quick Configuration Guide.

Create Device Traffic Rules

Add rules for VMware Tunnel to control how traffic is directed through the VMware Tunnel when using the Per-App Tunnel component. These rules allow you to tunnel, block, or bypass traffic as needed.

 Watch a tutorial video explaining how to create device traffic rules: [Configure the network traffic rules for Per-App Tunnel](#).

Prerequisites

- Configured VMware Tunnel with the Per-App Tunnel component enabled.
- For iOS and Android, applies to mobile applications configured for Per App VPN for VMware Tunnel. See [Configure Public Apps to Use Per App Profile on page 75](#) for more information.

Procedure

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Network Traffic Rules > Device Traffic Rules**.
2. Select whether to **Inherit** or **Override** the **Device Traffic Rules** settings. **Inherit** means you can use the settings of the current organization group's parent OG, while **Override** enables the settings for editing so you can modify the current OG's settings directly.
3. Configure the Device Traffic Rules settings:

Settings	Descriptions
Default Action	<p>This rule is automatically configured and applies to all applications except Safari.</p> <p>The default action is always applied last.</p> <ul style="list-style-type: none"> • Tunnel – All apps, except Safari, on the device configured for Per App VPN 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 VMware Tunnel for internal communications. • Block – Blocks all apps, except Safari, on the device configured for Per App VPN 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. • Bypass – All apps, except Safari, on the device configured for Per App VPN 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 VMware Tunnel to access their destination directly.

Settings	Descriptions
Add	Select Add to create a rule.
Rank	Select the up or down arrows to rearrange the ranking of your network traffic rules. You can also select-and-drag the rule. The up and down arrows only display when you have more than one rule created.
Application	Select Add to add a triggering application for the network rule. This drop-down menu is populated with applications with Per App VPN enabled and Safari for macOS. If you configure rules for the Safari app for macOS, the traffic rules override and disable any domain rules configured in existing profiles.
Action	Select the action from the drop-down menu that VMware Tunnel applies to all network traffic from the triggering app when the app starts. <ul style="list-style-type: none"> • Tunnel – Sends app network traffic for specified domains through the tunnel to your internal network • Block – Blocks all traffic sent to specified domains. • Bypass – Bypasses the VMware Tunnel so the app attempts to access specified domains directly. • 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
Destination Hostname	Enter the hostname applicable to the action set for the rule. For example, enter all the domains to block traffic from accessing using the Block action. Use a comma (,) to distinguish between hostnames. You may use wildcard characters for your hostnames. Wildcards must follow the format: <ul style="list-style-type: none"> • *.<domain>.* • *<domain>.* • *.* — You cannot use this wildcard for Safari domain rules. • * — You cannot use this wildcard for Safari domain rules. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>Note: Currently for all the iOS devices only the default traffic rule is supported for IPs as we do not consider IP based connections for evaluating the traffic rules.</p> </div>

4. Select **Save** to save your changes.
5. Select **Publish Rules** to update your applicable VMware Tunnel device profiles to a new version with the new network traffic rules. The updated device profiles publish to the assigned smart groups.

Create Server Traffic Rules

Add rules for the VMware Tunnel to manage how traffic is directed through a third-party proxy. These rules allow you to bypass the proxy or send traffic through it.

The server traffic rules only apply to VMware Tunnel servers using the Per-App Tunnel component.

To configure server traffic rules:

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Network Traffic Rules**. Select the **Server Traffic Rules** tab.
2. Configure the server traffic rule settings:

Settings	Descriptions
Outbound Proxy	
Add	Select to add a third-party outbound proxy. You may add additional outbound proxies by selecting Add again.
Hostname	Enter the proxy hostname.
Port	Enter the port the third-party proxy uses to listen to the VMware Tunnel.
Authentication	Select the proxy authentication method used. Selecting Basic or Ntlm displays the Credential text box.
Credentials	Enter the Username and Password for proxy authentication.
Network Rules	
Add	Select to add a server traffic rule.
Destination	Enter the destination hostname that triggers the traffic rule. Rules for a Windows 10 device must use IP address as the hostname. Windows 10 devices support using the following wildcards: <ul style="list-style-type: none"> • 10.10.* • 10.10.0.0/16 If you are entering multiple hostnames, separate them by commas. You can use regular expressions in the hostname.
Action	Select the action that the VMware Tunnel applies to server traffic for the destination hostname. <ul style="list-style-type: none"> • Bypass – Bypass the proxy and send all traffic directly to the destination hostname. • Proxy – Send server traffic through the outbound proxy. Selecting Proxy displays the Outbound Proxy menu.
Outbound Proxy	Select the Outbound proxy to handle server traffic for the destination hostname. If you select multiple outbound proxies, the proxies are used in a round-robin format. The proxies that populate this menu are those proxies added in the Outbound Proxy Settings section.

3. (Optional) Add any additional server traffic rules.

4. Select **Save** to save your changes.
5. Select **Publish Rules** to update send the rules to your VMware Tunnel server and auto-configure the servers to use these rules.
Consider checking that your proxies are active and functional before publishing rules.

Configure Advanced Settings for the Proxy Component

The Advanced settings tab lets you configure more settings that are optional for the Proxy component. Except where noted, you can configure these settings before or after installation.

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration** and select the **Advanced** tab.
2. Configure the following VMware Tunnel Proxy component settings.

Setting	Description
RSA Adaptive Auth Integration	Enable this setting if you want to integrate the Proxy component with RSA authentication for comprehensive Web browsing security.
Access Logs	<p>Enable this setting to tell VMware Tunnel to write access logs to syslog for any of your own purposes. These logs are not stored locally. They are pushed to the syslog host over the port you define. Communication to the syslog server occurs over UDP, so ensure that UDP traffic is allowed over this port.</p> <p>In relay-endpoint deployments, the relay server writes the access logs, in a cascade deployment, the back-end server writes the access logs and in a basic deployment, the basic server writes the access logs.</p> <p>There is no correlation between this syslog integration and the integration accessed on Groups & Settings > All Settings > System > Enterprise Integration > Syslog.</p> <p>This feature can be enabled during initial configuration or after installation in the Advanced settings tab in the Workspace ONE UEM console. If configured after installation, the automatic configuration logic updates the tunnel server config with the updated access log settings and restarts the service.</p> <p>Syslog Hostname: Enter the URL of your syslog host. This setting displays after you enable Access Logs.</p> <p>Port: Enter the port over which you want to communicate with the syslog host. This setting displays after you enable Access Logs.</p>
API and AWCM outbound calls via proxy	Enable this option if the communication for initialization between the VMware Tunnel and Workspace ONE UEM API or AWCM is through an outbound proxy.
Show detailed errors	Enable this option to ensure client applications (for example, VMware Browser) are informed when the VMware Tunnel fails to authenticate a device.
Log Level	Set the appropriate logging level, which determines how much data is reported to the LOG files.

Setting	Description
Authentication	Maintain your SSL certificates <ul style="list-style-type: none"> If you are using AirWatch SSL, select Regenerate to regenerate the certificates If you are using public SSL certificates and you need to add a new certificate, consider using Public SSL Certificate Rotation.

- If applicable, configure the following Relay - Endpoint Authentication Credentials settings, which are used for authentication between the relay and endpoint servers. These text boxes are pre-populated for you after configuration, but you can change them, for example, to meet your organization password strength requirements.

Setting	Description
Username	Enter the user name used to authenticate the relay and endpoint servers.
Password	Enter the password used to authenticate the relay and endpoint servers.

- Select **Save**.

Enable and Configure Kerberos Proxy Settings for the Proxy component

Kerberos KDC Proxy is supported for the Proxy component. VMware Tunnel Proxy supports Kerberos authentication in the requesting application. Kerberos KDC proxy (KKDCP) is installed on the endpoint server.

Workspace ONE UEM KKDCP acts as a proxy to your internal KDC server. Workspace ONE UEM-enrolled and compliant devices with a valid Workspace ONE UEM issued identity certificate can be allowed to access your internal KDC. For a client application to authenticate to Kerberos-enabled resources, all the Kerberos requests must be passed through KKDCP. The basic requirement for Kerberos authentication is to make sure that you install the Endpoint with the Kerberos proxy setting enabled during configuration in a network where it can access the KDC server.

Before you begin:

- For HTTPS sites, VMware Browser for Android supports Kerberos authentication only when the site also has NTLM authentication enabled. This requirement is because the Android WebView, on which the VMware Browser is built, does not support Kerberos authentication natively.
- HTTP Sites do not require NTLM authentication as the VMware Tunnel can perform Kerberos authentication without NTLM being enabled.
- Currently, this functionality is only supported with the VMware Browser v2.5 and higher for Android.

Enable Kerberos proxy settings

Complete the following steps to enable Kerberos proxy settings:

- During the configuration, check the box **Use Kerberos proxy** and enter the **Realm** of the KDC server.
- If the Realm is not reachable, then you can configure the **KDC server IP** on the **Advanced** settings tab in system settings.

Only add the IP if the Realm is not reachable, as it takes precedence over the Realm value entered in the configuration.

By default the Kerberos proxy server uses port 2040, which is internal only. Therefore, no firewall changes are required to have external access over this port.

3. Save the settings and download the installer to install VMware Tunnel Proxy.
4. Enable Kerberos from the SDK settings in the Workspace ONE UEM console so the requesting application is aware of the KKDCP. Navigate to **Groups & Settings > All Settings > Apps > Settings And Policies** and select **Security Policies**. Under Integrated Authentication, select **Enable Kerberos**. Save the settings.

Configure Kerberos Proxy Settings

Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration** and select the **Advanced** tab to configure the following Kerberos Proxy settings, which display only if you select **Use Kerberos Proxy** during the VMware Tunnel configuration.

If the realm info you entered during configuration does not work properly, you can enter the KDC IP address here, which overrides the information that you provided during configuration. You must reinstall the VMware Tunnel after changing these settings. A restart does not work.

Complete the following settings to configure Kerberos proxy settings:

Setting	Description
KDC Server IP	Enter your KDC Server IP address. This text box displays only if you select Use Kerberos Proxy during VMware Tunnel configuration.
Kerberos Proxy Port	Enter the port over which VMware Tunnel can communicate with your Kerberos Proxy. This text box displays only if you select Use Kerberos Proxy during VMware Tunnel configuration.

Configure Outbound Proxy for the Proxy Component

Many organizations use outbound proxies to control the flow of traffic to and from their network. Outbound proxies can also be used for performing traffic filtering, inspection, and analysis.

It is not mandatory to use outbound proxies with VMware Tunnel, but your organization may choose to deploy them behind one or more VMware Tunnel servers based on recommendations from your security and network teams. For VMware Tunnel on Linux, Workspace ONE UEM supports outbound proxies for the two VMware Tunnel components: Proxy and Per-App Tunnel.

The following table illustrates outbound proxy support for the VMware Tunnel Proxy component on Linux:

Proxy Configuration	Supported?
Outbound Proxy with no auth	✓
Outbound Proxy with basic auth	✓
Outbound Proxy with NTLM auth	✓
Multiple Outbound Proxies	✓ (Use Proxy Tool)
PAC Support	✓ (Use Proxy Tool)

During installation, the installer prompts you whether to use an outbound proxy. For relay-endpoint configurations, the outbound proxy communication is configured on the endpoint server that resides in your internal network and can communicate with the outbound proxy.

Outbound Proxy with Authentication

If you want to use an outbound proxy, then enter 'Yes' when prompted during Tunnel installation, which then prompts you for the following information:

- Proxy Host
- Proxy Port
- Whether the proxy requires any authentication (Basic/NTLM) and appropriate credentials

Entering this information and completing the installer enables outbound proxy support. This sends all traffic from the VMware Tunnel Proxy server – except requests to the Workspace ONE UEM API/AWCM servers – to the outbound proxy you configure. If you want to send the requests to the API/AWCM servers through your outbound proxy as well, then you must enable the **Enable API and AWCM outbound calls via proxy** setting on the **VMware Tunnel > Advanced** settings page.

PAC Files and Multiple Outbound Proxies

A PAC file is a set of rules that a browser checks against to determine where traffic is routed. If you want to use a proxy auto configuration (PAC) file, then provide the path to the PAC file location when prompted during Tunnel installation. If you want to use a PAC file for an outbound proxy that requires authentication, or if you want to use multiple proxies with different hostnames, or if some proxies require authentication (basic/NTLM) and some do not, then refer to [Use the Proxy Tool for PAC Files and Multiple Outbound Proxies \(Proxy Component\)](#) on page 32.

Use the Proxy Tool for PAC Files and Multiple Outbound Proxies (Proxy Component)

You can use the proxy tool if VMware Tunnel routes its outbound requests through an outbound proxy that has rules set in a PAC file that also requires authentication.

To use the tool, perform the following steps:

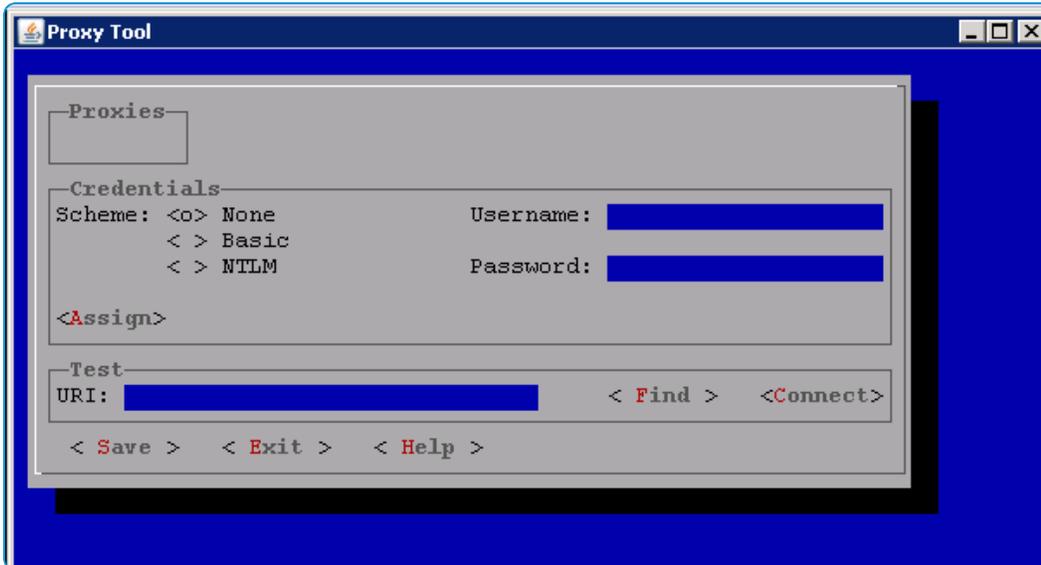
1. Within Linux CLI mode, navigate to `/opt/vmware/tunnel/proxy/tools`.
2. Convert the proxy tool to an executable by using the following command:

```
chmod a+x proxytool.sh
```

3. Run proxy-tools by using the following command:

```
sudo sh Proxytools.sh
```

4. Select your authentication method, which can be **None**, **Basic**, or **NTLM** for a single service account. Also enter your credentials, if applicable, and the **URI** of the proxy for testing.



5. Select **Save**.

After saving, check that the proxy settings updated correctly by running the following command:

```
cat /opt/vmware/tunnel/proxy/conf/proxy-credentials.xml
```

VMware Tunnel Proxy Tools

The Proxy Tool is an application you can run to configure multiple outbound proxies for the VMware Tunnel. For more information, see [Use the Proxy Tool for PAC Files and Multiple Outbound Proxies \(Proxy Component\) on page 32](#).

Use the following commands to navigate the application:

- Use arrows, tab, shift+tab to navigate.
- Use Enter or spacebar to select/deselect a proxy.
- Use Alt+Enter to see details of the highlighted proxy.
- Use Ctrl+V to paste on text controls.
- Use F1 to invoke context-sensitive help.
- Use Esc to exit a window.

SSL Offloading the Proxy Component

Use SSL Offloading to ease the burden of encrypting and decrypting traffic from the VMware Tunnel server. Only the VMware Tunnel Proxy component supports SSL Offloading.

SSL Offloading and SSL re-encryption is not supported for the Per-App Tunnel component because this component uses SSL certificate pinning on the client and server side, creating an end-to-end encrypted tunnel. No SSL manipulation is supported for the Per-App Tunnel component because this component uses SSL certificate pinning between the client and server side. This creates an end-to-end encrypted tunnel that can only be decrypted by the server itself. All traffic to the Per-App Tunnel component on port 8443 must be allowed to pass through to the VMware Tunnel server.

The Tunnel Proxy encrypts traffic to HTTP endpoints using HTTP tunneling with an SSL certificate and sends that traffic over port 2020 as HTTPS. To enable SSL Off loading for this component, enable SSL Offloading in the VMware Tunnel console configuration and select SSL Offloading during installation on the Relay server. Enabling this setting ensures the relay expects all unencrypted traffic to the port you configured. The original host headers of the request must be forwarded to the tunnel server from wherever traffic is SSL off loaded.

You can perform SSL offloading with products such as F5's BIG-IP Local Traffic Manager (LTM), or Microsoft Forefront Unified Access Gateway, Threat Management Gateway (TMG) or Internet Security and Acceleration Server (ISA) solutions. Support is not exclusive to these solutions. VMware Tunnel Proxy is compatible with general SSL offloading solutions if the solution supports the HTTP CONNECT method. In addition, ensure that your SSL offloading solution is configured to forward original host headers to the VMware Tunnel relay server. The SSL Certificate configured in the Workspace ONE UEM console for the Tunnel Proxy must be imported to the SSL Termination Proxy.

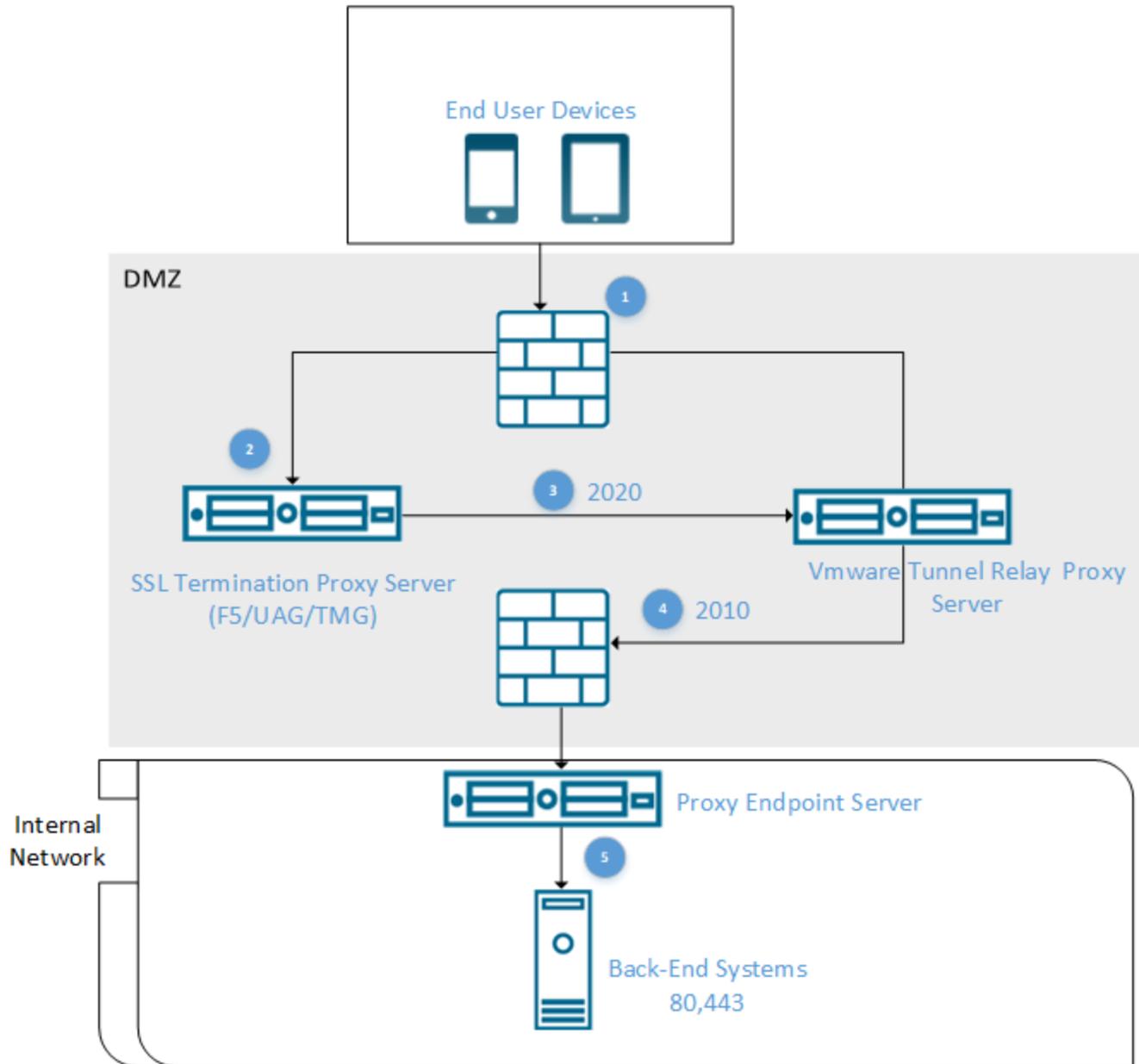
Ensure settings are configured properly in the UEM console, VMware Tunnel server, and your SSL Off loading solution in order to successfully implement SSL Offloading for the Tunnel Proxy.

SSL Offloading Requirements

- HTTP CONNECT method supported by SSL offloading solution
- SSL Offloading solution configured to forward original host headers
- VMware Tunnel Proxy SSL certificate installed on your SSL termination proxy.

If you are using a Workspace ONE UEM Certificate and not a public SSL certificate, then you can export the SSL certificate from the UEM console by navigating to **Settings > System > Enterprise Integration > VMware Tunnel > Configuration** then selecting the **Advanced** tab and selecting the Export Certificate button under **Authentication**.

The following diagram illustrates how SSL offloading affects traffic in a relay-endpoint configuration.



Note: SSL offloading for basic configuration has communication from the SSL termination proxy going directly to the VMware Tunnel endpoint.

SSL Offloading Traffic Flow

1. A device requests access to internal resources from AirWatch Software Development Kit enabled application, which can be either an HTTP or HTTPS endpoint.
 - Requests to HTTP and HTTPS endpoints are sent over port 2020 by default, which is the port you configure in the Workspace ONE UEM console during VMware Tunnel Proxy configuration.
2. The traffic reaches an SSL Termination Proxy (customers use their own SSL termination proxy), which must meet the

SSL Offloading requirements.

If you are using a Workspace ONE UEM Certificate and not a public SSL certificate, then you can export the SSL certificate from the UEM console by navigating to **Settings > System > Enterprise Integration > VMware Tunnel > Configuration** then selecting the **Advanced** tab and selecting the Export Certificate button under **Authentication**.

3. Requests to HTTP(S) endpoints have their SSL certificate offloaded and are sent to the relay server unencrypted over port 2020 by default. Traffic sent to the endpoint over port 2010 is encrypted with the UEM issued Tunnel certificate. SSL Offloading between the Relay and Endpoint is not supported for VMware Tunnel Proxy.
4. The traffic continues from the relay server to the endpoint server on port 2010 by default.
5. The endpoint server communicates with your back end systems to access the requested resources.

Chapter 6:

VMware Tunnel Deployment with Unified Access Gateway

VMware offers a hardened virtual appliance deployment known as Unified Access Gateway that hosts Workspace ONE services like Per-App Tunnel, and is the preferred method for deployment. Deploying Tunnel on Unified Access Gateway can be done from either vSphere or Hyper-V and can be automated using PowerShell.

For more information on Unified Access Gateway, see Deploying and Configuring Unified Access Gateway documentation on <https://docs.vmware.com/en/Unified-Access-Gateway/index.html>.

System Requirements for Deploying VMware Tunnel with Unified Access Gateway

To deploy VMware Tunnel with Unified Access Gateway, ensure that your system meets the following requirements:

Hypervisor Requirements

Unified Access Gateway that deploys the VMware Tunnel requires a hypervisor to deploy the virtual appliance. You must have a dedicated admin account with full privileges to deploy the OVF.

Supported Hypervisors

- VMware vSphere v6.0+ web client
- Microsoft Hyper-V on Windows Server 2012 R2 or Windows Server 2016

Software Requirements

Ensure that you have the most recent version of Unified Access Gateway. VMware Tunnel supports backwards compatibility between Unified Access Gateway and the Workspace ONE UEM console. The backward compatibility allows you to upgrade your VMware Tunnel server shortly after upgrading your Workspace ONE UEM console. To ensure parity between Workspace ONE UEM console and VMware Tunnel, consider planning an early upgrade.

Hardware Requirements

The OVF package for Unified Access Gateway automatically selects the virtual machine configuration that VMware Tunnel requires. Although you can change these settings, do not change the CPU, memory, or disk space to smaller values than the default OVF settings.

To change the default settings, power off the VM in vCenter. Right-click the VM and select **Edit Settings**.

The default configuration uses 4 GB of RAM and 2 CPUs. You must change the default configuration to meet your hardware requirements. To handle all the device loads and maintenance requirements, consider running a minimum of two VMware Tunnel servers.

Number of Devices	Up to 40,000	40,000-80,000	80,000-120,000	120,000-160,000
Number of Servers	2	3	4	5
CPU Cores	4 CPU Cores*	4 CPU Cores each	4 CPU Cores each	4 CPU Cores each
RAM (GB)	8	8	8	8
Hard Disk Space (GB)	10 GB for distro (Linux only) 400 MB for installer ~10 GB for log file space**			
*It is possible to deploy only a single VMware Tunnel appliance as part of a smaller deployment. However, consider deploying at least two load-balanced servers with four CPU Cores each regardless of the number of devices for uptime and performance purposes.				
**10 GB for a typical deployment. Scale the log file size based on your log use and requirements for storing the logs.				

Network Requirements for VMware Tunnel

For configuring the ports listed below, all the traffic is uni-directional (outbound) from the source component to the destination component.

Source Component	Destination Component	Protocol	Port	Verification	Note
Devices (from Internet and Wi-Fi)	VMware Tunnel Proxy	HTTPS	2020*	After installation, run the following command to validate: <pre>netstat -tlnp grep [Port]</pre>	1
Devices (from Internet and Wi-Fi)	VMware Tunnel Per-App Tunnel	TCP	8443*	After installation, run the following command to validate: <pre>netstat -tlnp grep [Port]</pre>	1
Admin UI	Unified Access Gateway	TCP	9443		1

Source Component	Destination Component	Protocol	Port	Verification	Note
VMware Tunnel Basic Endpoint Configuration					
VMware Tunnel	AirWatch Cloud Messaging Server**	HTTPS	SaaS: 443 On-Prem: 2001*	<pre>curl -Iv https://<AWCM URL>:<port>/awcm/status</pre> The expected response is HTTP 200-OK.	2
VMware Tunnel	Workspace ONE UEM REST API Endpoint SaaS: https://asXXX.awmdm.com On-Prem: Most commonly your DS or Workspace ONE UEM console	HTTP or HTTPS	SaaS: 443 On-Prem: 80 or 443	<pre>curl -Iv https://<API URL>/api/mdm/ping</pre> The expected response is HTTP 401-unauthorized.	5
VMware Tunnel	Internal resources	HTTP, HTTPS, or TCP	80, 443, Any TCP	Confirm that the VMware Tunnel can access internal resources over the required port.	4
VMware Tunnel	Syslog Server	UDP	514*		
Workspace ONE UEM console	VMware Tunnel Proxy	HTTPS	2020	On-premises customers can test the connection using the following telnet command: <Tunnel Proxy URL> <Port>	6
VMware Tunnel Cascade Configuration					
VMware Tunnel Front-End	AirWatch Cloud Messaging Server**	TLS v1.2	SaaS: 443 On-Prem: 2001*	Verify by using <code>wgetto https://<AWCM URL>:<port>/awcm/status</code> and ensure that you receive HTTP 200 response.	2
VMware Tunnel Front-End	VMware Tunnel Back-End	TLS v1.2	8443*	Telnet from VMware Tunnel Front-End to the VMware Tunnel Back-End server on port.	3

Source Component	Destination Component	Protocol	Port	Verification	Note
VMware Tunnel Back-End	AirWatch Cloud Messaging Server**	TLS v1.2	SaaS: 443 On-Prem: 2001*	Verify by using <code>whet</code> to https://<AWCM URL>:<port>/awcm/status and ensure that you receive HTTP 200 response.	2
VMware Tunnel Back-End	Internal websites/web apps	TCP	80 or 443		4
VMware Tunnel Back-End	Internal resources	TCP	80, 443, Any TCP		4
VMware Tunnel Front-End and Back-End	Workspace ONE UEM REST API Endpoint SaaS: https://asXXX.awmdm.com On-Prem: Most commonly your DS or Workspace ONE UEM console	TLS v1.2	80 or 443	<pre>curl -Ivv https://<API URL>/api/mdm/ping</pre> The expected response is HTTP 401-unauthorized.	5
VMware Tunnel Relay-Endpoint Configuration					
VMware Tunnel Relay	AirWatch Cloud Messaging Server**	HTTP or HTTPS	SaaS: 443 On-Prem: 2001*	<pre>curl -Ivv https://<AWCM URL>:<port>/awcm/status.</pre> The expected response is HTTP 200-OK.	2

Source Component	Destination Component	Protocol	Port	Verification	Note
VMware Tunnel Endpoint and Relay	Workspace ONE UEM REST API Endpoint SaaS: https://asXXX.awmdm.com On-Prem: Most commonly your DS or Workspace ONE UEM console	HTTP or HTTPS	80 or 443	<pre>curl -Ivv https://<API URL>/api/mdm/ping</pre> <p>The expected response is HTTP 401-unauthorized.</p> <p>The VMware Tunnel Endpoint requires access to the REST API Endpoint only during the initial deployment.</p>	5
VMware Tunnel Relay	VMware Tunnel Endpoint	HTTPS	2010*	Telnet from VMware Tunnel Relay to the VMware Tunnel Endpoint server on port.	3
VMware Tunnel Endpoint	Internal resources	HTTP, HTTPS, or TCP	80, 443, Any TCP	Confirm that the VMware Tunnel can access internal resources over the required port.	4
VMware Tunnel	Syslog Server	UDP	514*		
Workspace ONE UEM console	VMware Tunnel Proxy	HTTPS	2020	On-premises customers can test the connection using the telnet command: <Tunnel Proxy URL> <Port>	6

Source Component	Destination Component	Protocol	Port	Verification	Note
<p>*This port can be changed if needed based on your environment's restrictions.</p> <p>**For SaaS customers who need to whitelist outbound communication, refer to the following Knowledge Base article that lists up-to-date IP ranges that Workspace ONE currently owns: VMware AirWatch IP ranges for SaaS data centers.</p> <p>Note Reference:</p> <ol style="list-style-type: none"> 1. Devices connect to the public DNS configured for VMware Tunnel over the specified port. If 443 is used, Per-App Tunnel component listens on port 8443. 2. For the VMware Tunnel to query the Workspace ONE UEM console for compliance and tracking purposes. 3. For VMware Tunnel Relay topologies to forward device requests to the internal VMware Tunnel endpoint only. 4. For applications using VMware Tunnel to access internal resources. 5. The VMware Tunnel must communicate with the API for initialization. Ensure that there is connectivity between the REST API and the VMware Tunnel server. Navigate to Groups & Settings > All Settings > System > Advanced > Site URLs to set the REST API server URL. This page is not available to SaaS customers. The REST API URL for SaaS customers is most commonly your Console or Devices Services server URL. 6. This is required for a successful "Test Connection" to the VMware Tunnel Proxy from the Workspace ONE UEM console. The requirement is optional and can be omitted without loss of functionality to devices. For SaaS customers, the Workspace ONE UEM console must already have inbound connectivity to the VMware Tunnel Proxy on port 2020 due to the inbound Internet requirement on port 2020. 					

Network Interface Connection Requirements

You can use one, two, or three network interfaces, and the VMware Tunnel virtual appliance requires a separate static IP address for each. Many DMZ implementations use separated networks to secure the different traffic types. Configure the virtual appliance according to the network design of the DMZ in which it is deployed. Consult your network admin for information regarding your network DMZ.

- One network interface is appropriate for POCs (proof of concept) or testing. With one NIC, external, internal, and management traffic is all on the same subnet.
- With two network interfaces, external traffic is on one subnet, and internal and management traffic are on another subnet.
- Using three network interfaces is the most secure option. With a third NIC, external, internal, and management traffic all has their own subnets.

Installing VMware Tunnel with Unified Access Gateway

After configuring your VMware Tunnel settings, deploy VMware Tunnel as an edge service on the VMware Unified Access Gateway appliance to simplify the installation process. VMware supports installation using either VMware vSphere and Unified Access Gateway Admin UI or PowerShell scripting.

Installing VMware Tunnel using VMware vSphere

The vSphere web client deployment method allows you to deploy the Unified Access Gateway through vSphere and then configure your custom settings in an admin UI. VMware Tunnel installs as a service on Unified Access Gateway on VMware vSphere or Microsoft Hyper-V. This deployment method simplifies configuration, installation, maintenance, and upgrades. After configuring VMware Tunnel in the UEM console, download and install the .ova file or .vhdx (hyper-v).

Installing VMware Tunnel using PowerShell script

The PowerShell script deployment method automates the settings based on the pre-configured script. The PowerShell script method calls the API server before running so you get a quick validation of the entered information before deploying the Unified Access Gateway. Consider using the PowerShell method for the best deployment experience.

Install VMware Tunnel using vSphere

After configuring the VMware Tunnel in the Workspace ONE UEM console and downloading the VMware Unified Access Gateway OVA file, use VMware vSphere to install the Unified Access Gateway onto your server. The Unified Access Gateway simplifies installation of the VMware Tunnel.

Important: VMware Tunnel Unified Access Gateway deployment does not support the VMware vSphere desktop client. You must use the VMware vSphere web client or the PowerShell deployment method.

Requirements

- Windows administrator privileges
- Dedicated vSphere Admin Account with full privileges to deploy OVF
- VMware-ClientIntegrationPlugin (available on my.vmware.com)
- Communication between the Windows machine used to deploy the OVA and your vSphere instance
- vSphere v6.0+
- vSphere ESX host with a vCenter Server is needed.

You must select the vSphere datastore and the network to use. You must associate a vSphere Network Protocol Profile with every referenced network name. This Network Protocol Profile specifies network settings such as IPv4 subnet mask, gateway etc. The deployment of Unified Access Gateway uses these values so ensure the values are correct.

- Determine the number of network interfaces and static IP addresses to configure for the Unified Access Gateway appliance.

Procedure

1. Log in to the vSphere Web client.
2. Navigate to VMs and Templates.
3. Select the folder where you want to deploy the Unified Access Gateway OVA file. Right-click the file and select **Deploy OVF Template**.
4. Select the OVA file on your local machine or enter the URL for the OVA file. Click **Next**.

5. Review the template details and select **Next**.
6. Enter a unique **Name** for the deployment then select the folder or data center to hold the OVA file and select **Next**.
7. Select the number of Network Interface Controllers (NICs) you want to associate with the appliance for your deployment configuration. Click **Next**.

For best results, consult your network admins. Using three NICs provides the most security.

For more information, see the Unified Access Gateway Documentation Center:

<https://docs.vmware.com/en/Unified-Access-Gateway/>.

8. On the Select a Resource screen, select a location to run the template.
9. Select the storage and disk format options:

Settings	Descriptions
Virtual Disk Format	For evaluation and testing, select the Thin Provision format. For production environments, select one of the Thick Provision formats
VM Storage Policy	The values in this text box are defined by your vSphere administrator.

When finished, select **Next**.

10. Configure the **Network Mapping** settings.

Enter the vSphere network names. A vSphere Network Protocol Profile must be associated with every referenced network name.

The network profiles determine the IP protocol, DNS servers, gateway, and IPv4 subnet mask. If these are values are empty, you must enter the values.

When finished, select **Next**.

11. Configure the **Properties** settings. These settings include the **Network Properties** and the **Password Options**.

- Customize the **Network Properties** as they relate to your VMware Tunnel network configuration.
- Customize the **Password Options**.
 - Configure the password for the root user of the VM.
 - Configure the password for the REST API access.
The REST API password is the password for the admin UI. You must follow the password requirements:
 - The password must be 8 characters long.
 - The password must contain at least one special character which includes: !@#*\$*()
 - The password must contain at least one lowercase character.
 - The password must contain at least one uppercase character.

Caution: You must follow the password requirements. If you do not properly follow the instructions, installation fails without explanation. There is no validation at the end of this deployment. If you mistakenly enter in the wrong password, there is no warning informing you of an incorrect password.

When finished, select **Next**.

12. Review the OVA settings and select the **Power on after deployment**.
13. Select **Finish** to deploy the Unified Access Gateway.

To complete the configuration of the VMware Tunnel, you must log into the Unified Access Gateway admin UI to customize your settings.

Install VMware Tunnel using PowerShell Script

As an alternative to using the vSphere client to deploy the VMware Tunnel OVA file, you can use a PowerShell script. The PowerShell method provides settings validation checks to prevent errors during deployment. PowerShell enables you to deploy multiple instances of VMware Tunnel quickly and easily. Use the same .ini template to run the script multiple times.

The PowerShell method requires adding your VMware Tunnel configuration settings to the .ini template and running the script. When the script runs, it prompts the user for necessary authentication to appliance root user, REST API (admin UI), Workspace ONE UEM administrator, optional outbound proxy password, and vCenter. Each password is then validated so you can easily troubleshoot why the deployment failed.

Configure the vSphere .INI Template

After configuring the VMware Tunnel in the Workspace ONE UEM console and downloading the OVA file, configure the vSphere template.ini file with your Unified Access Gateway settings. The PowerShell script uses the template to configure your Unified Access Gateway deployment.

 Watch a tutorial video explaining how to deploy the VMware Tunnel Unified Access Gateway using PowerShell: http://players.brightcove.net/1971571333001/default_default/index.html?videoId=5133660358001.

To configure the template.ini:

1. Download the Unified Access Gateway Using vSphere ZIP from Workspace ONE UEM Resources (<https://resources.air-watch.com/view/sbfsfykltpqfxhvg9tpty/en>).
2. Unzip the file and locate the template.ini file.
3. Right click the file and select **Open With**. Select notepad or your preferred file editor.
4. Configure the template.ini settings:

Settings	Descriptions
vSphere Settings	
name=<VIRTUAL_MACHINE_NAME>	Enter the Unified Access Gateway unique name. Example: name=TunnelAppliance

Settings	Descriptions
source=<OVA_FILE_PATH>	<p>Enter the full file path to the OVA file on your local machine.</p> <p>Example: source=C:\access-point.ova</p>
target=vi://<USERNAME>:PASSWORD@<VSPHEREDOMAIN>/<LOCATION/TO/PLACE/APPLIANCE/IN/VSPHERE>	<p>Enter the vCenter user name and address/hostname. Then enter the location to place the appliance in vSphere. Do not remove the PASSWORD. PASSWORD in upper case results in a password prompt during deployment so that passwords do not need to be specified in this INI file.</p> <p>Example: target=vi://admin@vmware.com:PASSWORD@vsphere.com /MyMachines/host/Development/Resources/MyResourcePool</p>

Settings	Descriptions
deploymentOption=<NUMBER_OF_NICS> dns=<DNS_IP> ip0=<NIC1_IP_ADDRESS> ip1=<NIC2_IP_ADDRESS> ip2=<NIC3_IP_ADDRESS>	<p>Enter the number of Network Interface Controllers you want to associate with the appliance for your deployment configuration. Your options are:</p> <ul style="list-style-type: none"> • onenic • twonic • threenic <p>Then enter the address for each NIC you are using. Delete the excess lines if you are not using all three.</p> <p>The different IP addresses entered change based on your NIC settings.</p> <ul style="list-style-type: none"> • If you use one NIC, then the IP address is used for all communications. • If you use two NICs, then ip0 is for external communications and ip1 is for internal communications. • If you use three NICs, then ip0 is for external communications. Ip1 is for the admin UI only and ip2 is for internal communications. <p>For best results, consult your network admins. Three NICs provide the most security.</p> <p>Example: deploymentOption=threenic</p> <p>For dns=, enter the DNS server address to configure the appliance resolv.conf file. If you use multiple DNS servers, enter the addresses separated by a space value. Do not use commas.</p>
ds=<DATA_STORE_NAME>	Enter the name of your vSphere datastore.
netInternet=<NIC1_IP_NETWORK_NAME> netManagementNetwork=<NIC2_IP_NETWORK_NAME> netBackendNetwork=<NIC3_IP_NETWORK_NAME>	Enter the vSphere network names. A vSphere Network Protocol Profile must be associated with every referenced network name. This specifies network settings such as IPv4 subnet mask, gateway etc.
honorCipherOrder=<true_or_false>	Enter true to force the TLS cipher order to be the order specified by the server.
VMware Tunnel Settings	
tunnelGatewayEnabled=<true_or_false>	Enter true if you are using the VMware Tunnel Per-App Tunnel component. Example: tunnelGatewayEnabled=true

Settings	Descriptions
tunnelProxyEnabled=<true_or_false>	Enter true if you are using the VMware Tunnel Proxy component. Example: tunnelProxyEnabled=true
apiServerUrl=<API_SERVER_URL>	Enter the API server URL.
apiServerUsername=<API_SERVER_USERNAME>	Enter the user name of an Workspace ONE UEM console admin user account. This user is an admin user with API permissions. Consider using an account with Console Administrator privileges.
organizationGroupCode=<ORGANIZATION_GROUP_CODE>	Enter the Organization Group ID the VMware Tunnel is configured for.
airwatchServerHostname= <HOSTNAME>	Enter the hostname or IP address for the Unified Access Gateway. Ensure that this field matches what is entered in the Workspace ONE UEM console to prevent installation issues.
outboundProxyPort=<OUTBOUND_PROXY_PORT>	Enter the outbound proxy port if you use an outbound proxy for the initial setup API call or for tunnel traffic. This field is commented out by default.
outboundProxyHost=<OUTBOUND_PROXY_HOST>	Enter the outbound proxy host if you use an outbound proxy for the initial setup API call or for tunnel traffic. This field is commented out by default.
airwatchOutboundProxy=<true or false>	Enter true if you want to route tunnel traffic through an outbound proxy for the initial setup API call or for tunnel traffic. This field is commented out by default.
ntlmAuthentication=<true or false>	Enter true if you use NTLM authentication for the initial setup API call or for tunnel traffic. This field is commented out by default.
hostEntry1=<HOSTNAME>	Enter additional host entries for the appliance. You can add multiple host entries. Increase the number for each entry. For example hostEntry2, hostEntry3, and so on. This field is commented out by default.
trustedCert1=<CERT_FILE_PATH>	Enter the file path for the trusted certificates. You can add multiple trusted certificates. Increase the for each entry. For example, trustedCert2, trustedCert3, and so on. This field is commented out by default.

5. Save the file in the same folder as the PowerShell script and run the PowerShell script.

Configure the Hyper-V .INI Template

After configuring the VMware Tunnel in the Workspace ONE UEM console, download and configure the Hyper-V template.ini file with your Unified Access Gateway settings. The PowerShell script uses the template to configure your Unified Access Gateway deployment.

 Watch a tutorial video explaining how to deploy the VMware Tunnel Unified Access Gateway using PowerShell: [VMware Tunnel Powershell deployment](#).

To configure the template.ini:

1. Download the Unified Access Gateway Using Hyper-V ZIP from Workspace ONE UEM Resources [VMware Tunnel on Unified Access Gateway v3.3 \(Using HyperV\)](#).
2. Unzip the file and locate the template.ini file.
3. Right click the file and select **Open With**. Select notepad or your preferred file editor.
4. Configure the template.ini settings:

Settings	Descriptions
Hyper-V Settings	
name=<VIRTUAL_MACHINE_NAME>	Enter the Unified Access Gateway unique name. This name must be different every time you deploy the Unified Access Gateway. Example: name=TunnelAppliance
source=<OVA_FILE_PATH>	Enter the full file path to the OVA file on your local machine. Example: source=C:\access-point.ova

Settings	Descriptions
deploymentOption=<NUMBER_OF_NICS> dns=<DNS_IP> ip0=<NIC1_IP_ADDRESS> ip1=<NIC2_IP_ADDRESS> ip2=<NIC3_IP_ADDRESS>	<p>Enter the number of Network Interface Controllers you want to associate with the appliance for your deployment configuration. Your options are:</p> <ul style="list-style-type: none"> • onenic • twonic • threenic <p>Then enter the address for each NIC you are using. Delete the excess lines if you are not using all three.</p> <p>The different IP addresses entered change based on your NIC settings.</p> <ul style="list-style-type: none"> • If you use one NIC, then the IP address is used for all communications. • If you use two NICs, then ip0 is for external communications and ip1 is for internal communications. • If you use three NICs, then ip0 is for external communications. Ip1 is for the admin UI only and ip2 is for internal communications. <p>For best results, consult your network admins. Three NICs provide the most security.</p> <p>Example: deploymentOption=threenic</p> <p>For dns=, enter the DNS server address to configure the appliance resolv.conf file. If you use multiple DNS servers, enter the addresses separated by a space value. Do not use commas.</p>
ds=<DATA_STORE_NAME>	Enter the name of your Hyper-V datastore.
netInternet=<NIC1_IP_NETWORK_NAME> netManagementNetwork=<NIC2_IP_NETWORK_NAME> netBackendNetwork=<NIC3_IP_NETWORK_NAME>	<p>Enter the Hyper-V network names. A Hyper-V Network Protocol Profile must be associated with every referenced network name. This specifies network settings such as IPv4 subnet mask, gateway etc.</p>
honorCipherOrder=<true_or_false>	Enter true to force the TLS cipher order to be the order specified by the server.
VMware Tunnel Settings	
tunnelGatewayEnabled=<true_or_false>	<p>Enter true if you are using the VMware Tunnel Per-App Tunnel component.</p> <p>Example: tunnelGatewayEnabled=true</p>

Settings	Descriptions
tunnelProxyEnabled=<true_or_false>	Enter true if you are using the VMware Tunnel Proxy component. Example: tunnelProxyEnabled=true
apiServerUrl=<API_SERVER_URL>	Enter the API server URL.
apiServerUsername=<API_SERVER_USERNAME>	Enter the user name of an Workspace ONE UEM console admin user account. This user is an admin user with API permissions. Consider using an account with Console Administrator privileges.
organizationGroupCode=<ORGANIZATION_GROUP_CODE>	Enter the Organization Group ID the VMware Tunnel is configured for.
airwatchServerHostname= <HOSTNAME>	Enter the hostname or IP address for the Unified Access Gateway. Ensure that this field matches what is entered in the Workspace ONE UEM console to prevent installation issues.
outboundProxyPort=<OUTBOUND_PROXY_PORT>	Enter the outbound proxy port if you use an outbound proxy for the initial setup API call or for tunnel traffic. This field is commented out by default.
outboundProxyHost=<OUTBOUND_PROXY_HOST>	Enter the outbound proxy host if you use an outbound proxy for the initial setup API call or for tunnel traffic. This field is commented out by default.
airwatchOutboundProxy=<true or false>	Enter true if you want to route tunnel traffic through an outbound proxy for the initial setup API call or for tunnel traffic. This field is commented out by default.
ntlmAuthentication=<true or false>	Enter true if you use NTLM authentication for the initial setup API call or for tunnel traffic. This field is commented out by default.
hostEntry1=<HOSTNAME>	Enter additional host entries for the appliance. You can add multiple host entries. Increase the number for each entry. For example hostEntry2, hostEntry3, and so on. This field is commented out by default.
trustedCert1=<CERT_FILE_PATH>	Enter the file path for the trusted certificates. You can add multiple trusted certificates. Increase the for each entry. For example, trustedCert2, trustedCert3, and so on. This field is commented out by default.

5. Save the file in the same folder as the PowerShell script and run the PowerShell script.

Run the VMware Tunnel PowerShell Script

After configuring the .ini template file, run the PowerShell script to configure the OVA and deploy VMware Tunnel. The PowerShell script provides validation checks that are not available when deploying the OVA using vSphere.

Before you can run the PowerShell script, you must configure the INI file to pass the VMware Tunnel configuration to the OVA file.

Prerequisites

- Windows administrator privileges
- PowerShell 4
 - The PowerShell script runs on Windows 8.1 or later machines or Windows Server 2008 R2 or later.
 - The machine can also be a vCenter Server running on Windows or a separate Windows machine.
- VMware OVF Tool 4.1 (available on my.vmware.com)
- VMware-ClientIntegrationPlugin (available on my.vmware.com)
- Configured .ini template file to pass the configuration values to the appliance (part of the OVA download package available on Workspace ONE UEM Resources at <https://resources.air-watch.com/view/sbfsfykltpqfxhvg9tpy/en>)
- PowerShell script to configure the appliance (part of the OVA download package available on Workspace ONE UEM Resources at <https://resources.air-watch.com/view/sbfsfykltpqfxhvg9tpy/en>)
- Communication between the Windows machine used to deploy the OVA and your vSphere instance

Supported Hypervisors

- vSphere v5, 5.1, 5.5, or 6
 - vSphere ESX host with a vCenter Server is needed.
 - You must select the vSphere datastore and the network to use. You must associate a vSphere Network Protocol Profile with every referenced network name. This Network Protocol Profile specifies network settings such as IPv4 subnet mask, gateway etc. The deployment of Unified Access Gateway uses these values so make sure the values are correct.
- Microsoft Hyper-V
 - Windows Server 2012 R2 or Windows Server 2016

Procedure

1. Open PowerShell as an administrator.
2. Navigate to the folder containing your PowerShell script and modified .ini template.
3. Enter the following command:

```
.\apdeploy.ps1 <Ini file name>
```

Example:

```
.\apdeploy.ps1 AWTunnel.ini
```

4. Enter the password for each prompt:
 - Appliance Password (for the root user)
 - REST API (admin UI) password
 - API server password
 - (Optional) Outbound proxy if using a proxy with authentication.
 - If you are using vSphere, password for the vSphere User that can deploy VMs

After entering each password, PowerShell validates the entered password.

Once all passwords are entered, the Unified Access Gateway uploads to the hypervisor and the machine configures itself and installs. You must wait for the script to finish for the network to initialize. Progress can be tracked by viewing the machine from vSphere or Hyper-V.

Running the PowerShell with the values matching an existing instance in vSphere destroys the existing appliance and deploys a new instance instead. You cannot run the same INI template for Hyper-V. The Unified Access Gateway name must be different each time you deploy through PowerShell.

After a successful deployment, the Workspace ONE UEM Appliance Agent starts immediately and the monitoring services for VMware Tunnel start after 60 seconds.

Configure VMware Tunnel Settings in the Unified Access Gateway UI

After deploying the VMware Tunnel on the VMware Unified Access Gateway, you must configure the custom VMware Tunnel settings to meet your organizational needs. Configure these settings in the Unified Access Gateway admin UI hosted on your Unified Access Gateway.

To configure the VMware Tunnel settings:

1. Navigate to the URL of your Unified Access Gateway admin UI. The url uses this format: `https://[IP ADDRESS]:9443/admin/`.
2. Enter "admin" as the username.
3. Enter your admin UI password. Select **Login**.
4. Select **Configure Manually**.
5. Next to **Edge Service Settings**, select **Show**.
6. Next to **VMware Tunnel Settings**, select the settings icon () to configure your VMware Tunnel deployment.
7. Customize **VMware Tunnel Settings**:

Settings	Descriptions
Enable VMware Tunnel Settings	Set to Yes to use the configured VMware Tunnel settings. After configuration, setting this option to No does not disable the VMware Tunnel.

Settings	Descriptions
API Server URL	Enter the URL to your Workspace ONE UEM API server. The appliance contacts the Workspace ONE UEM API server to fetch your VMware Tunnel configuration. For example, https://asXXX.example.com.
API Server Username	Enter the user name of an Workspace ONE UEM console admin user account. You must have Console Administrator privileges at a minimum.
API Server Password	Enter the password of an Workspace ONE UEM console admin user account. You must have Console Administrator privileges at a minimum.
Organization Group ID	Enter the Group ID for the organization group the VMware Tunnel is configured.
Tunnel Server Hostname	Enter the hostname for your VMware Tunnel configuration. The hostname must match the hostname entered in the VMware Tunnel configuration wizard. The Unified Access Gateway configures the instance as a relay server or an endpoint server based on the hostname. Ensure that you properly enter the hostname to avoid any issues in deployment. This is the Tunnel server hostname.

8. (Optional) Select the **More** drop-down menu to configure additional settings including Workspace ONE UEM Outbound Proxy Settings if you use an outbound proxy to make the initial call to the API server:

Settings	Description
Outbound Proxy Host	Enter the outbound proxy hostname.
Outbound Proxy Port	Enter the outbound proxy port.
Outbound Proxy User	Enter the user name if your proxy requires authentication.
Outbound Proxy Password	Enter the password for your outbound proxy if your proxy requires authentication.
NTLM Authentication	Enable if your proxy requires NTLM authentication.
Use for VMware Tunnel Proxy	Enable to use these proxy settings as the outbound proxy for your VMware Tunnel deployment.
Host Entries	Enter the host entries for the server. You can enter multiple host entries separated by commas. They must follow this format: IP address hostname hostname alias (optional). For example, 10.192.168.1 example1.com, 10.192.167.2 example2.com. Use this option if your DNS is not publicly available or accessible from the DMZ.
Trusted Certificates	Select Select to upload a PEM certificate to add to the trusted store. Select the plus icon to upload additional certificates. This feature only supports PEM certificates.

9. The Support Settings screen on this page allows you to download the **Log Archive** and export your custom settings using the **Export Access Point Settings** option.

To finish, select **Save**. The Workspace ONE UEM Appliance Agent starts immediately and the monitoring services for VMware Tunnel start after 60 seconds.

Upgrade VMware Tunnel deployed with Unified Access Gateway

VMware Tunnel is backwards compatible with updated versions of the Workspace ONE UEM console. Upgrade the VMware Tunnel product whenever you perform any major version upgrades.

Upgrade Using vSphere

1. Access the Unified Access Gateway admin UI from a browser.
2. Select **Configure Manually**.
3. Scroll down to the bottom and select **Export Unified Access Gateway Settings**.
4. Download the new OVA package from Workspace ONE UEM Resources : [Download Unified Access Gateway](#).
5. Deploy the new OVA in place of the existing OVA. Follow the steps you used before. See [Install VMware Tunnel using vSphere on page 43](#) for more information.
6. Instead of manually configuring the settings, select **Import Settings**.
7. Browse for the downloaded export JSON file.
8. Select **Import**.

The Unified Access Gateway appliance supports a Zero Downtime Upgrade process. For more information, see the [Unified Access Gateway Documentation](#).

Upgrade Using PowerShell Script

1. Download the new OVA package from Workspace ONE UEM Resources: [Download Unified Access Gateway](#).
2. Use the same .ini template from your previous deployment with the PowerShell script.
3. Follow the steps you use before. See [Run the VMware Tunnel PowerShell Script on page 51](#) for more information.

Chapter 7:

VMware Tunnel Deployment on a Linux Server

For customers who do not want to use the Unified Access Gateway deployment, Workspace ONE UEM offers the Linux installer so you can configure, download, and install VMware Tunnel onto a server. The Linux installer has different prerequisites than the Unified Access Gateway method. To run the Linux installer, you must meet specific hardware, software, and general requirements before you can begin installation. It is considered to be a best practice to use the Unified Access Gateway method as it simplifies the requirements and installation process.

Note: For information on installing the legacy VMware Tunnel Windows server, see the [VMware Tunnel for Windows Installation Guide](#).

System Requirements for Deploying VMware Tunnel on a Linux Server

To deploy VMware Tunnel for Linux, ensure that your system meets the requirements. Use the following requirements as a basis for creating your VMware Tunnel server.

Hardware Requirements for VMware Tunnel

Ensure your VMware Tunnel server meets all the following hardware requirements.

- VM or Physical Server (64-bit)
- Hardware Sizing

Number of Devices	Up to 5,000	5,000 to 10,000	10,000 to 40,000	40,000 to 100,000
CPU Cores	1 server with 2 CPU Cores*	2 load-balanced servers with 2 CPU Cores each	2 load-balanced servers with 4 CPU Cores each	4 load-balanced servers with 4 CPU Cores each
RAM (GB)	4	4 each	8 each	16 each

Number of Devices	Up to 5,000	5,000 to 10,000	10,000 to 40,000	40,000 to 100,000
Hard Disk Space (GB)	10 GB for distro (Linux only) 400 MB for installer ~10 GB for log file space**			

*It is possible to deploy only a single VMware Tunnel server as part of a smaller deployment. However, consider deploying at least 2 load-balanced servers with 2 CPU Cores each regardless of number of devices for uptime and performance purposes.

**About 10 GB is for a typical deployment. Log file size should be scaled based on your log usage and requirements for storing logs.

Software Requirements for VMware Tunnel

Ensure your VMware Tunnel server meets all the following software requirements.

Requirement	Notes
Red Hat Enterprise Linux 6 and Red Hat Enterprise Linux 7	(Recommended UI-less)
Pre-Installation Package	The VMware Tunnel Linux installer automatically downloads required packages when it is connected to the Internet. If your server is offline or has restricted outbound access, then you must run the following commands on your VMware Tunnel server before you install. Openssl: <code>sudo yum -y install openssl</code> Haveged: <code>sudo yum -y install haveged*</code> Nscd: <code>sudo yum -y install nscd</code> Json-c: <code>sudo yum -y install json-c</code> libxml2: <code>sudo yum -y install libxml2</code> log4cpp: <code>sudo yum -y install log4cpp*</code> protobuf: <code>sudo yum -y install protobuf*</code>
Internally registered DNS record	(Optional): For a basic endpoint deployment, register the internal DNS record Relay-endpoint: Register the internal DNS entry for the endpoint server.
Externally registered DNS record	Basic endpoint: Register the public DNS record for the basic tunnel server. Relay-endpoint: Register the public DNS record for the relay server.

Requirement	Notes
(Optional) SSL Certificate from a trusted third party	<p>Workspace ONE UEM certificates are automatically generated by default as part of your Tunnel configuration.</p> <p>Alternatively, you can upload the full chain of the public SSL certificate to the Workspace ONE UEM console during configuration.</p> <p>Ensure that the SSL certificate is trusted by all device types being used. (that is, not all Comodo certificates are natively trusted by Android).</p> <p>SAN certificates are not supported.</p> <p>Ensure that the subject of the certificate is the public DNS of your Tunnel server or is a valid wildcard certificate for the corresponding domain.</p> <p>If your SSL certificate expires, then you must reupload the renewed SSL certificate and redownload and rerun the installer.</p>
IPv6 enabled locally	IPv6 must be enabled locally on the Tunnel server hosting Per-App Tunnel. Workspace ONE UEM requires it to be enabled for the Per-App Tunnel service to run successfully.

You must have the most recent version of the VMware Tunnel installer. The VMware Tunnel supports backwards compatibility between the installer and the UEM console. This backwards compatibility provides a small window to allow you to upgrade your VMware Tunnel server shortly after upgrading your UEM console. Consider upgrading as soon as possible to bring parity between the UEM console and the VMware Tunnel.

Network and Security Requirements for VMware Tunnel

For configuring the ports listed below, all the traffic is uni-directional (outbound) from the source component to the destination component.

Source Component	Destination Component	Protocol	Port	Verification	Note
Devices (from Internet and Wi-Fi)	VMware Tunnel Proxy	HTTPS	2020*	After installation, run the following command to validate: netstat -tlnp https://<VMware_Tunnel_Host>:<port>	1
Devices (from Internet and Wi-Fi)	VMware Tunnel Per-App Tunnel	TCP	8443* (for Per-App Tunnel)		1
VMware Tunnel – Basic Endpoint Configuration					
VMware Tunnel	AirWatch Cloud Messaging Server**	HTTPS	SaaS: 443 On-Prem: 2001*	Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response.	2

Source Component	Destination Component	Protocol	Port	Verification	Note
VMware Tunnel	Internal Web sites / Web apps	HTTP or HTTPS	80 or 443		4
VMware Tunnel	Internal resources	HTTP, HTTPS, or TCP	80, 443, Any TCP		4
VMware Tunnel	Workspace ONE UEM REST API Endpoint SaaS: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com On-Prem: Most commonly your DS or Console server	HTTP or HTTPS	SaaS: 443 On-Prem: 80 or 443	<pre>curl -Ivv https://<API URL>/api/mdm/ping</pre> The expected response is HTTP 401 – unauthorized.	5
Console Server	VMware Tunnel Proxy	HTTPS	On-Prem: 2020	Verify after installation using telnet command from the console server to the Tunnel Proxy on port 2020 (On-Premesis only).	6
VMware Tunnel — Cascade Configuration					
VMware Tunnel Front-End	AirWatch Cloud Messaging Server**	TLS v1.2	SaaS: 443 On-Prem: 2001*	Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response.	2
VMware Tunnel Front-End	VMware Tunnel Back-End	TLS v1.2	8443*	Telnet from VMware Tunnel Front-End to the VMware Tunnel Back-End server on port	3
VMware Tunnel Back-End	AirWatch Cloud Messaging Server**	TLS v1.2	SaaS: 443 On-Prem: 2001*	Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response.	2
VMware Tunnel Back-End	Internal Web sites / Web apps	TCP	80 or 443		4
VMware Tunnel Back-End	Internal resources	TCP	80, 443, Any TCP		4

Source Component	Destination Component	Protocol	Port	Verification	Note
VMware Tunnel Front-End and Back-End	Workspace ONE UEM REST API Endpoint SaaS: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com On-Prem: Most commonly your DS or Console server	TLS v1.2	80 or 443	<pre>curl -Ivv https://<API URL>/api/mdm/ping</pre> The expected response is HTTP 401 – unauthorized.	5
VMware Tunnel – Relay Endpoint Configuration					
VMware Tunnel Relay	AirWatch Cloud Messaging Server**	HTTP or HTTPS	SaaS: 443 On-Prem: 2001*	Verify by using wget to https://<AWCM URL>:<port>/awcm/status and ensuring you receive an HTTP 200 response.	2
VMware Tunnel Relay	VMware Tunnel Endpoint	HTTPS	2010*	Telnet from VMware Tunnel Relay to the VMware Tunnel Endpoint server on port	3
VMware Tunnel Endpoint	Internal Web sites / Web apps	HTTP or HTTPS	80 or 443		4
VMware Tunnel Endpoint	Internal resources	HTTP, HTTPS, or TCP	80, 443, Any TCP		4
VMware Tunnel Endpoint and Relay	Workspace ONE UEM REST API Endpoint SaaS: https://asXXX.awmdm.com or https://asXXX.airwatchportals.com On-Prem: Most commonly your DS or Console server	HTTP or HTTPS	80 or 443	<pre>curl -Ivv https://<API URL>/api/mdm/ping</pre> The expected response is HTTP 401 – unauthorized.	5
Console Server	VMware Tunnel Proxy	HTTPS	On-Prem: 2020	Verify after installation using telnet command from the console server to the Tunnel Proxy on port 2020 (On-Premesis only).	6

*This port can be changed if needed based on your environment's restrictions.

For SaaS customers who need to whitelist outbound communication, refer to the following Knowledge Base article that lists up-to-date IP ranges that Workspace ONE currently owns: [VMware AirWatch IP ranges for SaaS data centers](#)

1. For devices attempting to access internal resources.
2. For the VMware Tunnel to query the UEM console for compliance and tracking purposes.
3. For VMware Tunnel Relay topologies to forward device requests to the internal VMware Tunnel endpoint only.
4. For applications using VMware Tunnel to access internal resources.
5. The VMware Tunnel must to communicate with the API for initialization. Ensure that there is connectivity between the REST API and the VMware Tunnel server.
6. This is required for a successful "Test Connection" to the VMware Tunnel Proxy from the UEM console. This requirement is optional and can be omitted without loss of functionality to devices.

Single-Tier VMware Tunnel Installation

After ensuring that your server meets all the proper requirements, configuring VMware Tunnel settings in the Workspace ONE UEM console, and downloading the installer to your Linux server, you can run the installer to enable the service.

Prerequisites

- Download the installer onto the server. The link in the Workspace ONE UEM console directs you to Workspace ONE UEM Resources to download the installer.
- Download the config.xml file from the Workspace ONE UEM console onto the server.

Procedure

Perform the following steps on your single VMware Tunnel server:

1. Create a dedicated install directory for the installer on the back-end server (for example, /tmp/Install/) and copy the BIN file to this location. You can use file transfer software such as FileZilla or WinSCP to perform the action.
If this server is also being used for Content Gateway, the dedicated install directory for Proxy must be different than the install directory for Content Gateway.
2. Once on the Linux server, navigate to the folder you copied the file to and then run the BIN file by using the following command:

```
$ sudo ./VMwareTunnel.bin
```

If you are installing for the first time, the following screen displays:

```

Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

=====
AirWatch Tunnel                               (created with InstallAnywhere)
=====

Preparing CONSOLE Mode Installation...

=====
Introduction
=====

InstallAnywhere will guide you through the installation of AirWatch Tunnel.
It is strongly recommended that you quit all programs before continuing with
this installation.

Respond to each prompt to proceed to the next step in the installation.  If you
want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:

```

Press **Enter**.

3. Read and accept the licensing agreement by entering 'y'.
4. After accepting the licensing agreement, you must choose your installation method.

```

=====
Tunnel Installation Setup
=====

  1- Provide API Server Information
  2- Import Config.xml file

Select the installation type: █

```

- Option 1: Provide API Server Information
 - a. Enter the following information. After entering each value, the system dialog asks you to confirm the entry.
 - VMware API URL
 - Organization Group Code
 - Console Server Username
 - Console Server Password
 - b. Enter the hostname of the Tunnel server.
 - c. The installer chooses the components to install based on the Workspace ONE UEM console configuration.

Press **Enter**.

Continue to Step 5.

- Option 2: Import Config.xml file
 - a. Select the components you want to install.
 - b. Enter the file path of the configuration file.
 - c. Enter the VMware Tunnel certificate password as entered in the Workspace ONE UEM console.
 Continue to Step 5.

5. Enter Y to grant the installer firewall permissions needed for VMware Tunnel.

Note: The ports you see may differ from the ones shown because the installer shows the values you set during VMware Tunnel configuration.

6. Review and verify the summary information.

```
=====
Pre-Installation Summary
-----

Please Review the Following Before Continuing:

Product Name:
  VMware Tunnel

Install Folder:
  /opt/vmware/tunnel

Product Features:
  VMware Per-App Tunnel,
  VMware Proxy

Disk Space Information (for Installation Target):
  Required: 111.9 MegaBytes
  Available: 31,787.58 MegaBytes

PRESS <ENTER> TO CONTINUE: █
```

When the installer finishes, press **Enter** to exit the installer.

The product begins installation. If there were any errors, the installer displays an error message with details and logs the error in the installation log file. The log file is saved in the directory that you installed the VMware Tunnel in.

Multi-Tier VMware Tunnel Installation

During a Linux installation, you specify whether you are installing proxy, Per-App Tunnel, or both. If you install both, they share a front-end and back-end servers. If you are installing Per-App Tunnel as part of a relay-endpoint configuration, then the Linux versions of the Proxy component must be installed as well. You cannot install the VMware Tunnel Proxy for Windows version of proxy and the VMware Tunnel Per-App Tunnel component in a relay-endpoint configuration.

Install the VMware Tunnel Front-End Server (Linux)

After ensuring that your servers meets all the proper requirements, configuring VMware Tunnel settings in the Workspace ONE UEM console, and downloading the installer to your Linux server, you can run the installer to enable the

service.

Note: If you are installing the Proxy component either alone or in combination with the Per-App Tunnel component, the installer refers to the front-end server as the relay server. Proxy uses the relay-endpoint mode for communication. The relay-endpoint deploys alongside the cascade mode services on the same server. Consider using just the Per-App Tunnel component for your VMware Tunnel solution as it has additional features and functionality that the Proxy component does not.

Prerequisites

- Download the installer and transfer to the server. The link in the Workspace ONE UEM console directs you to Workspace ONE UEM Resources to download the installer.
- If you are using the API method, the installer prompts for the necessary configuration information. You do not need to download the vpn_config.xml file.
- If you are using the configuration file method, download the vpn_config.xml (per-app config) file and config.xml (proxy config) file from the Workspace ONE UEM console and transfer to the server.

Procedure

Perform the following steps on the front-end server:

1. Create a dedicated install directory for the installer on the front-end server (for example, /tmp/Install/) and copy the BIN file to this location. You can use file transfer software such as FileZilla or WinSCP to perform the action.
2. Once on the Linux server, navigate to the folder you copied the file to and then run the BIN file by using the following command:

```
$ sudo ./VMwareTunnel.bin
```

If you are installing for the first time, the following screen displays:

```
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

=====
AirWatch Tunnel                               (created with InstallAnywhere)
=====

Preparing CONSOLE Mode Installation...

=====
Introduction
=====

InstallAnywhere will guide you through the installation of AirWatch Tunnel.

It is strongly recommended that you quit all programs before continuing with
this installation.

Respond to each prompt to proceed to the next step in the installation. If you
want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:
```

Press **Enter**.

3. Read and accept the licensing agreement by entering 'y'.
4. After accepting the licensing agreement, you must choose your installation method.

```
=====
Tunnel Installation Setup
-----

  1- Provide API Server Information
  2- Import Config.xml file

Select the installation type: █
```

- Option 1: Provide API Server Information
 - a. Enter the following information. After entering each value, the system dialog asks you to confirm the entry.
 - VMware API URL
 - Organization Group Code
 - Console Server Username
 - Console Server Password
 - b. Enter the hostname of the Tunnel server.
 - c. The installer chooses the components to install based on the Workspace ONE UEM console configuration.

```
=====
Feature Selection Summary
-----

Please Review the Following Before Continuing:

Product Name:
  VMware Tunnel

Product Features:
  VMware Per-App Tunnel,
  VMware Proxy

PRESS <ENTER> TO CONTINUE: █
```

Press **Enter**.

Continue to Step 5.

- Option 2:
 - a. Download and copy the Tunnel Proxy and Per-app VPN configuration files to a single directory on the server. Confirm that the Proxy and Per-app VPN configuration file names are not modified from their original config.xml and vpn_config.xml names, respectively. If they have been modified, rename the files to match these names when copied into the common directory on the Linux server. If you are installing one of the Tunnel services, copy the respective configuration file.

- b. Enter the directory path that contains both configuration files.
 - c. Enter the certificate password for both configuration files when prompted.
5. Enter the hostname of the Tunnel server. The hostname must match the hostname that is used to configure VMware Tunnel in Workspace UEM. For example, if your VMware Tunnel Front end server is configured to use tunnel.acme.com, enter the same address.
 6. Enter Y to grant the installer firewall permissions needed for VMware Tunnel.

Note: The ports you see may differ from the ones shown because the installer shows the values you set during VMware Tunnel configuration.

7. Review and verify the summary information.

```
=====
Pre-Installation Summary
-----

Please Review the Following Before Continuing:

Product Name:
  VMware Tunnel

Install Folder:
  /opt/vmware/tunnel

Product Features:
  VMware Per-App Tunnel,
  VMware Proxy

Disk Space Information (for Installation Target):
  Required: 111.9 MegaBytes
  Available: 31,787.58 MegaBytes

PRESS <ENTER> TO CONTINUE: █
```

When the installer finishes, press **Enter** to exit the installer.

The product begins installation. If there were any errors, the installer displays an error message with details and logs the error in the installation log file. The log file is saved in the directory that you installed the VMware Tunnel in.

To complete your installation, see [Install the VMware Tunnel Back-End Server \(Linux\) on page 66](#).

Install the VMware Tunnel Back-End Server (Linux)

In multi-tier configurations, you install the back-end server after installing the front-end server. If you have not already, perform the steps described in [Install the VMware Tunnel Front-End Server \(Linux\) on page 63](#).

Note: If you are installing the Proxy component either alone or in combination with the Per-App Tunnel component, the installer refers to the back-end server as the endpoint server. Proxy uses the relay-endpoint mode for communication. The relay-endpoint deploys alongside the cascade mode services on the same server. Consider using just the Per-App Tunnel component for your VMware Tunnel solution as it has additional features and functionality that the Proxy component does not.

Prerequisites

- Download the installer onto the server. The link in the Workspace ONE UEM console directs you to Workspace ONE UEM Resources to download the installer.
- Download the config.xml file from the Workspace ONE UEM console onto the server.

Procedure

Perform the following steps on the endpoint server:

1. Create a dedicated install directory for the installer on the back-end server (for example, /tmp/Install/) and copy the BIN file to this location. You can use file transfer software such as FileZilla or WinSCP to perform the action.
2. Once on the Linux server, navigate to the folder you copied the file to and then run the BIN file by using the following command:

```
$ sudo ./VMwareTunnel.bin
```

If you are installing for the first time, the following screen displays:

```
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

=====
AirWatch Tunnel                               (created with InstallAnywhere)
=====

Preparing CONSOLE Mode Installation...

=====
Introduction
=====

InstallAnywhere will guide you through the installation of AirWatch Tunnel.

It is strongly recommended that you quit all programs before continuing with
this installation.

Respond to each prompt to proceed to the next step in the installation. If you
want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:
```

Press **Enter**.

3. Read and accept the licensing agreement by entering 'y'.
4. After accepting the licensing agreement, you must choose your installation method.

```
=====
Tunnel Installation Setup
=====

1- Provide API Server Information
2- Import Config.xml file

Select the installation type: █
```

- Option 1: Provide API Server Information
 - a. Enter the following information. After entering each value, the system dialog asks you to confirm the entry.
 - VMware API URL
 - Organization Group Code
 - Console Server Username
 - Console Server Password
 - b. Enter the hostname of the Tunnel server.
 - c. The installer chooses the components to install based on the Workspace ONE UEM console configuration. Press **Enter**.
 - Option 2: Import Config.xml file
 - a. Download and copy the Tunnel Proxy and Per-app VPN configuration files to a single directory on the server. Confirm that the Proxy and Per-app VPN configuration file names are not modified from their original config.xml and vpn_config.xml names, respectively. If they have been modified, rename the files to match these names when copied into the common directory on the Linux server. If you are installing one of the Tunnel services, copy the respective configuration file.
 - b. Enter the directory path that contains both configuration files.
 - c. Enter the certificate password for both configuration files when prompted.
5. Enter the hostname of the Tunnel server. The hostname must match the hostname that is used to configure VMware Tunnel in Workspace UEM. For example, if your VMware Tunnel Back-End server is configured to use tunnel.acme.com, enter the same address.
 6. Enter **Y** or **N** for whether you want to use an outbound proxy as part of your VMware Tunnel configuration. This option only displays if you are installing the Proxy component.
 7. Enter **Y** to grant the installer firewall permissions needed for VMware Tunnel.

Note: The ports you see may differ from the ones shown because the installer shows the values you set during VMware Tunnel configuration.

8. Review and verify the summary information.

```

=====
Pre-Installation Summary
-----

Please Review the Following Before Continuing:

Product Name:
  VMware Tunnel

Install Folder:
  /opt/vmware/tunnel

Product Features:
  VMware Per-App Tunnel,
  VMware Proxy

Disk Space Information (for Installation Target):
  Required: 111.9 MegaBytes
  Available: 31,787.58 MegaBytes

PRESS <ENTER> TO CONTINUE: █

```

When the installer finishes, press **Enter** to exit the installer.

The product begins installation. If there were any errors, the installer displays an error message with details and logs the error in the installation log file. The log file is saved in the directory that you installed the VMware Tunnel in.

Upgrade VMware Tunnel Deployed on a Linux Server

VMware Tunnel is backwards compatible with updated versions of the Workspace ONE UEM console. Upgrade the VMware Tunnel product whenever you perform any major version upgrades.

To upgrade an existing VMware Tunnel, download the latest version of the installer from the UEM console. Load the installer onto one or more VMware Tunnel servers and run the installer following the same procedures outlined in the installation chapters of this documentation based on your deployment model. Any custom changes made to configuration files following the original installation will be overridden, and must be manually updated after the upgrade is complete.

Create a back-up of any custom configuration files that you might want to reference after the upgrade and create a snapshot of each VMware Tunnel server before the upgrade.

To upgrade VMware Tunnel:

1. Log in to the UEM console and navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel**.
2. Select the **General** tab and then select the **Download Linux Installer** hyperlink which redirects you to Workspace ONE UEM Resources to download the installer.
3. Create a directory for the Tunnel installer and copy the VMwareTunnel.bin file to this location.
4. Continue with the steps for [Install the VMware Tunnel Front-End Server \(Linux\) on page 63](#) or [Install the VMware Tunnel Back-End Server \(Linux\) on page 66](#).

The installer detects the existing VMware Tunnel instance running on the server and prompts you to confirm the upgrade.

Uninstalling VMware Tunnel

Perform the following steps on your VMware Tunnel servers to remove the component.

1. Navigate to the `/opt/vmware/tunnel/_tunnel_installation/` directory.

```
cd /opt/vmware/tunnel/_tunnel_installation/
```

2. Execute **Uninstall_Tunnel**.

```
sudo ./Uninstall_Tunnel
```

3. Review installer logs at `/opt/vmware/tunnel/_tunnel_installation/Logs`, if necessary.

Chapter 8:

VMware Tunnel Management

Consider configuring additional functionality to enhance your VMware Tunnel deployment. These features allow you more control over device access and networking support.

For instance the following additional functionalities allows you to maintain and manage your VMware Tunnel deployment:

- RSA authentication controls access to internal resources through two-factor authentication.
- Configure VMware Tunnel to rotate public SSL certificates to maintain the end-user service experience.
- Use VMware Browser to control how the end users access internal sites by configuring communication between the application and VMware Tunnel.

Deploying Per-App Tunnel to devices

After configuring and installing VMware Tunnel with the Per-App Tunnel component, the workflow to enable and use per app tunneling in Workspace ONE UEM includes:

1. Creating a VPN profile for your end-user devices. These profiles depend on your device platform.
If your platform uses user profiles and device profiles, such as Windows Desktop and Android, you must create user profiles.
2. After creating a VPN profile, push the profiles and the apps to the devices.
For iOS and Android platforms, you must enable the Use VPN check box on the Deployment tab of the Add Application page to use app tunneling.

Windows Desktop devices use the native Per-App VPN functionality. Add the apps to the VPN profile to enable Per-App Tunnel functionality.

An on-demand feature lets you configure apps to connect automatically using VMware Tunnel when launched. The connection remains active until a time-out period of receiving no traffic, then it is disconnected. When using VMware Tunnel, no IP address is assigned to the device, so you do not need to configure the network or assign a subnet to connected devices.

In addition, iOS apps can use the iOS DNS Service to send DNS queries through the VMware Tunnel server to the DNS server on a corporate network. This service allows applications such as Web browsers to use your corporate DNS server to look up the IP address of your internal Web servers.

Configure Per-App Tunnel Profile for iOS

Configure Per-App Tunnel for iOS to allow those devices to connect to internal sites you define through the VMware Tunnel. Using this functionality requires you to configure and install the Per-App Tunnel component as part of your VMware Tunnel installation.

Procedure

To configure a VPN profile for Per-App Tunnel:

1. Navigate to **Devices > Profiles > List View > Add** and select **iOS**.
2. Configure the profile's **General** settings. Consider setting the Deployment type for this profile to Auto so end-users receive it automatically.
3. Select the **VPN** payload from the list.
4. Enter a **Connection Name**, which is the name that displays on the user's device in the VMware Tunnel application, and select **VMware Tunnel** as the **Connection Type**.
The **Server** text box populates automatically with your VMware Tunnel component server URL.
5. Select **Enable VMware Tunnel** to always push the VMware Tunnel version of the profile to device. Do not use this option if you have devices in the assignment group that do not have the VMware Tunnel app but still use the legacy AirWatch Tunnel App.
6. Verify or select **AppProxy** as the **Provider Type**.
7. Select **Save & Publish**.

What to do next

Configure an internal or public app to use the profile when making connections to the domains you specified.

Configure Per-App Tunnel Profile for Android

Configure Per-App Tunnel for Android to allow those devices to connect to internal sites you define through the VMware Tunnel. Using this functionality requires you to configure and install the Per-App Tunnel component as part of your VMware Tunnel installation.

Note: If you are adding an internal application, Per-App VPN Profile tunneling currently supports only the Android (Legacy) devices. However, Android Work Profile and the Work Managed devices do not support Per-App VPN Profile tunneling for all the internal applications.

Procedure

To configure a VPN profile for Per-App Tunnel:

1. Navigate to **Devices > Profiles > List View > Add** and select **Android** or **Android for Work**. For a Samsung Knox deployment, select **Android** and then select **Container**.

2. Configure the profile's **General** settings.
3. Select the **VPN** payload from the list.
4. Enter a **Connection Name** and select **VMware Tunnel** as the **Connection Type**.
The **Server** text box populates automatically with your VMware Tunnel component server URL. If this component is not configured, you see a message and hyperlink to the system settings page where you can configure it.
5. Select **Save & Publish**.

What to do next

Configure an internal or public app to use the profile when making connections.

Configure Per-App Tunnel Profile for Windows

Configure Per-App Tunnel for Windows to allow those devices to connect to internal sites you define through the VMware Tunnel. Using this functionality requires you to configure and install the Per-App Tunnel component as part of your VMware Tunnel installation.

Procedure

To configure a VPN profile for Per-App Tunnel:

1. Navigate to **Devices > Profiles > List View > Add** and select **Windows**. Then select **Windows Desktop** and **User**.
2. Configure the profile's **General** settings.
3. Select the **VPN** payload from the list.
4. Enter a **Connection Name** and select **VMware Tunnel** as the **Connection Type**.
The **Server** text box populates automatically with your VMware Tunnel component server URL. If this component is not configured, you see a message and hyperlink to the system settings page where you can configure it.
5. Configure the **Per App VPN** rules.
6. Configure the relevant **Policies** settings:

Settings	Description
Always On	Enable to force the VPN connection to be always on.
VPN Lockdown	Enable to force the VPN to always be on, never disconnect, disable any network access if the VPN is not connected, and prevent other VPN profiles from connecting on the device. A VPN profile with VPN Lockdown enabled must be deleted before you push a new VPN profile to the device.
Trusted Network Detection	Enter, separated by commas, trusted network addresses. The VPN does not connect when a trusted network connection is detected

7. Select **Add New Domain** to add all domains you want resolved through the VMware Tunnel server.
8. Select **Save & Publish**.

Configure Per-App Tunnel Profile for macOS

Configure Per-App Tunnel for macOS to allow macOS devices to connect to internal sites you define through the VMware Tunnel. This functionality requires you to configure and install the Per-App Tunnel component as part of your VMware Tunnel installation.

Procedure

To configure a VPN profile for Per-App Tunnel:

1. Navigate to **Devices > Profiles > List View > Add** and select **macOS**. Then select **User**.
2. Configure the **General** settings.
3. Select the **VPN** payload from the list.
4. Enter a **Connection Name** and select **VMware Tunnel** as the **Connection Type**.

The **Server** text box populates automatically with your VMware Tunnel component server URL. If this component is not configured, you see a message and hyperlink to the system settings page where you can configure it.

5. Enable **App Mapping**
6. Add the **Bundle ID** for each application you want to use with Per-App Tunnel.

To find the Bundle ID for a macOS application, see [Extract macOS Bundle ID for Per-App Tunnel on page 74](#).

7. Select **Save & Publish**.

To configure the Safari domains, see [Configure Network Traffic Rules for the Per-App Tunnel Component on page 25](#).

Extract macOS Bundle ID for Per-App Tunnel

To use non-native Per-App Tunnel functionality on macOS devices, you must extract the app Bundle ID. Extract the Bundle ID before pushing the VPN profile to macOS devices.

Procedure

To extract the Bundle ID:

1. On a macOS device, find the file path for the app you want to flag for Per-App Tunnel.
For example: `/Applications/Google\ Chrome.app/`.
2. Open the terminal.
3. Run the following command to get the Application Bundle ID: `codesign -dv --entitlements - /Applications/Google\ Chrome.app/`
4. Review the output.

```
Executable=/Applications/Google Chrome.app/Contents/MacOS/Google Chrome
Identifier=com.google.Chrome Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20200 size=273 flags=0x800(restrict) hashes=3+3
location=embeddedSignature size=8949 Timestamp=Mar 20, 2018 at 2:23:20 AM
Info.plist entries=36 TeamIdentifier=EQHXZ8M8AV Sealed Resources version=2
rules=7 files=203 Internal requirements count=1 size=240
```

- Copy the Application Bundle ID from the output. The Bundle ID follows `identifier`. In the above example it is `com.google.Chrome`.
- Run the following command to get the Designated Requirement: `codesign -d -r- /Applications/Google\ Chrome.app/`
- Review the output.

```
Executable=/Applications/Google Chrome.app/Contents/MacOS/Google Chrome
designated => (identifier "com.google.Chrome" or identifier
"com.google.Chrome.beta" or identifier "com.google.Chrome.dev" or identifier
"com.google.Chrome.canary") and (certificate leaf =
H"85cee8254216185620ddc8851c7a9fc4dfe120ef" or certificate leaf =
H"c9a99324ca3fcb23dbcc36bd5fd4f9753305130a")
```

- Copy the Designated Requirement from the output. Designated Requirement is the entire string followed by `"designated =>"`.

In the above example, it is `(identifier "com.google.Chrome" or identifier "com.google.Chrome.beta" or identifier "com.google.Chrome.dev" or identifier "com.google.Chrome.canary") and (certificate leaf = H"85cee8254216185620ddc8851c7a9fc4dfe120ef" or certificate leaf = H"c9a99324ca3fcb23dbcc36bd5fd4f9753305130a")`

- To whitelist Chrome, enter the Application Bundle ID and Designated Requirement in the UEM console Tunnel profile.

For example, from the above sample output, enter the following:

Settings	Description
Application Bundle ID	<code>com.google.Chrome</code>
Designated Requirement	<code>(identifier "com.google.Chrome" or identifier "com.google.Chrome.beta" or identifier "com.google.Chrome.dev" or identifier "com.google.Chrome.canary") and (certificate leaf = H"85cee8254216185620ddc8851c7a9fc4dfe120ef" or certificate leaf = H"c9a99324ca3fcb23dbcc36bd5fd4f9753305130a")</code>

Configure Public Apps to Use Per App Profile

After you create a per app tunnel profile you can assign it to specific apps in the application configuration screen. This tells that application to use the defined VPN profile when establishing connections.

- Navigate to **Apps & Books > Applications > Native**.
- Select the **Public** tab.
- Select **Add Application** to add an app or **Edit** an existing app.
- On the Deployment tab, select **Use VPN** and then select the profile you created.
- Select **Save** and publish your changes.

For additional instructions on adding or editing apps, please see the **VMware Workspace ONE UEM Mobile Application Management Guide**.

This workflow only applies to Android and iOS devices.

Configure Internal Apps to Use Per App Profile

After you create a per app tunnel profile you can assign it to specific apps in the application configuration screen. This tells that application to use the defined VPN profile when establishing connections.

1. Navigate to **Apps & Books > Applications > Native**.
2. Select the **Internal** tab.
3. Select **Add Application** and add an app.
4. Select **Save & Assign** to move to the Assignment page.
5. Select **Add Assignment** and select **Per-App VPN Profile** in the **Advanced** section.
6. **Save & Publish** the app.

For additional instructions on adding or editing apps, please see the **VMware Workspace ONE UEM Mobile Application Management Guide**.

This workflow only applies to Android and iOS devices.

VMware Tunnel SSL Certificate Life Cycle Management

VMware Tunnel supports rotating your public SSL certificates with zero downtime for end users. Rotating your public SSL certificate and the profile grace period ensures that your end users do not experience a service interruption.

To rotate your public SSL certificates, you must upload a new certificate to the Workspace ONE UEM console. Adding a new certificate enables you to prepare new VPN profiles configured for VMware Tunnel before rotating the certificate on the server.

To prepare the end-user devices for rotation, you must add a new version of the VPN profiles configured for VMware Tunnel. The new profile version contains the new public SSL certificate. Before rotating the server certificate, you must push the new profile version to devices.

When the certificate is close to expiring or is compromised, the UEM console notifies the user and you can activate the new public SSL certificate to trigger the rotation and maintain the service. After you activate the certificate, VMware Tunnel server requires clients to have the new certificate to authenticate.

Rotate the Public SSL Certificate

Configure VMware Tunnel to rotate public SSL certificates to maintain the end-user service experience. VMware Tunnel only supports rotating public SSL certificates.

Note: For immediate certificate rotation, your front-end and back-end servers must be able to communicate with AWCM. Otherwise the rotation might take up to four hours.

Procedure

Complete the following steps to rotate the public SSL certificate:

To prepare a new public SSL certificate:

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration** and select the **Advanced** tab.
2. Scroll down to the **Per-App Tunnel Authentication** section.
3. Select **Add** and upload a new public SSL certificate.
4. Select **Save** to add the certificate to the database.
5. In the UEM console, publish a new version of your VPN profiles configured for VMware Tunnel to devices.

After all the end-user devices have the new profile version, select **Activate Certificate** to use the new certificate. If you have uploaded an incorrect certificate and wish to remove the certificate from the database, select **Remove**.

Integrating VMware Proxy Tunnel with RSA

VMware Tunnel integrates with RSA Adaptive Authentication to allow end users to access internal endpoints using step-up authentication. This integration applies only to the VMware Tunnel Proxy component.

RSA Adaptive Authentication studies user and device patterns, such as location, and then determines whether or not to prompt users to log in based on its algorithm. For example, if end users attempt to access an intranet site and are prompted to authenticate, then they may not be asked to authenticate an hour later if no other device attributes have changed significantly. However, if end users travel to another country or state, then the system may prompt them to authenticate again to access the same site.

RSA Adaptive Authentication Requirements

Before you begin the integration between VMware Tunnel and RSA Adaptive Authentication, ensure that you have read and understood the following requirements:

- Access to RSA Adaptive Authentication server v7.0.
- Authentication Manager integrated with the RSA SecurID plug-in to validate the SecurID tokens.
 - This integration is limited to the use of the RSA SecurID plug-in, along with the RSA Adaptive Authentication service. A Question-Answer based implementation of step-up authentication is not supported with this release.
- VMware Tunnel Proxy component installed. Currently, this integration works only with the Proxy component of VMware Tunnel.

Client Compatibility

- VMware Browser for iOS v4.5+
- VMware Browser for Android v3.1+
- VMware AirWatch Software Development Kit for iOS v5.5+
- VMware AirWatch Software Development Kit for Android v15.11+

Configure RSA Authentication

VMware Tunnel integrates with RSA Adaptive Authentication to allow end users to access internal endpoints using step-up authentication. There are two main workflows to consider when using step-up authentication with this integration:

- Users who have not set their SecurID PIN
- Users who have set their SecurID PIN

For users who have not set their SecurID PIN

In this scenario, when a user initiates a connection with the VMware Tunnel for the first time (for example, when attempting to access an internal Web site), the VMware Tunnel automatically enrolls the user in the RSA Adaptive Authentication database with the **Adaptive Auth User identifier** value set in the Workspace ONE UEM console. Next, the user is prompted to set the SecurID PIN. The user must remember this PIN, because it is the combination of this PIN and the SecurID token number that makes the final passcode that is required to authenticate against the authentication manager to get intranet access. On subsequent requests, users are asked to enter their passcode (PIN + token).

After the user sets the SecurID PIN for the first time and authenticates against the manager, RSA Adaptive Authentication may or may not challenge the user again for several hours. The RSA Adaptive Authentication algorithm decides when to challenge users after the initial authentication. This system is adaptive and studies the user and device patterns. Based on the data that it collects about the user and device, it then decides whether or not to challenge users on subsequent access attempts.

For users who have set their SecurID PIN

Users who have set their SecurID PIN are not asked to set their PIN again and can continue using their existing PIN. The VMware Tunnel enrolls such users in the RSA Adaptive Authentication database, and they are prompted to enter their passcode (a combination of their PIN + token).

Configure RSA Authentication in the UEM console.

In the UEM console, you must enter some of the basic information related to your RSA Adaptive Authentication environment, such as host names, admin credentials, and an Adaptive Auth user identifier, which is a unique identifier for every user in your Active Directory and Authentication Manager.

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration** and select the **Advanced** tab.

- Configure the following RSA Adaptive Authentication settings.

Setting	Description
RSA Adaptive Auth Integration	Enable this setting if you want to integrate the Proxy component with RSA authentication for comprehensive Web browsing security.
Adaptive Auth Server URL	Enter your RSA Adaptive Auth server URL. This setting displays after you enable RSA Adaptive Auth Integration.
Adaptive Auth Admin Username	Enter the RSA admin account user name. This setting displays after you enable RSA Adaptive Auth Integration.
Adaptive Auth Admin Password	Enter the RSA admin account password for the user name you entered. This setting displays after you enable RSA Adaptive Auth Integration.
Adaptive Auth Version	Enter your RSA Adaptive Authentication version. This setting displays after you enable RSA Adaptive Auth Integration.
Adaptive Auth User Identifier	Enter the RSA Adaptive Auth user identifier. This setting displays after you enable RSA Adaptive Auth Integration.

- Select **Save**.

Using VMware Browser for VMware Tunnel

Using VMware Browser for VMware Tunnel controls how the end users access internal sites by configuring communication between the application and the VMware Tunnel. Once configured, access to URLs you specify (using VMware Browser) goes through the VMware Tunnel.

Note: Consider using VMware Browser with the Per-App Tunnel component of VMware Tunnel. The Per-App Tunnel component provides better performance and functionality than the Proxy component. VMware Browser with the Per-App Tunnel component does not require additional configuration.

If you are using VMware Browser with the VMware Tunnel Proxy component:

- Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
- Select **Enabled** for **AirWatch App Tunnel** and specify the **App Tunnel Mode** as **VMware Tunnel – Proxy**.
- (Optional) Enable the split tunnel for iOS devices by entering URLs into the **App Tunnel Domains** text box. If a URL that is about to be invoked contains a domain that matches the list in the settings, this URL request goes through the VMware Tunnel. If the URL domain does not match the domain in the list, it goes directly to the Internet. Leave the text box empty to send all requests through the VMware Tunnel.
- Select **Save**.
- Ensure the VMware Browser is using the Shared SDK profiles for iOS and Android by navigating to **Groups & Settings > All Settings > Apps > VMware Browser** and selecting them under **SDK Profile**.

Caveats and Known Limitations

- For VMware Tunnel, the current authentication scheme requires the use of a chunk aggregator of fixed size. A low value puts restrictions on the amount of data that is sent from the devices in a single HTTP request. By contrast, a high value causes extra memory to be allocated for this operation. Workspace ONE UEM uses a default optimum value of 1 MB, which you can configure based on your maximum expected size of upload data. Configure this value in the proxy.properties file on the VMware Tunnel server in the **/conf** directory.

Chapter 9:

Health and Monitoring

Basic health check lets you analyze whether your VMware Tunnel is operating within the acceptable performance limits. Use the following sections to monitor and assess the health of your VMware Tunnel service.

Access Logs and Syslog Integration

Workspace ONE UEM supports exporting access logs to the syslog server for the Proxy and the Per-App Tunnel components of VMware Tunnel. Access logs are generated in the standard HTTP Apache logs format and directly transferred to the syslog host you defined. They are not stored locally on the VMware Tunnel server.

In relay-endpoint deployments, the relay server writes the access logs, in a cascade deployment, the back-end server writes the access logs and in a basic deployment, the basic server writes the access logs.

For instructions on enabling access log and syslog integration, see [Configure Advanced Settings for the Proxy Component on page 29](#) and [Configure Advanced Settings for the Per-App Tunnel Component on page 22](#).

Under high loads and peak hours, average of 10,000 devices for an hour roughly generates around 0.5 GB of logs to the syslog server. However, your mileage might depend on the load that you might have on your VMware Tunnel server. For additional support, contact your syslog administrator.

KKDCP Access Logs

The path for KKDCP logs for VMware Tunnel for Linux is: `/var/log/vmware/proxy/proxy.log`.

Monitor and Analyze VPN Report

VPN report gives detailed statistics on the VPN use. Network administrators can monitor the activities being performed over the VPN and use the statistical report during troubleshooting .

There are two types of statistical reports administrators can run to get information about the VPN:

- VPN Whitelist Report that fetches the Whitelist information. For more information, see [Run VPN Whitelist Report on page 82](#).
- VPN Statistics Report to get statistical information about the number of connected devices, downstream traffic , service synchronization time and so on. For more information, see [Run VPN Statistics Report on page 82](#).

Run VPN Whitelist Report

Network administrators can run the `vpnreport whitelist` to get the whitelist information report for the devices.

The whitelist report allows administrators to complete the following actions:

- Print the report in an XML format.
- Get the whitelist information for a device with UDID.
- Print the help information.
- Get the verbose output.

You can run the `vpnreport whitelist` from the command line using the following steps:

1. Navigate to the `vpnd` folder.
2. Run the `/vpnreport whitelist` as root.

What to Do Next

You can run the following commands that are supported by the VPN report:

Command	Action
<code>-x, --xml</code>	Print whitelist in an XML format.
<code>-u, --udid=<udid></code>	Get the whitelist information for the device with UDID.
<code>-h, --help</code>	Print the help information.
<code>-v, --verbose</code>	View the verbose output.

Run VPN Statistics Report

Administrators can run the VPN Statistics report to get statistical information about the number of connected devices, downstream traffic, service synchronization time and so on. The report displays interactive graphs that visually represent statistical information.

You can run the `vpnreport stat` from the command line using the following steps:

1. Navigate to the `vpnd` folder.
2. Run the `/vpnreport stat` as root.

What to Do Next

You can use the following menu options while working with the report:

Menu Options	Descriptions
Tab	Select graph
Up/Down	Select field
+/-	Scale up/down
Left/Right	Adjust refresh rate

You can use the following legend to analyze the report:

Legend	Descriptions
Last digit 0	empty
Last digit 1	.
Last digit 2 to 4	
Last digit 5 to 9	*
Any value larger or equal to 10	#

Chapter 10:

VMware Tunnel Troubleshooting and Support

Read through the VMware Tunnel Troubleshooting and Support section if you encounter issues with your VMware Tunnel deployment.

Troubleshooting using the Tunnel_snap Utility

The tunnel_snap utility collects all the necessary diagnostic data that might be required for troubleshooting your VMware Tunnel deployment. This utility helps troubleshooting by reducing the back and forth communication with support and saves time.

The utility captures data from the following files:

- awcm.dat
- ca.pem
- device.xml
- dh2048.pem
- server.conf
- tunnel_init.log
- tunnel.log
- tunnel.log.1
- version.info
- vpn.dat

Use this utility while troubleshooting any issue related to the VMware Tunnel. You must run the utility on each VMware Tunnel server separately.

Run the utility in the following folder:

```
/opt/vmware/tunnel/vpnd/
```

Use the following command to run the utility:

```
sudo ./tunnel_snap.sh
```

The utility collects the diagnostic data in:

```
/opt/vmware/tunnel/vpnd/tunnel_snap.tar
```

Send the collected data to UEM Support for help in troubleshooting.

Upgrade Java Without Reinstalling Tunnel Proxy

When a new version of Java releases, you must update the server hosting the Tunnel Proxy server. VMware Tunnel supports a method that does not require reinstalling the Tunnel Proxy component.

To upgrade Java without reinstalling Tunnel Proxy:

1. Download the latest RPM package for Java from the official Oracle site.
2. Upload the RPM package to your Linux server.
3. Install the RPM package. For example:

```
sudo rpm -i jdk8u112-linux-x64.rpm
```

4. Run the following command to ensure Java is upgraded correctly:

```
ls -la /usr/java/latest
```

5. Restart the Tunnel Proxy service.

Troubleshooting Per-App Component

Per-App Tunnel logs are stored in the native syslog system of Linux. Logs are stored in **/var/log/vmware/tunnel** and can be sorted by the following command (as root):

```
tail -f /var/log/vmware/tunnel/vpnd/tunnel.log
```

Commands Used to Troubleshoot Per-App Tunnel Component

The following table lists the commands that are used to troubleshoot Per-App Tunnel Component:

Component	Function	Command
Virtual Appliance	Start the Service	<code>systemctl start vpnd</code>
Virtual Appliance	Stop the Service	<code>systemctl stop vpnd</code>
Virtual Appliance	Restart the Service	<code>systemctl restart vpnd</code>
CentOS/RHEL 6.x	Start the Service	<code>service vpnd start</code>
CentOS/RHEL 6.x	Stop the Service	<code>Service vpnd stop</code>
CentOS/RHEL 6.x	Restart the Service	<code>service vpnd restart</code>
CentOS/RHEL 7.x	Start the Service	<code>service vpnd start</code>
CentOS/RHEL 7.x	Stop the Service	<code>service vpnd stop</code>
CentOS/RHEL 7.x	Restart the Service	<code>Service vpnd restart</code>

Access Unified Access Gateway Logs

You can access the VMware Tunnel logs from the Unified Access Gateway without logging into the appliance by accessing a specific URL based on your deployment. To download a ZIP file that contains your logs, enter the following URL in a browser: `https://<virtual appliance domain name>:9443/rest/v1/monitor/support-archive`.

Change Per-App Log Level

You can change the log levels for the Per-App component in the Workspace ONE UEM console by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration > Advanced**.

1. Edit `/opt/vmware/tunnel/vpnd/server.conf`
2. Change `log_level <VALUE>` to `log_level 4` and **Save**. If you are writing logs to rsyslog, enable debugging in the rsyslog configuration file.
3. Stop and Start the service.
4. Revert changes and restart both services when finished.

Enable Debug in rsyslog:

You can enable Debug in rsyslog in the Workspace ONE UEM console by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration > Advanced**.

1. Edit `rsyslog.conf` as root.
2. Change `log_level <VALUE>` to `log_level 4` and **Save**.
3. Stop and Start the service.
4. Revert changes and restart both services when finished.

Troubleshooting Proxy Component

Read through the following topic if you encounter issues with the Proxy Component.

Proxy logs are stored in the native syslog system of Linux. Logs are stored in `/var/log/vmware/proxy` and can be sorted by the following command (as root):

```
tail -f /var/log/vmware/proxy/proxy.log
```

Commands Used to Troubleshoot Proxy Tunnel Component

The following table lists the commands that are used to troubleshoot Proxy Tunnel Component:

Component	Function	Command
Proxy – Any CentOS/RHEL version/Virtual Appliance	Start the Service	<code>sudo service proxy start</code>
Proxy – Any CentOS/RHEL version/Virtual Appliance	Stop the Service	<code>sudo service proxy stop</code>
Proxy – Any CentOS/RHEL version/Virtual Appliance	Restart the Service	<code>sudo service proxy status</code>

Access Unified Access Gateway Logs

You can access the VMware Tunnel logs from the Unified Access Gateway without logging into the appliance by accessing a specific URL based on your deployment. To download a ZIP file that contains your logs, enter the following URL in a browser:

`https://<virtual appliance domain name>:9443/rest/v1/monitor/support-archive`

Change Proxy Log Level

You can change the log levels for the Proxy component in the Workspace ONE UEM console by navigating to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration > Advanced**. In cases where communication between the VMware Tunnel and AWCM or API breaks, you can still change the log level with the following steps:

1. Edit the `/opt/vmware/tunnel/proxy/conf/logback.xml` file.
2. Change `<root>log-level=VALUE` to **DEBUG** and Save on file.
3. Stop and Start the service.
4. Revert changes and restart the proxy service when finished.

Verify Proxy Connectivity

Verifying Proxy connectivity post-installation can help determine whether your installation was successful.

1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Configuration**.
2. Select **Test Connection**. You must select the button for the correct component. If you are using Per-App Tunnel, select the button in the Per-App Tunnel section. If you are using Proxy, select the **Test Connection** button in the Proxy component.

For the Per-App Tunnel component, this page displays server IP address, version info, API server connectivity, and AWCM server connectivity. For the Proxy component, this page displays version info, connectivity through HTTP/S, and certificate chain validation.

If you are an on-premises customer and your Workspace ONE UEM console server is installed on the internal network, then you may see fail connection for the **Console To** line items. This expected behavior occurs when the Console server does not have access to the front-end server in the DMZ and does not affect functionality.

Proxy Component Error Codes

The following sections list out the error codes or messages for the VMware Tunnel Proxy component. You can use these error codes and message to better monitor your Workspace ONE UEM deployment.

Code	Name	Meaning
0	UNKNOWN	Unknown error. A runtime exception while processing the request
1	MISSING_HEADER	Headers are missing. This can include headers such as "Proxy-Authorization". Possible Cause: The request was stripped in transit or a bad request was sent from the app. Possible Solution: Check all hops between the device and VMware Tunnel to see if another network component (e.g. proxy, VPN) stripped the header.
2	WRONG_ENCODING	Proxy-Authorization header value is not Base64 encoded. Possible Cause: The request was stripped in transit or a bad request was sent from the app. Possible Solution: Check all hops between the device and VMware Tunnel to see if another network component (e.g. proxy, VPN) stripped the header.
3	TOKENS_DONT_MATCH	Client identification tokens in Proxy-Authorization header do not follow <i>alg:%s;uid:%s;bundleid:%s</i> format. ID_FORMAT should contain encryption algorithm, uid and bundleID in a specific format. One or more of these is not present. Possible Cause: The request was stripped in transit or a bad request was sent from the app. Possible Solution: Check all hops between the device and VMware Tunnel.
4	INVALID_ALGO	The algorithm in the Proxy-Authorization token is not supported
5	EMPTY_CERT_CHAIN	There is no certificate present in the digital signature passed in the Proxy-Authorization header Possible Solution: Check all hops for a stripped certificate.
6	SINGLE_SIGNER	Error thrown if there are multiple signers found in the certificate chain. The request is expected to be signed by only one entity. Possible Cause: A bad certificate. Possible Solution: Create another certificate with a single signer.
7	SINGLE_SIGNER_CERT	Error thrown if there are multiple certificates for signers. The VMware Tunnel expects only one signer. The request signer should sign it with only one certificate. Possible Cause: A bad certificate. Possible Solution: Create another certificate with a single signer.

Code	Name	Meaning
8	INVALID_SIGN	The signer information could not be verified. Possible Solution: Import the signer into the trusted certificate store on the server.
9	UNTRUSTED_ISSUER	The certificate used for signing wasn't issued by Device-Root of the given OG. Possible Cause: Workspace ONE UEM device root is different for enrolled OG and the OG on which VMware Tunnel is configured. Possible Solutions: (1) Override the Workspace ONE UEM device root certificate and regenerate the VMware Tunnel certificate. (2) Export the Workspace ONE UEM certificate from the Console or reinstall the VMware Tunnel.
10	MISSING_SIGN_TIME	The signing time attribute which is used to determine potential replay attack is missing in the signature Possible Cause: A bad certificate. Possible Solution: Determine which certificate is bad in a request log. Create a correct certificate (if the cert is not a Workspace ONE UEM certificate). Re-run the VMware Tunnel installer.
11	POTENTIAL_REPLAY	There is more than a 15 minute interval between signature creation by the requester (AW Browser, Wrapping, etc) and verification by VMware Tunnel
12	INVALID_SIGN_DATA	There is discrepancy in the data that was signed by the requester (AW Browser, Wrapping, etc) and what was expected to be signed by VMware Tunnel. Any method other than the "CONNECT" request is sent to the VMware Tunnel and is rejected. Possible Cause: An invalid request. Possible Solution: Check all hops for what changed with the request at each hop.
13	DATA_UNAVAILABLE	The requester's (AW Browser, Wrapping, etc) related data is not available with VMware Tunnel even after making an API call. No data available for Udid: #####, BundleId: #####. Possible Cause: VMware Tunnel does not have device details. Possible Solutions: Check the VMware Tunnel to API connection. Restart the VMware Tunnel service.
14	INVALID_THUMBPRINT	The thumbprint of the certificate used by the requester (AW Browser, Wrapping, etc) for signing and the one expected by VMware Tunnel is different. Invalid SHA-1 thumbprint. Udid: #####, BundleId: #####. VMware Tunnel expected: XYZ, Found:ABC Possible Cause: Occurs only when device is re-enrolled. Possible Solutions: Re-install the Client (AWB, Wrapped App). Check the VMware Tunnel to AWCM connection. Restart VMware Tunnel Service.

Code	Name	Meaning
15	NOT_COMPLIANT	The device making the request is not compliant (Must be in compliance states of 'Compliant' or 'Not Available'). Possible Cause: VMware Tunnel expected: X,Y, Found: Z Possible Solution: Check the compliance status in the Device Dashboard.
16	NOT_MANAGED	The device is not managed by Workspace ONE UEM. Possible Cause: The device is not enrolled. Possible Solution: Enroll the device.
17	INVALID_CERT	The certificate used by the requester (AW Browser, Wrapping, etc) for signing is not valid (ex. signing time does not fall in the certificate lifetime). Possible Solution: Identify the invalid certificate.
18	NEED_CHUNK_AGGREGATION	Chunk aggregation is not enabled in MAG.properties file
19	HOST_DISCREPANCY	Host name in the URI does not match the one in the host header, deemed as a potential replay attack