VMware Tunnel on Linux

VMware Workspace ONE UEM

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

Contents

Introduction to VMware Tunnel on Linux

1

Workspace ONE UEM powered by AirWatch provides you with VMware Tunnel that offers secure 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.

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 Chapter 3 Understanding the Key Concepts of 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 architecture and security features. For more information, see Chapter 4 VMware Tunnel Architecture.

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 Chapter 6 Configure VMware Tunnel.

VMware Tunnel offers two architecture models for deployment, that is single-tier and multi-tier. For more information on deployment models and components, see Chapter 5 VMware Tunnel Deployment Model.

Deploy VMware Tunnel with 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. The Tunnel service on Unified Access Gateway is same as what the Linux installer provides.

Deploy VMware Tunnel 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.

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 Chapter 9 VMware Tunnel Management .

VMware Tunnel Troubleshooting

The VMware Tunnel supports troubleshooting logs to aid in diagnosing issues in your deployment. For more information, see Chapter 11 VMware Tunnel Troubleshooting and Support.

Supported Platforms for VMware Workspace ONE Tunnel

2

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

Supported Console Versions

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

Supported Platforms

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

Platform	Requirements
iOS	iOS 10.3+
macOS	macOS 10.12+
Android	Android 5.0+
Windows 10	Windows 10 Build 17.04+

Android Considerations

- After installing VMware Workspace ONE Tunnel for Android, end users must run the application at least once and accept the connection request.

- The key icon in the notification center displays on the device because there is an application installed that uses the Per application 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.

- Certain Android devices allow end users to disable the VPN on an OS level. This prevents the VMware Tunnel from working on the device.

Windows 10 Considerations for the UWP application

- After installing VMware Workspace ONE 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.

- Configure dns_server_address_1 and/or dns_server_address_2.

- VMware Tunnel shows as configured when the profile or certificates are successfully installed on Desktop for user profiles. Device profiles for desktop and Windows Phones rely on the successful installation of a profile certificate only.

- To enable functionality for the Windows devices, make sure that you add `NAT` to the `vpn_mode` setting in the server.conf and restart services.

Windows 10 Considerations for the Desktop application

- Make sure that the Windows desktop application either uses Workspace ONE Intelligent Hub for enrollment or is pushed down from the UEM console. For more information, see Workspace ONE Intelligent Hub for Windows enrollment documentation.

- Windows 10 desktop application requires device traffic rules for defining managed applications and domain filtering.

- To enable functionality for the Windows 10 desktop devices, make sure that you add `NAT` to the `vpn_mode` setting.

iOS and macOS Considerations

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

Note   Make sure that you enforce a strong device passcode and device encryption on all your devices. These settings provide an added layer of security. For more information on configuring these settings on each of the platforms, refer to the platform-specific guides.

Understanding the Key Concepts of VMware Tunnel

3

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 become familiar with the VMware Tunnel technologies and features.

VMware Tunnel 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.VMware Tunnel requires a TCP/UDP pass-through configuration on the load balancer for the per-app VPN capabilities. The VMware Tunnel Proxy authenticates devices based on the HTTP header information in the request and ensures 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. VMware Tunnel Proxy supports SSL offloading, bridging, and TCP pass-through.

DTLS and TLS Connection for UDP and TCP traffic

You can open a TCP port and a UDP port on the VMware Tunnel server to support TCP and UDP traffic. VMware Tunnel client seamlessly sends the UDP traffic over DTLS and TCP over TLS. After the TLS channel is established, the VMware Tunnel client establishes a secondary DTLS channel.

If the traffic is UDP, a new UDP datagram flow is created to carry the traffic. The flow is transmitted through the new DTLS channel to the VMware Tunnel server. From the server, a UDP connection is established to the UDP host, and the data in the flow is delivered to the UDP host through the connection and conversely.

Similarly, if the traffic is TCP, a new TCP flow is created to carry the traffic. The flow is transmitted through the original TLS channel to the VMware Tunnel Server. From the server, a TCP connection is created to the TCP host and the data is transmitted through the connection to the TCP host and conversely.

Firewall and Load Balancer Configuration

Since DTLS is transmitted on the top of UDP Protocol, the firewall and the load balancer must be configured to allow the UDP traffic to pass through.

To allow the VMware Tunnel client to establish a DTLS connection to the VMware Tunnel server, the firewall must allow the UDP traffic in and out of the VMware Tunnel Server UDP listing port. For example, if the VMware Tunnel server is setup to listen on port 443, the UDP port 443 must be opened at the firewall to allow all the incoming connection from the devices.

In addition, if a load balancer is used to distribute loads between multiple VMware Tunnel servers, the load balancer must be set up so that the UDP traffic from the device must always go to the same VMware Tunnel server.

For information on load balancing with Unified Access Gateway appliances, see Unified Access Gateway Load Balancing Topologies in the Unified Access Gateway Documentation.

Note The Per App VPN configuration file, server.conf, offers an option to whitelist IP addresses of the load balancer health monitoring. If you choose to perform the health monitoring, specify the IP addresses of the health monitoring servers within the configuration file that sends the following pings to avoid the health monitoring pings to be counted as bad TLS/DTLS handshakes.

- Maximum of 8 addresses.

- Incoming_ping_address_1 0.0.0.0 (Make sure to uncomment this line).

- Incoming_ping_address_2 0.0.0.0 (Make sure to uncomment this line).

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 Workspace ONE Tunnel with Workspace ONE Web, you can provide secure internal browsing to any intranet site and web application that resides within your network. Because Workspace ONE Web 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, Workspace ONE Web 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

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 Workspace ONE Tunnel apps for iOS, Android, Windows Desktop, and macOS allow both internal, public, and purchased (iOS) 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.

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.

Proxy Component

Proxy is the VMware Tunnel component that handles securing traffic between an end-user device and a website through the Workspace ONE Web mobile application. VMware Tunnel Proxy is also available on Windows.

To use an internal application with VMware Tunnel Proxy, then ensure the VMware Workspace ONE SDK 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 platform 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 on ESXi, Hyper-V, AWS or Azure 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.

Note   Unified Access Gateway can be deployed with the FIPS version of the appliance. In such cases, only the Per-App Tunnel Component is available.

Load Balancing

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

VMware Tunnel 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.VMware Tunnel requires a TCP/UDP pass-through configuration on the load balancer for the per-app VPN capabilities. The VMware Tunnel Proxy authenticates devices based on the HTTP header information in the request and ensures 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. VMware Tunnel Proxy supports SSL offloading, bridging, and TCP pass-through.

DTLS and TLS Connection for UDP and TCP traffic

You can open a TCP port and a UDP port on the VMware Tunnel server to support TCP and UDP traffic. VMware Tunnel client seamlessly sends the UDP traffic over DTLS and TCP over TLS. After the TLS channel is established, the VMware Tunnel client establishes a secondary DTLS channel.

If the traffic is UDP, a new UDP datagram flow is created to carry the traffic. The flow is transmitted through the new DTLS channel to the VMware Tunnel server. From the server, a UDP connection is established to the UDP host, and the data in the flow is delivered to the UDP host through the connection and conversely.

Similarly, if the traffic is TCP, a new TCP flow is created to carry the traffic. The flow is transmitted through the original TLS channel to the VMware Tunnel Server. From the server, a TCP connection is created to the TCP host and the data is transmitted through the connection to the TCP host and conversely.

Firewall and Load Balancer Configuration

Since DTLS is transmitted on the top of UDP Protocol, the firewall and the load balancer must be configured to allow the UDP traffic to pass through.

To allow the VMware Tunnel client to establish a DTLS connection to the VMware Tunnel server, the firewall must allow the UDP traffic in and out of the VMware Tunnel Server UDP listing port. For example, if the VMware Tunnel server is setup to listen on port 443, the UDP port 443 must be opened at the firewall to allow all the incoming connection from the devices.

In addition, if a load balancer is used to distribute loads between multiple VMware Tunnel servers, the load balancer must be set up so that the UDP traffic from the device must always go to the same VMware Tunnel server.

For information on load balancing with Unified Access Gateway appliances, see Unified Access Gateway Load Balancing Topologies in the Unified Access Gateway Documentation.

Note The Per App VPN configuration file, server.conf, offers an option to whitelist IP addresses of the load balancer health monitoring. If you choose to perform the health monitoring, specify the IP addresses of the health monitoring servers within the configuration file that sends the following pings to avoid the health monitoring pings to be counted as bad TLS/DTLS handshakes.

- Maximum of 8 addresses.

- Incoming_ping_address_1 0.0.0.0 (Make sure to uncomment this line).

- Incoming_ping_address_2 0.0.0.0 (Make sure to uncomment this line).

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/UDP and HTTP(S).

VMware Tunnel Architecture

4

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. This component can be leveraged only by the applications having the Workspace ONE (AirWatch) SDK implemented or using the App Wrapping. This includes most of the VMware productivity applications.

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

VMware Tunnel provides granular access control to applications and services both in your network and in the cloud. The VMware Tunnel client provides per-app management, permitting explicit trust of individual applications you want to manage, and domain-based filtering for the easy definition of access control and split-tunneling policies.

VMware Tunnel is built on native frameworks provided across all major platforms. When an application is launched or creates a network request, that request is forwarded to the Tunnel client for routing. In this way, Tunnel provides local filtering for determining what traffic must be tunneled into your network, sent to the Internet or another proxy, or blocked from leaving the device.

Data that is passed to the Tunnel gateway leverages TLS and DTLS algorithms to perform the following checks as part of authentication:

- VMware Tunnel uses SSL pinning to ensure that the server identity is correct.

- VMware Tunnel performs TLS mutual authentication with a client certificate that uniquely identifies the device.

- VMware Tunnel gateway validates that the client certificate is on a whitelist of trusted certificates within the Workspace ONE UEM Console, and performs a device compliance check to ensure the integrity of the user's device.

For internal routing of traffic, it is required that the Tunnel gateway has properly configured DNS, as routing policies for Tunnel are defined on hostnames and not IP address. If internal DNS is not exposed in the DMZ, then it is recommended to deploy VMware Tunnel in a cascade mode to make use of the internal DNS controllers.

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.

Complete the following steps for 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 the 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 generates a unique self-signed certificate to be used as the server certificate. Optionally, you can also use your own Public SSL certificate instead of the self-signed certificate on the Front-end VMware Tunnel server (if VMware Tunnel is deployed using the cascade mode) or on the backend server (if VMware Tunnel is deployed using the basic mode).

4   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**.

Complete the following steps for 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 VMware Tunnel Device Root Certificate is used to generate client certificates for each device.

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   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.

5   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

5

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.

Deploying VMware Tunnel using Single-Tier Deployment

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. 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.

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.

| Saas Single-Tier Model | On-Premises Single-Tier Model |
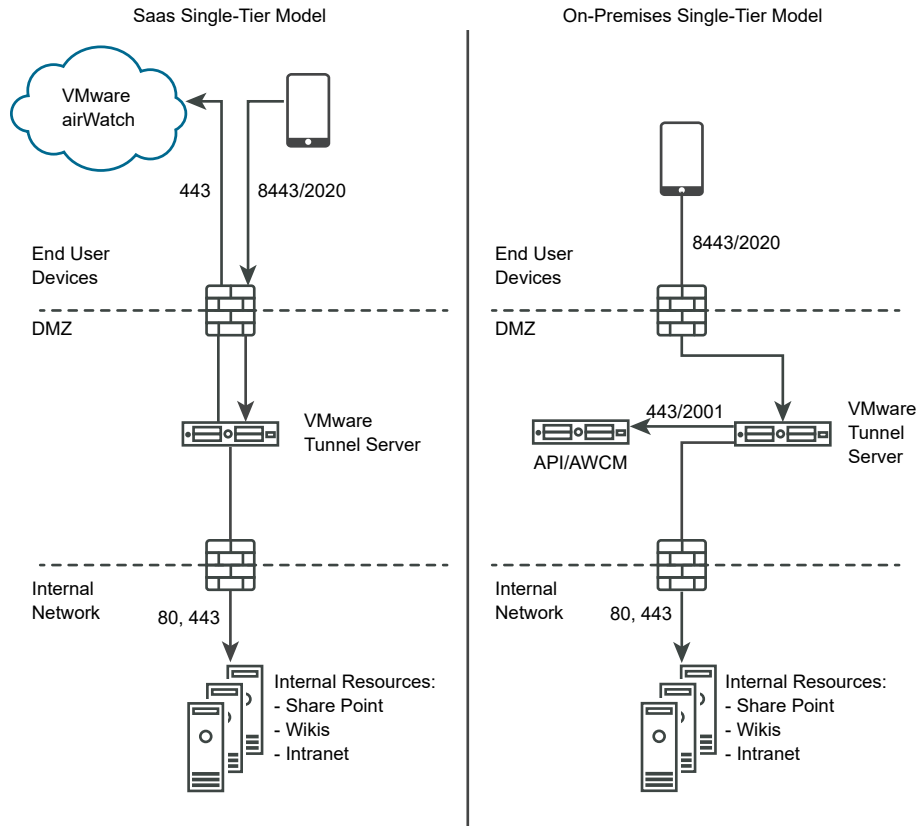
Deploying VMware Tunnel using Cascade Mode Deployment

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. If you use only the Proxy component, you must use the Relay-Endpoint model.

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. 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, device access control list, 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

The following diagram illustrates the Multi-Tier deployment for the Per-App Tunnel component in cascade mode:
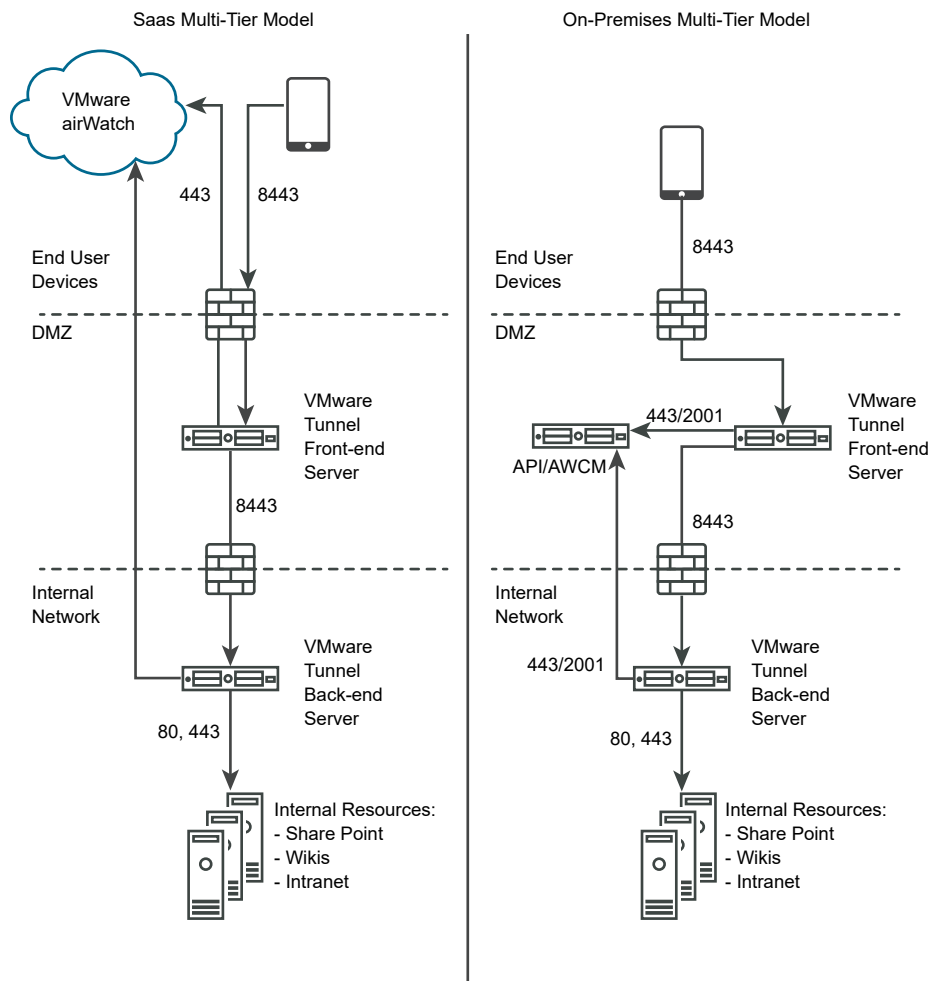
Deploying VMware Tunnel using Relay-Endpoint

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.

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, communication to API and AWCM from the relay server can be routed to the Outbound Proxy via endpoint server. 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.

Figure 5-1. On-premises configuration for Relay-Endpoint deployments
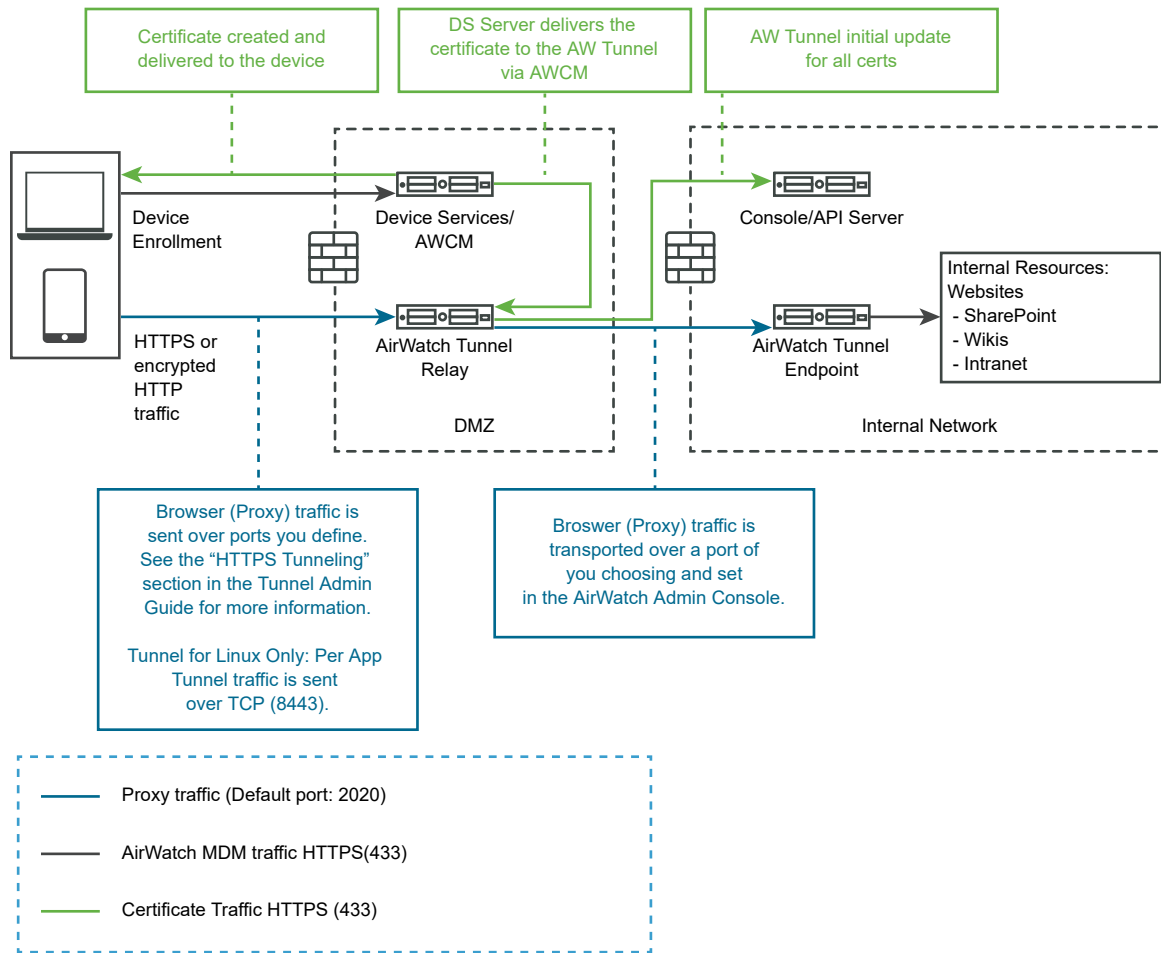
Figure 5-2. SaaS configuration for Relay-Endpoint deployments
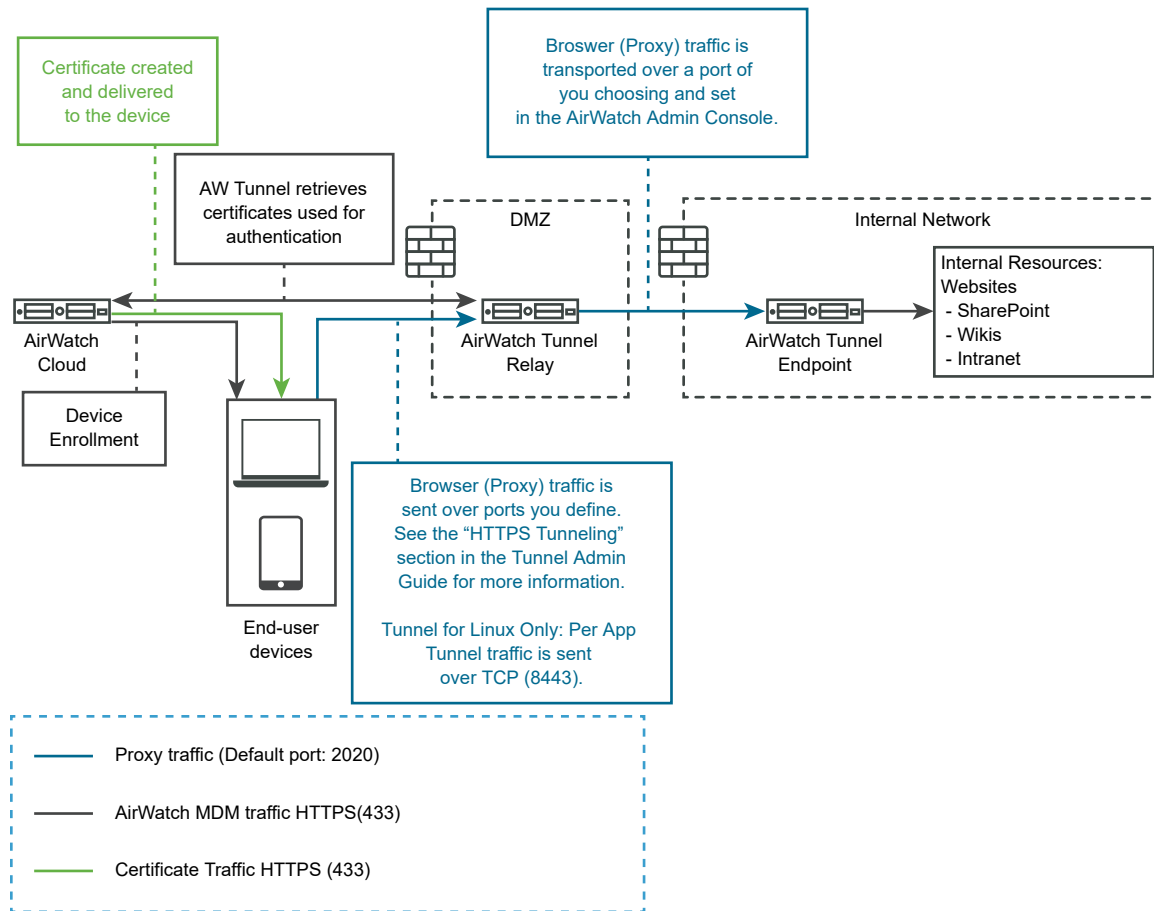
Configure VMware Tunnel

6

VMware Tunnel enables secure access for mobile workers and devices. Users have a simple experience and need not enable or interact with VMware Tunnel, and IT organizations may take a least-privilege approach to enterprise access, ensuring only defines apps and domains have access to the network. VMware Tunnel provides industry-best security and builds on TLS 1.2+ libraries, implements SSL Pinning to ensure no MITM attacks, and includes client certificates on the allowlist to ensure identity integrity. Combined with explicit definitions of managed applications and integration with Workspace ONE compliance engine, Tunnel can help customers attain Zero Trust goals for their workforce.

Preparing for your 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.

Prerequisites

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

- VMware Unified Access Gateway with VMware Tunnel edge service configured

- Workspace ONE UEM 1909 and later

- A device for the platform you plan to use (Windows 10, macOS, Android, or iOS)

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

- Organization Group created and set as Customer Type

- Device Root Certificate issued

- VMware Tunnel configured

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.

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.

3   After you complete the VMware Tunnel configuration, you also must configure various settings to enable the VMware Web and Per-App Tunnel-enabled apps to use VMware Tunnel. Doing so ensures all HTTP(S) and TCP/ UDP traffic for the specified applications is routed through the VMware Tunnel.

4   You can configure more settings that are optional for the VMware Tunnel deployment. Except where noted, you can configure these settings before or after installation.

This chapter includes the following topics:

- Configure AWCM Server and Enable API Access before VMware Tunnel installation

- Configure Per-App Tunnel

- Configure Network Traffic Rules for the Per-App Tunnel

- Integrating VMware Tunnel with NSX

- Configure VMware Tunnel Proxy

- Configure Outbound Proxy

Configure AWCM Server and Enable API Access before VMware Tunnel installation

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.

Procedure

1   Navigate to **Groups & Settings > All Settings > System > Advanced > API > REST API** and select the **Override** radio button.

2   Ensure that the **Enable API Access** check box is selected and an API Key is displayed in the text box.

3   Select **Save**.

Configure Per-App Tunnel

Configure the fundamental VMware Tunnel architecture to establish connectivity and trust within your environment with the Per-App Tunnel.

Procedure

1   Navigate to **Groups & Settings > All Settings > Configurations > Tunnel**. Select a Current Setting or **Override** to make new settings for the child.

    Note   Overriding Tunnel configuration does not override VMware Tunnel Proxy settings.

2   Under **Deployment Details**, select whether you are deploying VMware Tunnel in **Basic** or **Cascade** mode.

    When deploying in **Basic** mode, supply the public-facing **Hostname** and the **Port** number that is assigned for communication with the VMware Tunnel component.

    When deploying in Cascade mode, enter the **Hostname** of the back-end server and the **Port** number.

    Note   Make sure that you configure Per-App Tunnel and Tunnel Proxy with different ports.

3   Under **Server Authentication**, select the SSL provider of your choice.

    By default, AirWatch provides a certificate, however third-party certificates are also supported. When using a third-party certificate, make sure to include both public and private keys in either .PFX or .P12 format.

4   Under **Client Authentication**, select either **AirWatch** or a **Third Party CA** as the authentication provider for VMware Tunnel users.

    To use a third-party certificate authority, select the **Certificate Authority** and **Certificate Template** that are used to request a certificate from the CA.

    In order for the VMware Tunnel gateway to trust certificates issued by a third-party 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. If the Windows desktop Tunnel client is used with the Per-App Tunnel, then the template must contain CN={UDID}:vpn.air-watch.com.

    Certificates auto-renew based on your CA template settings.

5   Under **Networking**, define how VMware Tunnel communicates with Workspace ONE UEM and how the device traffic flows through your network.

    a   Select **Manage Server Traffic Rules with VMware Tunnel PAC Reader** if you are using the PAC Reader to manage the traffic rules.

    b   Select **Default AWCM + API traffic via Server Traffic Rules** if the communication between the VMware Tunnel and Workspace ONE UEM API or AWCM uses the outbound proxy.

6 Under **Logging**, you can configure settings related to the server logs.

a Select the level of logging for the VMware Tunnel from the **Service Logs** drop-down menu. It is considered to be a best practice to select the **Service Logs** as **Error** or **Info** unless you are troubleshooting.

b **Access Logs** provide a high-level record of users and devices using VMware Tunnel. In a cascade deployment, the back-end server performs the syslog transport.

From the **Access Logs** drop-down, you can select the following:

- **Syslog Hostname** : If you make this selection, enter the URL of your `syslog` host and the UDP Port over which you want to communicate. Ensure that the logging level for access logs is set appropriately in rsyslog.conf on the syslog server.

- **File** : If you make this selection, the filename is set to `/var/log/vmware/tunnel/vpnd/access.log`.

There is no correlation between this `syslog` integration and the integration accessed on **Groups & Settings > All Settings > System > Enterprise Integration > Syslog**.

7 Under **Custom Settings**, select **Add Custom Setting** and add the **Configuration Key**, and the **Configuration Value**.

You can configure the following **Configuration Key** and the **Configuration Value**:

Field	Syntax	Example	Description
keepalive_timeout	`keepalive_timeout <time in seconds>` Default Value= 300	`keepalive_timeout 300`	Time (in seconds) before disconnecting the device's connection without receiving a TCP keepalive.
client_ip_traffic	`client_ip_traffic <value>` Default Value= 1	`client_ip_traffic 1`	Set client-side IP mode: ■ `0`= Dual IPv4/IPv6. Both IPv4 and IPv6 traffic are enabled on the device side. ■ **1** = IPv4 Only. Only IPv4 traffic is enabled on the device side. ■ **2** = IPv6 Only. Only IPv6 traffic is enabled on the device side.

Field	Syntax	Example	Description
dns_ip_mode	`dns_ip_mode <value>` Default Value= 1	`dns_ip_mode 0`	Set DNS IPv4/IPv6 query mode: ■ 0 = Dual IPv4/IPv6. Both IPv4 and IPv6 results are allowed in the DNS query result. ■ **1** = IPv4 Only. Only allows IPv4 addresses in the DNS query result. ■ **2** = IPv6 Only. Only allow IPv6 addresses in the DNS query result.
dns_server_address_1, dns_server_address_2...	`dns_server_address_1 <ip address or domain name>`	`dns_server_address_1 1.2.3.4`	Specifies different DNS servers that devices uses for the DNS lookup. If not specified, settings from the `/etc/resolv.conf` is used. Up to 4 addresses can be specified using _1, _2, _3 and _4 suffix.
api_configuration_fetch_interval	`api_configuration_fetch_interval <min>` Default Value= 60	`api_configuration_fetch_interval 60`	Specifies the interval in minutes to redownload configuration including Server traffic rules from API (minimum=15)
dtls_channel	`dlts_channel <value>` Default Value= 1	`dlts_channel 1`	Specifies if a secondary DTLS channel must be enabled for device UDP traffic, this also requires additional firewall modification to allow the UDP port.

openssl_cipher_list	`openssl_cipher_list <value>`
	Default Value=
	`ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256`
		`openssl_cipher_list ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-GCM-SHA256`	Specifies the cipher suites allowed in TLS handshakes between servers and devices. Supports the format supported by OpenSSL ciphers command: https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

Field	Syntax	Example	Description
nsx_ethernet_interface	`nsx_ethernet_interface <interface name>`	`nsx_ethernet_interface eth1`	Specifies the ethernet interface where traffic to NSX will be routed to. Virtual interface is created based on this Ethernet interface. For example, if `nsx_host_id` is **2** and `nsx_ethernet_interface` is **eth1**. If two security groups with two IP sets (**192.168.0.0/24** and **192.168.1.0/24**) are defined, two virtual interfaces are needed. As a result, `eth1:001` will be created with **192.168.0.2** and `eth1:002` is created with **192.168.1.2**.
access_log_events	`access_log_events <events to log>` Default Value= 1,2,3,4,5	`access_log_events 1,2,3,4,5`	Specifies the events that must be logged in the access log. ■ **1 — Session connect** : Logs when a device connects to the tunnel server. ■ **2— Session disconnect** : Logs when a device disconnects from the tunnel server. ■ **3 — Stream connect** : Logs when a TCP connection is established between an application on the device and a host. ■ **4 — Stream disconnect** : Logs when a TCP connection is disconnected. **5 — HTTP request/ response**: Logs when an HTTP traffic is detected (unencrypted traffic only).

Field	Syntax	Example	Description
access_log_format	access_log_format <format> Default Value= `%h %l %u %t "%r" %>s %b "%{Referer}i" "% {User-Agent}i" "%{Device-UID}e"`	access_log_format `%h %l %u %t "%r" %>s %b "%{Referer}i" "% {User-Agent}i" "% {Device-UID}e"`	Access log format. Supported log variables: ■ **%h** - Remote host ■ **%l** - remote logname ■ **%u** - remote user ■ **%t** - time ■ **%r** - first line of request ■ **%s** - status ■ **%b** - size of response ■ **%{variable}i** - HTTP request header variables ■ **%{variable}e**- HTTP request response variables
access_log_custom_format _session_connect	access_log_custom_format_ session_connect <format> Default Value= `%{Connection}v % {Connection-ID}v %{Connection-Type}v %{Connection- Status}v % {Connection-Time}v %{Device-Uid}v %{Device-Name}v %{Device-IP}v->% {Cascade-IP}v %{Device-Vpn-IP}v %{VPN-Server- Connection- Availability}v`	access_log_custom_fo rmat_session_connect `%{Connection}v %{Connection-ID}v %{Connection-Type}v %{Connection- Status}v %{Connection-Time}v %{Device-Uid}v %{Device-Name}v %{Device-IP}v %{Device-Vpn-IP}v %{VPN-Server- Connection- Availability}v`	This setting defines access log message format when a new session is connected. See access_log_format for a list of supported specifiers.
access_log_custom_format _session_disconnect	access_log_custom_format_ session_disconnect <format> Default Value= `%{Connection}v %{Connection-ID}v %{Connection-Time}v %{Device-Uid}v %{Device-Name}v %{Device-App}v %{Remote-Connection- Status}v %{Remote-Host-Name}v %{Remote-Host-IP}v %{Remote-Bytes- Transferred}v`	access_log_custom_fo rmat_session_disconn ect `%{Connection}v %{Connection-ID}v %{Connection-Time}v %{Device-Uid}v %{Device-Name}v %{Device-App}v %{Remote-Connection- Status}v %{Remote-Host- Name}v %{Remote-Host-IP}v % {Remote-Bytes- Transferred}v`	This setting defines access log message format when a session is disconnected. See access_log_format for a list of supported specifiers.

Field	Syntax	Example	Description

access_log_custom_format _stream_connect	`access_log_custom_format_ stream_connect <format>`
	Default Value=
	
	`%{Connection}v`
	`%{Connection-ID}v`
	`%{Connection-Type}v`
	`%{Connection-Time}v`
	`%{Device-Uid}v`
	`%{Device-Name}v`
	`%{Device-Username}v`
	`%{Device-App}v`
	`%{Remote-Connection-Status}v`
	` %{Remote-Host-Name}v`
	`%{Remote-Host-IP}v`
		`access_log_custom_fo rmat_stream_connect %{Connection}v %{Connection-ID}v %{Connection-Type}v %{Connection-Time}v %{Device-Uid}v % {Device-Name}v %{Device-Username}v %{Device-App}v % {Remote-Connection-Status}v %{Remote-Host-Name}v %`	This setting defines access log message format when a new stream is connected. See access_log_format for a list of supported specifiers.

access_log_custom_format _stream_disconnect	`access_log_custom_format_ stream_disconnect <format>`
	
	` %{Connection-ID}v`
	`%{Connection-Time}v`
	`%{Device-Uid}v`
	`%{Device-Name}v`
	`%{Device-App}v`
	`%{Remote-Connection-Status}v`
	`%{Remote-Host-Name}v`
	`%{Remote-Host-IP}v`
	`%{Remote-Bytes-Transferred}v`
		`access_log_custom_fo rmat_stream_disconne ct %{Connection-ID}v %{Connection-Time}v %{Device-Uid}v %{Device-Name}v %{Device-App}v %{Remote-Connection-Status}v %{Remote-Host-Name}v %{Remote-Host-IP}v %{Remote-Bytes-Transferred}v`	This setting defines access log message format when a stream is disconnected. See access_log_format for a list of supported specifiers.

vpn_mode	`socks,nat`	`vpn_mode nat,socks`	Supported modes: socks: Per-App Tunnel with SOCKS Proxy for Android, iOS and MacOS devices nat: Per-App Tunnel with NAT Protocol for Windows devices tun (experimental): Per-App Tunnel using Linux TUN driver for Windows devices. Cannot be used together with 'nat' mode. This mode requires more configuration such as iptables NAT setup or corporate routing setup for the return traffic so customers are recommended to use 'nat' mode instead.

> **Note**   The **Custom Settings** that is used for defining the **Configuration Key** and the **Configuration Value** is available only in Workspace ONE UEM console 2003 or later. For older versions of the Workspace ONE UEMconsole, the server.conf file has to be manually modified. The service restart removes the configuration from Unified Access Gateway 3.7+.

8   Select **Save**.

What to do next

- **Edit**, **Disable**, or **Delete** the VMware Tunnel configuration.

- Download the **Installer** and **XML** to finish the setup.

- **Test Connection** to verify the server reachability.

You can now configure your advanced settings for the VMware Tunnel component.

Configure Network Traffic Rules for the Per-App Tunnel

Network traffic rules allow you to set granular control over how the VMware Tunnel directs traffic from devices. Using the Per-App Tunnel 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 application 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. 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 Workspace ONE Tunnel for iOS.

- macOS devices with VMware Workspace ONE Tunnel for macOS.

    Note
    - For macOS you can add apps under Device Traffic Rules and assign Device Traffic Rules if you are using UEM console 1910 or above.

    - If you using UEM console 1910 or above, the VPN profile for macOS will not have the App Mapping section and the apps have to be added on the Device Traffic Rules page.

- Android devices with VMware Workspace ONE Tunnel for Android.

- Windows desktop devices with VMware Workspace ONE Tunnel desktop application.

    Note Device Traffic Rules added are applicable only to Windows Tunnel Desktop Client and not for the Windows store App. Device wide VPN profile has to be enabled to use Windows Tunnel Desktop Client.

Create Device Traffic Rules

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

Before you create device traffic rules, verify the following:

- Make sure you have configured VMware Tunnel with the Per-App Tunnel component enabled.

- For iOS and Android applications, configure Per App VPN for VMware Tunnel. .

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

Administrators can create multiple Device Traffic Rules sets through Manage Traffic Assignments to segment traffic to internal resources, such as rules for employees devices that as less restricted them access to contractor devices.

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

Complete the following steps to create device traffic rules:

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

2 By default, the **Device Traffic Rules** settings of the Child OG are set to **Inherit** . You can override the DTR settings which allows to **Edit** the DTR settings for the current OG. Based on your configuration needs, you can also select Clear Override if you want to set it back to inherit the **Device Traffic Rules** settings of the current organization group's parent OG.

3   Click **Edit** . Click **Add** to create a new DTR set or you can edit the default DTR set.

Settings	Description
Tunnel Mode	- Per Application : Only the application configured for VPN would be consider and take action based on destination FQDN/IP - Full Device: Directs all application & all traffic from the device through an encrypted tunnel to the corporate data centre based on the destination FQDN/IP. **Note** - Full device tunnel mode is supported only on Windows Tunnel Desktop Client 2.1 and above for now. - We suggest to bypass the VMware Workspace one DS URL, while using Full device VPN with default action as Tunnel.
Add Rule	Select **Add Rule** to create a rule. These rules are only applicable to the Per-App Tunnel component of VMware Tunnel for Android, iOS, macOS, and Windows Desktop devices. For iOS, use the Workspace ONE Tunnel client application from the App store. For Windows Desktop, use the Workspace ONE Tunnel Desktop application. **Rank**: Select-and-drag the rule to rearrange the ranking of your network traffic rules. **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. **Tunnel** – Sends app network traffic for specified domains through the tunnel to your internal network. All apps, except Safari, on the device configured for Per App VPN sends the network traffic through the tunnel. For example, set the **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 the 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.

Settings	Description
	■ **Bypass** – Bypasses 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.
	■ **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.
	■ **Tunnel+Proxy** - Redirect traffic to a specified HTTP proxy that resides behind Tunnel.
	Note This action is supported by the Tunnel SDK on iOS and Android as used by the Workspace ONE Web app. The only configuration required here is the proxy host; the proxy destinations must be provided to the Workspace ONE Web app.
	4 **Destination**: 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 can use wildcard characters for your hostnames. Wildcards must follow the format:
	■ *.<domain>.*
	■ *<domain>.*
	■ *.* — You cannot use this wildcard for Safari domain rules.
	■ * — You cannot use this wildcard for Safari domain rules.
	■ We support IPV4 & Port range when applying the device traffic rule based on destination for Windows Tunnel Client desktop 2.1 and above. Refer Windows Tunnel 2.1 release document for the supported syntax
	■ For other platforms, default action will be applied for the IP based destination/traffic
	5 Select **Save** to save your changes.
Manage Applications	1 Click **Add**.
	2 Select the **Platform**.
	3 For Windows Tunnel Desktop Client, complete the following steps:
	■ Enter a **Frienly Name** for the application.
	■ Select the **App Type**.
	■ Enter the **App Identifier**.

Settings	Description
	The **App Identifier** is the path or the package family name (PFN) of the application. For a Store App, the Package Friendly Name (PFN) is used and can be found using the PowerShell command `Get-AppxPackage *<app_name>`. For a Desktop App, the filepath is used. For example, you can use `C:\Program Files (x86)\acme\app.exe`.
	Note macOS traffic rules can be created only if you are using UEM console 1910 or above.Older versions have to configure the rules via profile.
	4 For macOS applications, complete the following steps: - Enter the **Friendly Name** for the application. - Enter the **Package ID**. - Enter the **Designated Requirement** - Enter the **Path**. This text box is optional and is only applicable for macOS Catalina and above. Enter the **Path** when the whitelisting command-line utils are bundled inside an application. For example, executable `vmware-remotemks` has to be whitelisted with path details with the VMware Horizon Client application. - Select **Save** to save your changes. If you choose to make any changes to the application, in the **Manage Applications** window, select the application you like you edit and make changes. If you want to delete any application, in the **Manage Applications** window, select the application you like to delete and click **Delete**.

4 Enter the **Device Traffic Rule SET Name**.

5 Configure the Device Traffic Rules.

6 Click **Save** or **Save and Publish**.

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

8   To send the updated Device Traffic Rules to the devices post modifying the Device Traffic Rules, administrators must click **Save and Publish**. **Save and Publish** adds a version to the VPN profile and republishes Device Traffic Rules to all the devices

Note

■   You cannot delete the Default Traffic Rule set.

■   **Save and Publish** option is available only for the Default Traffic Rule set

■   If an administrator changes the Android application in the Device Traffic Rules and clicks **Save and Publish**, the VPN profiles for both iOS, Android profiles gets a version update and the VPN profile installs are queued for all the assigned devices.

■   Reinstalling the profile reissues the client certificate to the device with a new thumbprint.

Each assignment of Device Traffic Rules can be selected within your Tunnel profile. This allows you to create different policies for different types of personas based on user, device, or use-case.

Configure Server Traffic Rules using Outbound Proxy

You can configure server traffic 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. You can either add rules manually in the UEM console or via PAC files by using the VMware Tunnel PAC Reader.

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.

The following table illustrates outbound proxy support for the VMware Tunnel Per-App Tunnel 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.

If you want to send the requests to the API/AWCM servers through your outbound proxy as well, then you must enable the **Default AWCM + API traffic via Server Traffic Rules** Networking settings under **Groups & Settings > All Settings > Configurations > Tunnel**. Once enabled, add the respective web proxies for API/AWCM hostnames on the server traffic rules page.

Configure Server Traffic Rules from the UEM Console

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.

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

2   Select **Configure**.

3   In the Outbound Proxies section, select **Edit** and the select **Add Outbound Proxy** to add a third-party outbound proxy. You may add additional outbound proxies by selecting **Add Outbound Proxy** again.

Settings	Description
Host	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. Select **Basic** or **NTLM**.
User Name	Enter the **User name** for proxy authentication.
Password	Enter the **Password** for proxy authentication.

4   Select **Save** to save your changes.

5   In the Server Traffic Rules section, you can configure the server traffic rule settings.

6   Select **Edit**.

7   Select **Add Server Traffic Rule** to add a new server traffic rule. Enter the following information:

Settings	Description
Destination	Enter the destination hostname that triggers the traffic rule.
	Rules for applications on Windows 10 and macOS (except Safari) devices must use IP address as the hostname.
	You cannot use regular expressions except specfic wildcard characters. Windows 10 and macOS devices support using the following wildcards:
	■ 10.10.*
	■ 10.10.0.0/16
	If you are entering multiple hostnames, separate them by commas.
	For domains you want to resolve on Windows 10 devices through the VMware Tunnel server, you must add the domains to the Windows Desktop VPN profile for VMware Tunnel.
Action	Select the action that the VMware Tunnel applies to server traffic for the destination hostname.
	■ 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.
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 Proxies** section.

8   (Optional) Select **Add Server Traffic Rule** if you wish to add any additional server traffic rules.

9   Select **Apply** to save your changes.

10 Select **Close**.

Configure Server Traffic Rules using VMware Tunnel PAC Reader

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

Complete the following steps before you configure the server traffic rules using the PAC reader:

- Download the PAC Reader bundle from the Workspace ONE UEM Resources Portal. Install the PAC Reader on any Linux server such as your VMware Tunnel server. 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.

  Note Currently the PAC Reader has the following limitations:

  - Currently, the PAC Reader only supports Linux servers.

  - The PAC Reader currently 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 Reader only supports limited use of the variable declaration and use.

  Before you configure Outbound Proxy using VMware Tunnel PAC Reader, make sure that you meet the following network requirements:

  - Access to the Workspace ONE UEM API server: The PAC Reader requires access to the Workspace ONE UEM API server. The server is typically accessed over port 443. Consider installing the PAC Reader 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 Reader must have the access to that server.

  - RHEL 7 as the server OS.

Complete the following steps to configure the server traffic rules using the PAC reader:

1   Download the installer from the Workspace ONE UEM Resources Portal.

2   Create a dedicated install directory for the installer on the linux server. For example, you can create a dedicated install directory as `/tmp/Install/` for the installer and copy the `LinuxPacReaderInstaller.bin` file to this location.

3   Navigate to the directory you copied the file. Run `chmod 750 LinuxPacReaderInstaller.bin` command to assign the execute permission to the `LinuxPacReaderInstaller.bin` file.

4   Run the BIN file by using the required command: `sudo ./LinuxPacReaderInstaller.bin`

5 Configure the necessary properties in the pacreader.properties file.

Setting	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**.
Location group ID	Location Group ID where the VMware Tunnel server is deployed.
PAC Location	Path to the PAC file if stored locally on the machine else use the http/https link If you configure PAC_LINK, do not configure PAC_PATH.
API Certificate	: The Admin API Certificate which can be obtained from **UEM Console > Accounts > Administrators > > List View > Edit account > API > Certificates > Export Certificate** If you configure PAC_PATH, do not configure PAC_LINK.
API Certificate Password	Password for pfx/p12 API certificate file.
PAC Location	This can be a PAC file placed at `/opt/vmware/tunnel/pacreader` or an http link to PAC.

Complete the following steps after you configure the server traffic rules using the PAC reader:

- Open the `bash shell`.

- Go to the `pacreader installation directory. cmd:` `cd /opt/vmware/tunnel/pacreader`.

- Execute the following command to validate : `./pacreader validate`.

Integrating VMware Tunnel with NSX

You can integrate VMware Tunnel with the VMware NSX to extend security policies from the data center to mobile application endpoints. Integrating Tunnel and NSX enhances network microsegmentation by providing explicit mappings between network segments and mobile apps. By creating policies that dynamically follow mobile applications, you can eliminate complex and time-consuming firewall provisioning.

Integrate Tunnel with NSX to match per-app policies with security groups defined in NSX. This enhances the network and app security by minimizing the attack surface into your network. Complete the following steps to integrate VMware Tunnel with NSX.

Procedure

1 Navigate to **Groups & Settings > Configurations > VMware Tunnel**.

2 Under the NSX section, select **Configure** and **Enable NSX Integration**.

3 Select your NSX version. Both NSX-V and NSX-T are supported.

4 Enter the **NSX Manager URL**. The destination URML must contain the protocol and hostname or IP address.

5   Enter the **Admin Username** and **Password** .

6   Select **Sync with NSX**.

Results

Workspace ONE UEM adds the tagged groups to the page after successfully syncing with NSX. You may now assign mobile apps to their appropriate NSX security groups.

Configure VMware Tunnel Proxy

Configure VMware Tunnel Proxy using the configuration wizard. The options configured in the wizard are packaged in the installer, which you can download from the Workspace ONE UEM console and move to your Tunnel servers. Configure the VMware Tunnel Proxy in the UEM console under Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel Proxy. 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 Workspace ONE 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 Proxy, you need the details of the server where you plan to install. Before configuration, determine the deployment model, hostnames and ports, and which features of VMware Tunnel to implement. You can consider to change the access log integration, SSL offloading, enterprise certificate authority integration, and so on.

Complete the following steps to configure advanced settings for the VMware Tunnel Proxy:

Note

The wizard dynamically displays the appropriate options based on your selections, the configuration screens may display different text boxes and options.

1   Navigate to **Groups & Settings** > **All Settings** > **System** > **Enterprise Integration** > **VMware Tunnel** > **Proxy**.

- If you are configuring VMware Tunnel for the first time, then select **Configure** and follow the configuration wizard screens.

- If you are configuring VMwareTunnel for the first time, then select **Override**, then select the **Enabled VMware Tunnel** toggle switch, and then select **Configure**.

- **Note**

  Overriding VMware Tunnel Proxy settings does not override VMware Tunnel configuration settings.

2   On the **Deployment Type** screen, select **Enable Proxy (Windows & Linux)** the toggle switch, and then select the components that you want to configure using the **Proxy Configuration Type** drop-down menu.

3   In the drop-down menus that display, select whether you are configuring a **Relay-Endpoint**, or the **Proxy Configuration Type** deployment. To see an example for the selected type, select the information icon.

4   Select **Next**.

5   On the **Details** screen, configure the following settings. The options that are displayed on the **Details** screen depend on the configuration type you have selected in the **Proxy Configuration Type** drop-down menu.

-   **Basic Proxy Configuration Type**, enter the following information:

Setting	Description
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.
Relay Port	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 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.
Enable SSL Offloading	Select this check box if you want to use SSL Offloading to ease the burden of encrypting and decrypting traffic from the VMware Tunnel server.
Use Kerberos Proxy	To allow access to Kerberos authentication for your target back-end Web services, select the Kerberos proxy support This feature does not currently support Kerberos Constrained Delegation (KCD). The Endpoint server must be on the same domain as KDC for the Kerberos Proxy to communicate successfully with the KDC.

-   If you choose **Relay-Endpoint Proxy Configuration Type**, enter the following information:

Setting	Description
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://, and so on.
Relay Port	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.
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 must use different values.

Setting	Description
Enable SSL Offloading	Select this check box if you want to use SSL Offloading to ease the burden of encrypting and decrypting traffic from the VMware Tunnel server.
Use Kerberos Proxy	To allow access to Kerberos authentication for your target back-end Web services, select the Kerberos proxy support This feature does not currently support Kerberos Constrained Delegation (KCD).
	The Endpoint server must be on the same domain as KDC for the Kerberos Proxy to communicate successfully with the KDC.
	In the **Realm** text box, enter the Realm of the KDC server.

6 Select **Next**.

7 On the **SSL** screen, you can configure Public SSL Certificate that secures the client-server communication from the enabled application on a device to the VMware Tunnel. By default, this setup uses a AirWatch certificate for a secure server-client communication.

    a Select the **Use Public SSL Certificate** option if you prefer to use a third-party SSL certificate for encryption between Workspace ONE Web or SDK-enabled apps and the VMware Tunnel server.

    b Select **Upload** to 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.

8 Select **Next**.

9 On the **Authentication** screen, configure the following settings to select the certificates that devices use to authenticate to the VMware Tunnel.By default, all the components use AirWatch issued certificates. To use Enterprise CA certificates for the client-server authentication, select the **Enterprise CA** option.

    a Select **Default** to use AirWatch issued certificates. The default AirWatch issued client certificate does not automatically renew. To renew these certificates, republish 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.

    b Select Enterprise CA in place of AirWatch issued certificates for authentication between the Workspace ONE Web, 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.

    c Select the **Certificate Authority** and Certificate Template that are used to request a certificate from the CA.

    d Select **Upload** to 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.

10 Click Add to add an Intermediate Certificate.

11   Select **Next**.

12   On the **Miscellaneous** screen, you can use access logs for the proxy or Per-App Tunnel components. Enable the **Access Logs** toggle switch to configure the feature.

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 and configure advanced settings for VMware Tunnel.

a   Enter the URL of your syslog host in the **Syslog Hostname** field. This setting displays after you enable Access Logs.

b   Enter the port over which you want to communicate with the syslog host in the **UDP Port** field.

13   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.

14   On the **Configuration** screen, select the **General** tab. The **General** tab allows you to do the following:

a   You can select **Test Connection** to verify the connectivity.

b   You can select **Download Configuration XML** to retrieve the existing VMware Tunnel instance configuration as an XML file.

c   You can select the **Download Unified Access Gateway** hyperlink. This button downloads the non-FIPS OVA file. The download file also includes the PowerShell script and .ini template file for the PowerShell deployment method. You must download the VHDX or FIPS OVA from My Workspace ONE.

d   For legacy installer methods, you can select **Download Windows Installer**.This button downloads a single BIN file used for deploying the VMware Tunnel server. Configuration XML file required for installation can be downloaded from the Workspace ONE UEM console after confirming the certificate password.

15   Select **Save**.

Configure Advanced Settings for the VMware Tunnel Proxy

The **Advanced** on the Configuration screen lets you configure more settings that are optional for the VMware Tunnel Proxy. 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 settings.

Setting	Description
RSA Adaptive Auth Integration	Enable this setting if you want to integrate VMware Tunnel Proxy with the RSA authentication for a comprehensive Web browsing security.
Access Logs	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. In relay-endpoint deployments, the relay server writes the access logs and in a basic deployment, the basic server writes the access logs. There is no correlation between this syslog integration and the integration accessed on **Groups & Settings > All Settings > System > Enterprise Integration > Syslog**. This feature can be enabled during the initial configuration in the Advanced settings tab in the Workspace ONE UEMconsole. If configured after installation, you must reinstall VMware Tunnel. **Syslog Hostname**: Enter the URL of your syslog host and the UDP Port over which you want to communicate. Ensure that the logging level for access logs is set appropriately in rsyslog.conf on the syslog server. **UDP Port**: Enter the port over which you want to communicate with the syslog host. This setting displays after you enable Access Logs.
API and AWCM outbound calls via proxy	Enable this option if the communication 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, Workspace ONE Web) 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.
Authentication	Maintain your SSL certificates. If you are using AirWatch SSL, select **Regenerate** to regenerate the certificates.

3 If you are using a AirWatch certificate and not a public SSL certificate, then you can export the SSL certificate. Select **Export** if you choose to export the certificate.

4 Select **View Configuration XML** to view the configuration XML. You can also **Download** a local copy if required.

5   If applicable, configure the 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.

Table 6-1.

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 **Change** if you choose to change your password credentials.

6   Select **Save**.

Enable Kerberos VMware Tunnel Proxy Settings

Kerberos KDC Proxy is supported for the VMware Tunnel Proxy that 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.

Complete the following steps before you enable Kerberos VMware Tunnel Proxy Settings.

- For HTTPS sites, Workspace ONE Web for Android supports Kerberos authentication only when the site also has NTLM authentication enabled. This requirement is because the Android WebView, on which the Workspace ONE Web 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 Workspace ONE Web v2.5 and higher for Android.

Complete the following steps to enable Kerberos VMware Tunnel Proxy Settings:

1   During the configuration, check the box **Use Kerberos proxy** and enter the **Realm** of the KDC server.

2   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.

On Windows, once the VMware Tunnel Proxy is installed, you can see that a new Windows service called **AirWatch Kerberos Proxy** has been added.

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 VMware Tunnel Proxy Settings

You can configure Kerberos KDC Proxy for the proxy component. 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.

Complete the following steps to Configure Kerberos VMware Tunnel Proxy Settings:

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

2   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.

3   Complete the following settings to configure Kerberos proxy settings.

Table 6-2.

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

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 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.

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, 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.

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 use the Proxy Tool for PAC Files and Multiple Outbound Proxies.

Use the Proxy Tool for PAC Files and Multiple Outbound Proxies for VMware Tunnel Proxy

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.

Complete the following steps before you use the proxy Tool for PAC Files and Multiple Outbound Proxies for VMware Tunnel Proxy:

- To use the PAC file, edit the `proxy.properties` file and change the PROXY_SEARCH_STRATEGY to `2`.

- Uncomment the PAC_URL and enter the **PAC file URL** or the absolute path of the PAC file on the VMware Tunnel server.

Complete the following steps to use the Proxy Tool for PAC Files and Multiple Outbound Proxies for VMware Tunnel Proxy:

1 Within Linux CLI mode, navigate to **/opt/vmware/tunnel/proxy/tools**.

2 Convert the proxy tool to an executable file 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.
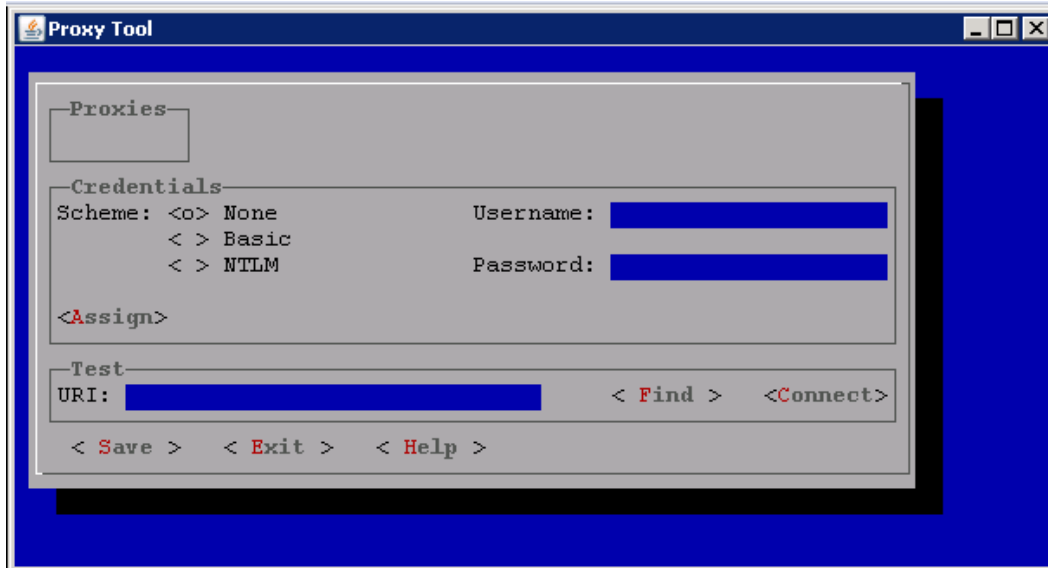
5 Select **Save**.

6 To restart the Proxy service, run the following command : `sudo systemctl restart proxy.service`.

   After saving, run the following command to check if the proxy settings is updated correctly:

```
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.

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.

Use SSL Offloading for the VMware Tunnel Proxy

Use SSL Offloading to ease the burden of encrypting and decrypting traffic from the VMware Tunnel server. Only the VMware Tunnel Proxy supports SSL Offloading. SSL Offloading and SSL re-encryption is not supported for the Per-App Tunnel because it uses SSL certificate pinning on the client and server side, creating an end-to-end encrypted tunnel. No SSL maniuplation is supported for the Per-App Tunnel because it 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 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, 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.
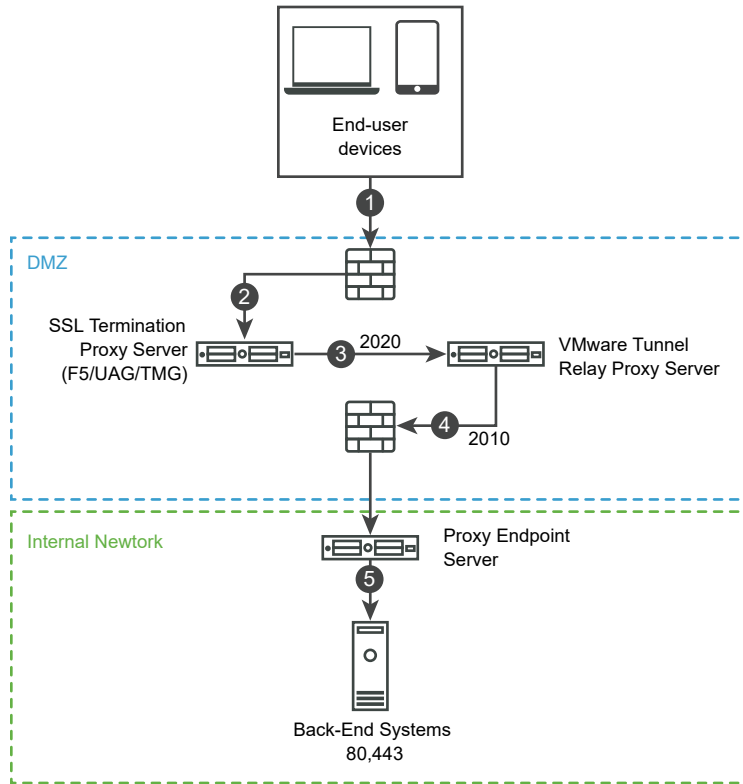
Note SSL offloading for basic configuration has communication from the SSL termination proxy going directly to the VMware Tunnel endpoint.

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.

VMware Tunnel Deployment with Unified Access Gateway

7

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 download the available Linux installer, go to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel Proxy**.

System Requirements for Deploying VMware Tunnel with Unified Access Gateway

Deploying VMware Tunnel with Unified Access Gateway, requires that your system meets a few hypervisor, software and hardware 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 6.0+ 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	DestinationComponent	Protocol	Port	Verification	Note
Devices (from Internet and Wi-Fi)	VMware Tunnel Proxy	HTTPS	2020*	After installation, run the following command to validate: `netstat –tlpn	grep [Port]`	1
Devices (from Internet and Wi-Fi)	VMware Tunnel Per-App Tunnel	TCP/UDP	8443*	After installation, run the following command to validate: `netstat –tlpn	grep [Port]`	1
Admin UI	Unified Access Gateway	TCP	9443		1

Table 7-1. VMware Tunnel Basic Endpoint Configuration

Source Component	DestinationComponent	Protocol	Port	Verification	Note

VMware Tunnel	AirWatch Cloud Messaging Server**	HTTPS	**SaaS:** 443
			On-Prem: 2001*
				`curl –Ivv https://`
				`<AWCM URL>:<port>/`
				`awcm/status`
				
				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
				`curl –Ivv https://`
				`<API URL>/api/mdm/ping`
				
				The expected response is `HTTP 401–unauthorized.`
					5

VMware Tunnel	Internal resources	HTTP, HTTPS, or TCP/UDP	80, 443, Any TCP/UDP	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

Table 7-2. VMware Tunnel Cascade Configuration

Source Component	DestinationComponent	Protocol	Port	Verification	Note
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 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
VMware Tunnel Back-End	AirWatch Cloud Messaging Server**	TLS v1.2	**SaaS:** 443 **On-Prem:** 2001*	Verify by using `whet` 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/UDP	80 or 443		4

Table 7-2. VMware Tunnel Cascade Configuration (continued)

Source Component	DestinationComponent	Protocol	Port	Verification	Note
VMware Tunnel Back-End	Internal resources	TCP/UDP	80, 443, Any TCP/UDP		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	`curl –Ivv https:// <API URL>/api/mdm/ping` The expected response is `HTTP 401–unauthorized.`	5

Table 7-3. VMware Tunnel Relay-Endpoint Configuration

Source Component	DestinationComponent	Protocol	Port	Verification	Note
VMware Tunnel Relay	AirWatch Cloud Messaging Server**	HTTP or HTTPS	**SaaS:** 443 **On-Prem:** 2001*	`curl –Ivv https://<AWCM URL>:<port>/awcm/status.` The expected response is `HTTP 200–OK.`	2
VMware TunnelEndpoint 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	`curl –Ivv https://<API URL>/api/mdm/ping` The expected response is `HTTP 401–unauthorized.` The VMware Tunnel Endpoint requires access to the REST API Endpoint only during the initial deployment.	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

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

Note Reference:

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.

- With a third NIC, external, internal, and management traffic all has their own subnets.

This chapter includes the following topics:

- Installing VMware Tunnel with Unified Access Gateway

- Configure VMware Tunnel Settings in the Unified Access Gateway UI

- Upgrade VMware Tunnel Deployed with Unified Access Gateway

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.

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.

Complete the following steps before you begin:

- Dedicated vSphere Admin Account with full privileges to deploy OVF

- Communication between the Windows machine used to deploy the OVA and your vSphere instance

- vSphere 6.0+.

- vSphere ESX host with a vCenter Server.

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

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.

Complete the following steps to install VMware Tunnel using vSphere

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, and 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 more information, see the Unified Access Gateway Documentation Center at Unified Access Gateway Documentation.

8   On the Select a Resource screen, select a location to run the template.

9 Select the storage and disk format options. When finished, select **Next**.

Table 7-4.

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.

10 Configure the **Network Mapping** settings. Enter the vSphere network names. The network protocol profiles associated with every referenced network name determine the DNS servers, gateway, and subnet mask. If it is absent, you must enter the values in the next step. When finished, select **Next**.

11 Configure the **Properties** settings.

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

- 1 Customize the **Network Properties** as they relate to your VMware Tunnel network configuration.

  2 Configure the password for the root user of the VM.

  3 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 If you do not properly follow the password requirements, 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.

  4 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.

Complete the following steps to configure the vSphere .INI Template:

1. Download the Unified Access Gateway Using vSphere ZIP from Workspace ONE UEM Resources. Workspace ONE UEM Resources are available at https://resources.air-watch.com/view/sbfsfykltpqfxhvg9tpy/en.

2. Download the Unified Access Gateway Using vSphere ZIP from Workspace ONE UEM Resources.

3. Unzip the file and locate the template.ini file.

4. Right click the file and select **Open With**. Select notepad or your preferred file editor.

5. Configure the template.ini settings.

Settings	Descriptions
name=<VIRTUAL_MACHINE_NAME>	Enter the Unified Access Gateway unique name. 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
target=vi:// <USERNAME>:PASSWORD@<VSPHEREDOMAIN>/ <LOCATION/TO/PLACE/APPLIANCE/IN/VSPHERE>	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. Example: target=vi:// admin@vmware.com:PASSWORD@vsphere.com/ MyMachines/host/Development/Resources/ MyResourcePool

Settings	Descriptions
deploymentOption=<NUMBER_OF_NICS> dns=<DNS_IP> ip0=<NIC1_IP_ADDRESS> ip1=<NIC2_IP_ADDRESS> ip2=<NIC3_IP_ADDRESS>	Enter the number of Network Interface Controllers you want to associate with the appliance for your deployment configuration. Your options are: ■ onenic ■ twonic ■ threenic Then enter the address for each NIC you are using. Delete the excess lines if you are not using all three. The different IP addresses entered change based on your NIC settings. ■ 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. For best results, consult your network admins. Example: deploymentOption=threenic 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.
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. If you are not using network profiles, manually enter the netmask or prefix for the respective NICs and the IPv4/IPv6 default gateway.This specifies network settings such as IPv4 subnet mask, gateway etc.
netmask0=<NIC1_NETMASK> netmask1=<NIC2_NETMASK> netmask2=<NIC3_NETMASK>	Enter the subnet mask for the networks added when configuring the **netInternet**, **netManagementNetwork**, and **netBackendNetwork** settings.
defaultGateway	Enter the gateway for the network added when configuring the **netInternet** setting.
honorCipherOrder=<true_or_false>	Enter true to force the TLS cipher order to be the order specified by the server.
tunnelGatewayEnabled=<true_or_false>	Enter true if you are using the VMware Tunnel- Proxy. Example: tunnelGatewayEnabled=true
apiServerUrl=<API_SERVER_URL>	Enter the API server URL.To find the URL, navigate to **Groups & Settings** > **All Settings** > **Advanced** > **Site URLs** > **REST API 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 privleges.

Settings	Descriptions
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 to use these proxy settings as the outbound proxy for your VMware Tunnel - Proxy deployment.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 multple trusted certificates. Increase the for each entry. For example, trustedCert2, trustedCert3, and so on. This field is commented out by default.

6   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.

Complete the following steps to configure the Hyper-V .INI Template:

1   Download the Unified Access Gateway Using Hyper-V ZIP from Workspace ONE UEM Resources.Workspace ONE UEM Resources are available at 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
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
deploymentOption=<NUMBER_OF_NICS> dns=<DNS_IP> ip0=<NIC1_IP_ADDRESS> ip1=<NIC2_IP_ADDRESS> ip2=<NIC3_IP_ADDRESS>	Enter the number of Network Interface Controllers you want to associate with the appliance for your deployment configuration. Your options are: ■ onenic ■ twonic ■ threenic Then enter the address for each NIC you are using. Delete the excess lines if you are not using all three. The different IP addresses entered change based on your NIC settings. ■ 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. For best results, consult your network admins. Example: deploymentOption=threenic 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.
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>	Enter the virtual switch names. A virtual switch must to be created for the referenced networks.
netmask0=<NIC1_NETMASK> netmask1=<NIC2_NETMASK> netmask2=<NIC3_NETMASK>	Enter the subnet mask for the networks added when configuring the **netInternet**, **netManagementNetwork**, and **netBackendNetwork** settings.
defaultGateway	Enter the gateway for the network added when configuring the **netInternet** setting.
honorCipherOrder=<true_or_false>	Enter true to force the TLS cipher order to be the order specified by the server.

Settings	Descriptions
tunnelGatewayEnabled=<true_or_false>	Enter true if you are using the VMware Tunnel - Proxy. Example: tunnelGatewayEnabled=true
apiServerUrl=<API_SERVER_URL>	Enter the API server URL.To find the URL, navigate to **Groups & Settings** > **All Settings** > **Advanced** > **Site URLs** > **REST API 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 privleges.
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 to use these proxy settings as the outbound proxy for your VMware Tunnel - Proxy deployment.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 multple 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.

Configure the INI file to pass the VMware Tunnel configuration to the OVA file.

The following tools are required:

- 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)

- 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 Hypervisor:

  - vSphere v5, 5.1, 5.5, or 6 - vSphere ESX host with a vCenter Server

  - Microsoft Hyper-V - Windows Server 2012 R2 or Windows Server 2016

Complete the following steps to run the VMware Tunnel PowerShell Script:

1 Open PowerShell as an administrator.

2 Navigate to the folder containing your PowerShell script and modified .ini template.

3 Enter the following command: .

   a For vSphere deployments: .\uagdeploy.ps1 <Ini file name>

   b For Hyper-V: .\uagdeployhv.ps1 <Ini file name>

   ```
   .\uagdeploy.ps1 AWTunnel.ini
   ```

4   Enter the password for each prompt:

Setting	Description
Appliance Password	Enter password for the root user.
REST API	Enter the admin UI password.
API server password	Enter the API server password.
Outbound proxy	Optional. If using a proxy with authentication, enter outbound proxy.
vSphere User password	If using vSphere, enter the 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.

Procedure

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.
API Server URL	Enter the URL to your Workspace ONE UEM API server. To find the URL, navigate to **Groups & Settings > All Settings > Advanced > Site URLs > REST API URL**. 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 you 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- Proxy deployment.

Settings	Description
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 (Optional) On the Support Settings screen on this page, download the **Log Archive** and export your custom settings using the **Export Access Point Settings** option.

10 To finish, select **Save**.

Results

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.

The Unified Access Gateway appliance supports a Zero Downtime Upgrade process. For more information, see the Unified Access Gateway Documentation.

Upgrade VMware Tunnel Deployed with Unified Access Gateway Using vSphere

Complete the following steps to Upgrade VMware Tunnel Deployed with Unified Access Gateway 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.Workspace ONE UEM Resources are available at 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.

6 Instead of manually configuring the settings, select **Import Settings**.

7   Browse for the downloaded export JSON file.

8   Select **Import**.

Upgrade VMware Tunnel Deployed with Unified Access Gateway using the PowerShell Script

You can upgrade VMware Tunnel deployed with Unified Access Gateway using the PowerShell Script.

1   Download the new OVA package from Workspace ONE UEM Resources.Workspace ONE UEM Resources are available at Download Unified Access Gateway.

2   Use the same .ini template from your previous deployment with the PowerShell script.

3   Run the VMware Tunnel PowerShell Script.

VMware Tunnel Deployment on a Linux Server

8

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 download the available Linux installer, go to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel Proxy**.

System Requirements for Deploying VMware Tunnel on a Linux Sever

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
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 7.x	(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 : `sudo yum —y install openssl` Haveged: `sudo yum —y install haveged*` Nscd: `sudo yum —y install nscd` Json-c: `sudo yum —y install json—c` libxml2: `sudo yum —y install libxml2` log4cpp: `sudo yum —y install log4cpp*` protobuf :`sudo yum —y install protobuf*`
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.
(Optional) SSL Certificate from a trusted third party	Workspace ONE UEM certificates are automatically generated by default as part of your Tunnel configuration. Alternatively, you can upload the full chain of the public SSL certificate to the Workspace ONE UEM console during configuration. Ensure that the SSL certificate is trusted by all device types being used. (that is, not all Comodo certificates are natively trusted by Android). SAN certificates are not supported. 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. If your SSL certificate expires, then you must reupload the renewed SSL certificate and redownload and rerun the installer.
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 -tlpn https:// <VMware_Tunnel_Host > :<port >**	1
Devices (from Internet and Wi-Fi)	VMware Tunnel Per-App Tunnel	TCP/UDP	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
VMware Tunnel	Internal Web sites / Web apps	HTTP or HTTPS	80 or 443		4
VMware Tunnel	Internal resources	HTTP, HTTPS, or TCP/UDP	80, 443, Any TCP/UDP		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	`curl –Ivv https://<API URL>/api/mdm/ping` 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

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 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/UDP	80 or 443		4
VMware Tunnel Back-End	Internal resources	TCP/UDP	80, 443, Any TCP/UDP		4
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	`curl –Ivv https://<API URL>/api/mdm/ping` 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	`curl –Ivv https://<API URL>/api/mdm/ping` 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.

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.

This chapter includes the following topics:

- Single-Tier VMware Tunnel Installation
- Multi-Tier VMware Tunnel Installation
- Upgrade VMware Tunnel Deployed on a Linux Server
- Uninstall VMware Tunnel
- Migrating to VMware Tunnel

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

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:
```

3 Press **Enter**.

4 Read and accept the licensing agreement by entering '**y**'.

5 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: █
```

■

- ■ Provide API Server information.

    a Enter the following information. After entering each value, the system dialog asks you to confirm the entry.

        ■ Workspace ONE UEM API URL

        ■ Organization Group Code

        ■ Console Server Username

        ■ Console Server Password

    b Enter the hostname of the Tunnel server.

> The installer chooses the components to install based on the Workspace ONE UEM console configuration.

  c Press **Enter**.

- 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.

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: █
```

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

Results

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

Multi-tier installation requires the installation of two or more servers. Before you begin a multi-tier installation, review your architecture.

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.

Complete the following steps before you install the VMware Tunnel Front-End Server (Linux):

- 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.

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.

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.

2   Once on the Linux server, navigate to the folder you copied the file to and then run the BIN file by using the required 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:
```

3   Press **Enter**.

4   Read and accept the licensing agreement by entering '**y**'

5   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.

  ■   Workspace ONE UEM API URL

  ■   Organization Group Code

  ■   Console Server Username

  ■   Console Server Password

b   Enter the hostname of the Tunnel server.

    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: ▌
```

   c   Press **Enter**.

   d   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.

   b   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.

      1   If they have been modified, rename the files to match these names when copied into the common directory on the Linux server.

      2   If you are installing one of the Tunnel services, copy the respective configuration file.

   c   Enter the directory path that contains both configuration files.

   d   Enter the certificate password for both configuration files when prompted.

6   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.

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: █
```

9   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.

Install the VMware Tunnel Back-End Server (Linux)

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.

■   Download the installer onto the server. The link inS 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.

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. Press **Enter**.

```
$ 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:
```

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

    1   Enter the following information. After entering each value, the system dialog asks you to confirm the entry.

        - Workspace ONE UEM API URL

        - Organization Group Code

        - Console Server Username

        - Console Server Password

    2   Enter the hostname of the Tunnel server.

        The installer chooses the components to install based on the Workspace ONE UEM console configuration.

    3   Press **Enter**.

- Option 2: Import Config.xml file

    1   Download and copy the Tunnel Proxy and Per-app VPN configuration files to a single directory on the server.

    2   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.

> 3 Enter the directory path that contains both configuration files.

> 4 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: 
```

9 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.

Prerequisites

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 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.

Procedure

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 installing VMware Tunnel Front-End Server or Back-End Server.

Results

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

Uninstall VMware Tunnel

Uninstall VMware Tunnel from your servers when needed. The uninstallation process is simple.

This method of uninstallation only applies to servers installed using the legacy installer workflow and not servers install with the Unified Access Gateway workflow. Perform the following steps on your VMware Tunnel servers to remove the component.

Procedure

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.

Migrating to VMware Tunnel

The sample scenarios described in this chapter offer a few different possibilities for migrating to VMware Tunnel .These scenarios are general examples and might not exactly capture your situation, it is expected that VMware Tunnel can be implemented with little to no downtime for users.

Migrating from a Third-Party Full Device VPN to Per-App VMware Tunnel

As VMware Tunnel is a per-app VPN provider, it always take precedence over full-device VPNs configured on the device. Once VMware Tunnel is configured on the device, it is recommended to remove all the other configurations.

Migrating from a Third-Party Per-App VPN to Per-App VMware Tunnel

If you are using another per-app VPN provider, then all the applications need to be migrated over from the previous provider to VMware Tunnel.Once VMware Tunnel is configured and the profiles are pushed to the devices, you can flip the assignment to switch users from the previous VPN provider to VMware Tunnel.

Migrating from Proxy App Tunnel to Tunnel SDK

If you are migrating from VMware Tunnel- Proxy to Tunnel SDK (Per-App Tunnel) and want to retain the domains that are configured for tunneling, then configure the same domains in the Device Traffic Rules for VMware Tunnel. For more information, see Configure App Tunnel for the Default SDK Profile.

VMware Tunnel Management

9

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 deployment:

- RSA authentication controls access to internal resources through two-factor authentication.

- Configure to rotate public SSL certificates to maintain the end-user service experience.

- Use Workspace ONE Web to control how the end users access internal sites by configuring communication between the application and VMware Tunnel.

This chapter includes the following topics:

- Deploying Per-App Tunnel to devices

- VMware Tunnel SSL Certificate Life Cycle Management

- Integrating VMware Proxy Tunnel with RSA

- Using VMware Tunnel with Workspace ONE Web and other SDK-Built Apps

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 creating a VPN profile for your end-user devices. These profiles depend on your device platform. After you create a VPN profile, push the profiles and the apps to the devices. 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.

Application Configurations

Note Application configurations are key-value pairs that you deploy with the application to preconfigure features for users. You can enter supported pairs when you upload applications to the Workspace ONE UEM console and you can code them into your applications.

Currently, application configurations are available for Android and iOS. You must know the supported key-value pairs for your application to deploy them and to code them. To find supported application configurations, review the listed resources.

The application vendor sets the supported configurations for the application, so you can contact the vendor or visit other sites with information about application configurations.

- To find the supported application configurations, contact the application vendor.

- See these resources with information about application configurations.

  - AppConfig Community at https://www.appconfig.org/

  - VMware Workspace ONE UEM Developers at https://code.vmware.com/web/workspace-one.

The Workspace ONE UEM knowledge base has articles about working with application configurations when you develop applications. See Workspace ONE UEM Managed App Configuration at https://support.air-watch.com/articles/115006248807.

Privacy Dialog

VMware Workspace ONE Tunnel supports a privacy dialog that displays information regarding the application an admin configures. VMware Workspace ONE Tunnel only supports the privacy dialog for iOS and Android devices. You must deploy the VMware Workspace ONE Tunnel app to devices using Application Configurations during device assignment.

The dialog displays the following information to end users:

Table 9-1. Privacy Dialog Information

Information	Description
Data collected by the application	Provides a summary of data which is collected and processed by the application. Some of this data will be visible to administrators of theWorkspace ONE UEM console.
Device permissions	Provides a summary of device permissions requested for the app to enable product features and functionality, such as push notifications to the device.
Company's privacy policy	Enables administrators to display a customized privacy notice to their users through a configurable URL. If no privacy notice is provided, a default message will be shown to the user to contact their employer for more information.

Admin Configuration Settings

To configure the privacy dialog for VMware Workspace ONE Tunnel on iOS and Android devices, you must deploy the VMware Workspace ONE Tunnel app to your devices with Application Configurations.

You must use the following key-value pairs:

Table 9-2. VMware Tunnel Privacy Dialog Key-Value Pairs

Configuration	Key-Value Pair
Company Privacy Policy URL	- Key:`PrivacyPolicyLink` - Value Type: **String** - Values: `https://www.company.com/privacypolicy` This policy changes the default company privacy policy text to allow the user to view a specific privacy disclosure web page directly within the application
VMware Feature Usage Analytics	- Key:`PolicyAllowFeatureAnalytics` - Value Type: **Integer** - Values: `0` - Disabled `1` - Enabled This policy controls whether end users will see the **Data Sharing** opt-in during configuration of the apps. When disabled, data sharing is forced off for all users. Feature analytics data is collected to allow VMware to improve existing product features and invent new ones to make users even more productive
Diagnostics Data through VMware Intelligence and Apteligent	- Key: `PolicyAllowCrashReporting` - Value Type: **Boolean** - Values: `false` - Disabled `true` - Enabled This policy controls whether applications will report diagnostic data to Apteligent which is used to provide troubleshooting and support, for example, in the event of a crash. Disabling this setting may significantly impact the efficiency of investigating and resolving any issues with the application.

Example Configuration:

```
{"PolicyAllowFeatureAnalytics":1,
"PrivacyPolicyLink":"https://www.company.com/privacypolicy",
"PolicyAllowCrashReporting":true}
```

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.

Procedure

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 **Workspace ONE 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 iOS

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

Procedure

1 Navigate to **Devices > Profiles & Resources > 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 **Workspace ONE 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 Workspace ONE 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 Workspace ONE 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 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.

Complete the following steps before you Configure Per-App Tunnel Profile for macOS

1 Cofigure VMware Tunnel.

2 Configure Network Traffic Rules for Safari Split Tunneling.

3 Deploy VMware Tunnel.

Complete the following steps to configure Per-App Tunnel Profile for macOS:

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 **Workspace ONE 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.

7 Select **Save & Publish**.

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.

1 On a macOS device, find the file path for the app you want to flag for Per-App Tunnel./
   `Applications/Google\ Chrome.app/`

   Note

   Extracting the macOS Bundle ID for Per-App Tunnel does not work with the native MacOS system applications if the Application Bundle ID begins with com.apple.* on macOS 10.14 or later.

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
```

5   Copy the Application Bundle ID from the output.The Bundle ID follows identifier. In the
above example it is com.google.Chrome.

6   Run the following command to get the Designated Requirement.codesign —d —r— /
Applications/Google\ Chrome.app/

7   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")
```

8   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")
```

9   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.

Settings	Description
Application Bundle ID	com.google.Chrome
Designated Requirement	(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")

Configure VPN Profile for Workspace ONE Tunnel Universal Windows Platform (UWP) app

Configure VPN Profile for Windows platform (UWP) app to allow 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

1   Navigate to **Devices > Profiles > List View > Add** and select **Windows**. Then select **Windows Desktop** and **User Profile** or **Device Profile**.

2   Configure the profile's **General** settings.

3   Select the **VPN** payload from the list.

4   Enter a **Connection Name** and select **Workspace ONE 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.
	This feature only displays if the profile is set to Device context.
Trusted Network Detection	Enter comma separated trusted networks (For example,acme.com, abc.net and so on). Tunnel fails to connect when the device is on a trusted network.
DNS Resolution via Tunnel Gateway	In the DNS Resolution via Tunnel Gateway section, select **Add New Domain** to add domains to resolve through the VMware Tunnel server.
	Any domains added resolve though the VMware Tunnel server regardless of the app originating the traffic. For example, vmware.com will resolve through theVMware Tunnel server if you use the whitelisted Chrome or the non-whitelisted Edge apps.

7   Select **Save & Publish**.

Configure VPN Profile for Workspace ONE Tunnel Windows Desktop Application

Configure VPN Profile for Windows desktop applications for 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.

Prerequisites

The VMware Tunnel client for Windows Desktop requires that devices are enrolled in Workspace ONE UEM and have the Workspace ONE Intelligent Hub installed.

Procedure

1   Navigate to **Devices > Profiles > List View > Add** and select **Windows**. Then select **Windows Desktop** and **Device Profile**.

2   Configure the profile **General** settings.

3   Select the **VPN** payload from the list and select **Configure**.

4   Enter the **Connection Name** and select **Workspace ONE 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 the **Device Traffic Rules** created under the tunnel configuration page. For more information, see Configure Network Traffic Rules for the Per-App Tunnel.

6   Enable the **Desktop Client**.

7   Enter the XML code in the **Custom Configuration XML** text-box. You can set the following attributes based on your requirements:

Settings	Description
TrustedNetworkProbeUrl	You can use this attribute to detect if your device is connected to a trusted network, based on your device's ability to reach a private URL. You can specify a comma-separated list for redundancy.
DnsSearchDomain	You can use this attribute for resolving shortnames by using the search domains.
ServerCertSN	You can use this attribute for setting a third-party certificate for the server authentication. If you do not know your subject CN name, you can open the certificate on the Windows device and go to the **Details** tab. You can find a row named Subject which contains the CN name of the certificate.
StartTunnelPreLogon	Use this attribute to enable the Tunnel service to start before you login. This may be useful for specific domain authentication scenarios.

For example, you can enter the following XML code in the **Custom Configuration XML** text box.

```
<?xml version="1.0" encoding="utf-16"?>
<CustomConfiguration>
<TrustedNetworkProbeUrl>http://probeurl</TrustedNetworkProbeUrl>
<ServerCertSN>SubjectNameofCertificate</ServerCertSN>
<DnsSearchDomain>domainname</DnsSearchDomain>
</CustomConfiguration>
```

8   Configure the network settings for Tunnel.

Settings	Description
Trusted Network Detection	Enter comma-separated trusted networks (For example, acme.com, abc.net). VMware Tunnel is disabled when the device is on a trusted network.
	Note Alternatively from the Probe URL, trusted networks can be detected based on DNS connection-suffix. Probe URLs takes precedence over connection suffixes, and the Probe URL is the primary recommendation.
DNS Resolution via Tunnel Gateway	**Enhanced Domain Resolution**:
	If enabled, all the domains resolve though the VMware Tunnel server based on destination defined in the device traffic rule regardless of the application originating the traffic.
	Note This option is supported only on Windows Tunnel Desktop client 2.1 and above.
	Domain / Add New Domain: In the **DNS Resolution viaTunnelGateway** section, select **Add New Domain** to add domains to resolve through the VMware Tunnel server.
	Any domains added resolve though VMware Tunnel server regardless of the application originating the traffic. For example, `vmware.com` resolves through the VMware Tunnel server if you use Chrome's allow list or the deny list from the Edge application.
	Note If the Enhanced domain Resolution option is enabled, this option is hidden.

9   Select **Save & Publish**.

Note   If you are migrating your devices from the Windows UWP client to the Windows desktop client, we recommend that you remove the previous VMware Tunnel profile and application once the new profile has propagated to devices.

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.

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.

Procedure

1   Navigate to **Apps & Books > Applications > Native**.

2   Select the **Public** tab.

3   Select **Add Application** to add an app or **Edit** an existing app.

4   On the Deployment tab, select **Use VPN** and then select the profile you created.

5   Select **Save** and publish your changes.

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.

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.

Procedure

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.

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. 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.

Note   The certificate is pushed to the Unified Access Gateway front end only after you save the API settings on the front-end UEM console.

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

2   Select **Edit** to change the configuration settings.

3   In the **Server Authentication** section, you can configure Third Party SSL Certificate that secures client-server communication from enabled application on a device to the VMware Tunnel. By default, this setup uses a **AirWatch** certificate for secure server-client communication.

   a   Select **Third Party** option if you prefer to use a third-party SSL certificate for encryption between Workspace ONE Web or SDK-enabled apps and the VMware Tunnel server.

   b   Select **Add Certificate** to 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.

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 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

- Workspace ONE Web for iOS v4.5+

- Workspace ONE Web for Android v3.1+

- VMware AirWatch Software Development Kit for iOS v5.5+

- VMware AirWatch Software Development Kit for Android v15.11+

Integrate VMware Tunnel with RSA Authentication

Note 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.

2 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.

3 Select **Save**.

Using VMware Tunnel with Workspace ONE Web and other SDK-Built Apps

Using Workspace ONE Web 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 Workspace ONE Web) goes through the VMware Tunnel.

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

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.

Procedure

1 Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.

2 Select **Enabled** for **AirWatch App Tunnel** and specify the **App Tunnel Mode** as **VMware Tunnel – Proxy**.

3   (Optional) Enable the split tunnel for iOS devices by entering URLs into the **App Tunnel Domains** text box. Leave the text box empty to send all requests through the VMware Tunnel.

   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.

4   Select **Save**.

5   Ensure the Workspace ONE Web is using the Shared SDK profiles for iOS and Android by navigating to **Groups & Settings > All Settings > Apps > Workspace ONE Web** and selecting them under **SDK Profile**.

Health Monitoring and Testing VMware Tunnel

10

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.

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.

Important   You must enable access logs before you install any of the components. Any changes you make to the access logs configuration on the Workspace ONE UEM console require reinstallation of the VMware Tunnel server.

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.

■ VPN Statistics Report to get statistical information about the number of connected devices, downstream traffic , service synchronization time and so on.

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. Complete the following steps to Run VPN Whitelist Report:

1 Navigate to the `vpnd`folder.

2 Run the `./vpnreport whitelist` as root.

3 (Optional) Run the commands that are supported by the VPN report.

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

You can add `--json` to create a JSON output and `--text` to create a text output.

Here's a screen shot that shows the visual representation of the usage statistics about the number of connected devices, downstream traffic, service synchronization time and so on:
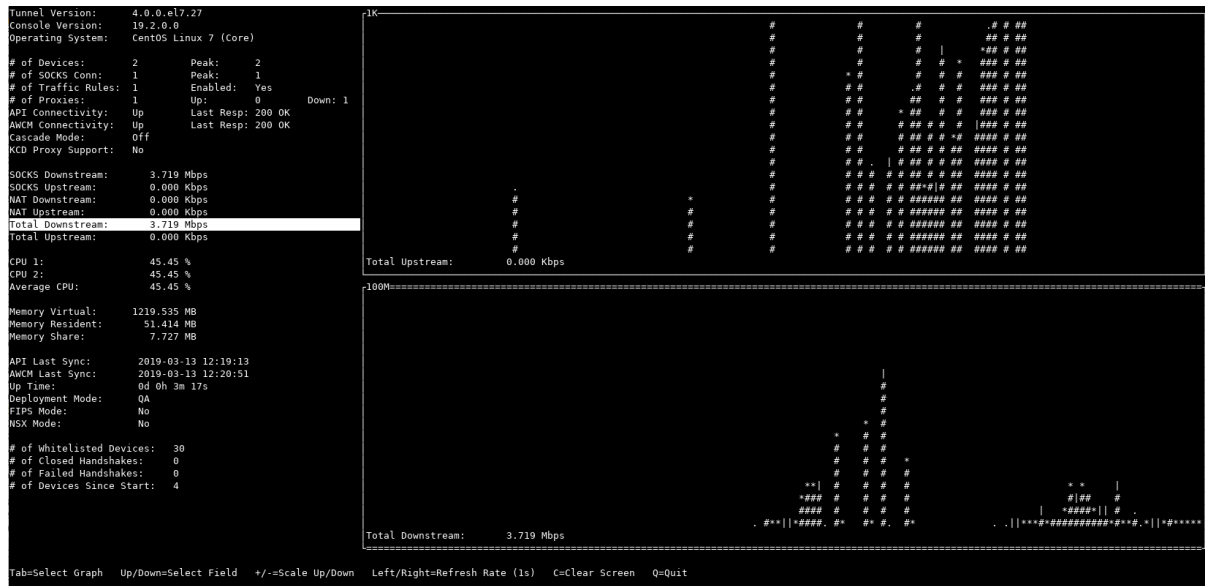
You can use the following menu options while working with the report:

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

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	#

VMware Tunnel Troubleshooting and Support

11

VMware Tunnel Troubleshooting and support section helps you resolve some of the VMware Tunnel deployment issues.

Troubleshooting VMware Tunnel 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:

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:

- awcm.dat

- ca.pem

- device.xml

- dh2048.pem

- server.conf

- tunnel_init.log

- tunnel.log

- tunnel.log.1

- version.info

- vpn.dat

`/opt/vmware/tunnel`

Use the following command to run the utility:

`sudo ./tunnel_snap.sh`

The utility collects the diagnostic data in:

_/opt/vmware/tunnel/tunnel_snap.tar _

Troubleshooting VMware Tunnel using the UAG web UI

The UAG web UI offers a simple way to check the service availability and collect all the UAG log files that includes the Tunnel and Proxy log files.

1   Click the Read more section that can assisit you with the troubleshooting.Monitoring Edge Services Status:

    Expand the **Edge Services** section and find VMware Tunnel. If the Tunnel is running as expected, it shows a green light on the left side of the service. Any other color indicates that either the service is not running, or is running with errors and requires further investigation.

    Collecting Logs from the Appliance:

    Download a .zip archive of logs from the **Support Settings** section of the Admin UI. These log files are collected from the /opt/vmware/gateway/logs directory on the appliance.

2   To check if the Tunnel and the Proxy services are installed correctly, always review the appliance-agent.log. The log displays the following information:

    `[main] INFO c.a.a.a.s.i.tunnel.TunnelInstaller — VMware Tunnel Proxy installation SUCCESS!!!! and/or [main] INFO c.a.a.a.s.i.tunnel.TunnelInstaller — VMware Tunnel Per—App Tunnel installation SUCCESS!!!!`

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.

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.`sudo rpm —1 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 Tunnel Component

Per-App Tunnel logs are stored in the native syslog system of Linux. This topic covers the commnans that can be used to troubleshoot Per-App Tunnel Component

Troubleshooting Proxy Tunnel Component

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
```

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

Commands Used to Troubleshoot Per-App Tunnel Component

Component	Function	Command
Unified Access Gateway/CentOS/RHEL 7.x	Start the Service	`systemctl start vpnd.services`
Unified Access Gateway/CentOS/RHEL 7.x	Stop the Service	`systemctl stop vpnd.service`
Unified Access Gateway/CentOS/RHEL 7.x	Restart the Service	`systemctl restart vpnd.service`

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.

Troubleshooting PAC Reader

If you have any issues with the VMware Tunnel PAC Reader, check the status and the logs of the PAC Reader to help troubleshoot any issues.

Before contacting Workspace ONE UEM Support, consider checking the PAC Reader logs for any issues. The logs are located in the home folder of the PAC Reader. This folder is the pacreader folder.

The following table lists the commands that are used to troubleshoot PAC Reader:

Function	Command
Start the PAC Reader	`./pacreader.sh start`
Stop the PAC Reader	`./pacreader.sh stop`
Check the PAC Reader status	`/pacreader status`
Run the PAC Reader in validation mode	`./pacreader.sh validate` This command tells the PAC Reader to fetch and parse the PAC file but does not push the rules to the Workspace ONE UEM console.

Troubleshooting Proxy Tunnel Component

Proxy logs are stored in the native syslog system of Linux. The topic covers the commnads that are used to Troubleshoot Proxy Tunnel Component.

Commands Used to Troubleshoot Proxy Tunnel Component

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
```

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	`sudo service proxy start`
Proxy – Any CentOS/RHEL version/Virtual Appliance	Stop the Service	`sudo service proxy stop`
Proxy – Any CentOS/RHEL version/Virtual Appliance	Restart the Service	`sudo service proxy status`

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 the Log Level of VMware Tunnel Proxy Component

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.

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 VMware Tunnel Proxy Connectivity

1   Navigate to **Groups & Settings** > **All Settings** > **System** > **Enterprise Integration** > **VMware Tunnel - Proxy**.

2   Select **Test Connection**.The page displays version info, connectivity through HTTP/S, and certificate chain validation.

Proxy Component Error Codes

You can use error codes and their messages to help monitor the health of your VMware Tunnel Proxy component. Learn more about the errors using their code, displayed name, and meaning to your Workspace ONE UEM Tunnel Proxy environment.

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 application. **Possible Solution:** select all hops between the device and VMware Workspace ONE 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 application. **Possible Solution:** select all hops between the device and VMware Workspace ONE Tunnelto 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 alg:%s;uid:%s;bundleid:%s 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 application. **Possible Solution:** select all hops between the device and VMware Workspace ONE 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:** select 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 Workspace ONE 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.
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 Workspace ONE Tunnel is configured. **Possible Solutions:** (1) Override the Workspace ONE UEM device root certificate and regenerate the VMware Workspace ONE Tunnel certificate. (2) Export the Workspace ONE UEM certificate from the Console or reinstall the VMware Workspace ONE Tunnel.

Code	Name	Meaning
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). Rerun the VMware Workspace ONE 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 Workspace ONE 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 Workspace ONE Tunnel. Any method other than the "CONNECT" request is sent to the VMware Workspace ONE Tunnel and is rejected. **Possible Cause:** An invalid request. **Possible Solution:** select 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 Workspace ONE Tunnel even after making an API call. No data available for Udid: #####, BundleId: ####. **Possible Cause:** VMware Workspace ONE Tunnel does not have device details. **Possible Solutions:** Check the VMware Workspace ONE Tunnel to API connection. Restart the VMware Workspace ONE 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 Workspace ONE Tunnel is different. Invalid SHA-1 thumbprint. Udid: ####, BundleId: ####. VMware Workspace ONE Tunnel expected: XYZ, Found:ABC Possible Cause: Occurs only when device is re-enrolled. **Possible Solutions:** Reinstall the Client (AWB, Wrapped application). Select the VMware Workspace ONE Tunnel to AWCM connection. Restart VMware Workspace ONE Tunnel Service.
15	NOT_COMPLIANT	The device making the request is not compliant (Must be in compliance states of 'Compliant' or 'Not Available'). **Possible Cause:** VMware Workspace ONE Tunnel expected: X,Y, Found: Z **Possible Solution:** select 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

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

This chapter includes the following topics:

■ [Troubleshooting Common Errors while working with VMware Tunnel](#)

Troubleshooting Common Errors while working with VMware Tunnel

This section covers common error messages that you may encounter while working with VMware Tunnel and the procedure to fix the root cause of the problem.

Device configuration error

When the Tunnel VPN profile is not installed on the device, end users might see `Device Not Configured` when they try to open a Tunnel client.

1   In the UEM console , navigate to the **Device Detail** page of the affected device and click the **Profiles** tab to confirm if the Tunnel VPN profile is installed.

2   For all the Android devices, open the Workspace ONE Intelligent Hub and under the **Profiles** section, check if the Tunnel VPN profile exists.

3   For all iOS devices, navigate to **Settings** > **VPN** and verify the VPN configuration details.

TLS Handshake Failure

You encounter this error if the SSL certificate present on the device does not match with the certificate on the server or if the certificate is not valid.

1   In the UEM console, navigate to the Tunnel configuration page and verify the Front-End Certificate Thumbprint under server **Authentication**.

2   For all the Android devices, open the Workspace ONE Intelligent Hub and under the **Profiles** section, verify the certificate thumbprint for the `Type.cer`.

    a   For all the iOS devices, navigate to **Settings** > **General** > **Device Management** > **Device Manager**.

    b   Click **More Details** and under the **Certificate** section, click the certificate with the Tunnel hostname.

3   Scroll down to the **SHA-1** text box and verify the certificate thumbprint.

4   On the server side, open `/opt/vmware/tunnel/vpnd/server.conf` and search for `ssl_thumbprint`.

5   Verify if the thumbprint on the device, server, and the UEM console is the same. If not, restart the `vpnd` service on the UEM console and republish the VPN profile.

DNS Resolution Failure

You might encounter DNS resolution error if the Tunnel server FQDN does not get resolved to an IP address.

1   From the device connected network,ensure that the Tunnel server FQDN resolves to an IP address.

2   In the command prompt, enter the following command: `nslookup <Tunnel_Server_FQDN>`. Tunnel server FQDN resolves to an IP address.

Unable to Reach the Tunnel Gateway

You may not be able to reach the Tunnel gateway if device is unable to communicate with the Tunnel server on the mentioned port.

1   From the device connected network, ensure that the device connects to the Tunnel server on the port that is mentioned in the tunnel configuration.The device must get connected and display the Tunnel server Front-end SSL certificate.

2   In the command prompt, enter the following command:

```
openssl s_client -connect <dest_fqdn>:<port> -servername
        <server_fqdn>
```

.

3   In the Tunnel server, enter the following command: `netstat -tlpn`

The server must display the port that is mentioned in the tunnel configuration.

4   In the Tunnel server, enter the following command: `systemctl status vpnd`. The service must be active and running.

Note

▪   Verify the Firewall and the load balancer rules.

▪   SSL Offloading and SSL Bridging are not supported for the Per-App Tunnel component.

Access Denied Error

You might encounter access denied error if the device details are not present on the Tunnel server or when the device is non-compliant.

1   Open the Workspace ONE Intelligent Hub and verify the complaince status.

2   Navigate to the Device detail page for the affected device and verify the device complaince status.

3   From the /opt/vmware/tunnel/vpnd directory, run `./vpnreport whitelist --udid=<Device_udid>`.In the result xml, the `ComplianceStatusId` must be 3 or 5 for the affected device UUID.

> **Note** The connection between the Tunnel server and the API server connection must be successful to achieve the expected result.

No Apps Assigned

You might encounter the `No Apps Assigned` error within the Workspace ONE tunnel application when the managed application is not mapped with the VMware VPN profile.

- Navigate to the internal or the public application under **Apps & Books** and check for the device in the assignment group where the App Tunneling is enabled.

Unable to access Internal sites from managed apps through the VPN

Intranet websites are not accessible from the Tunnel Server.

1   Ensure that you can access the internal websites from the tunnel server. If it is a Cascade mode, the internal site must be accessible from the Backend server.

2   Ensure that all the application binaries are whitelisted for the VPN.For example, applications like VMware Horizon Client and Microsoft Outlook might have multiple binaries that need to be whitelisted.

Device Traffic Rules is not sent to the devices

Device Traffic Rules 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. In some scenarios, the updated Device Traffic Rules is not sent to the devices. When the administrator changes the Device Traffic Rules and click **Save**, the Device Traffic Rules gets mapped to the profile, but the updated Device Traffic Rules is not replaced for the devices where the VPN profile is already installed. Device Traffic Rules is only updated for the newly enrolled devices or for the devices that have the VPN profile reinstalled.

To send the updated Device Traffic Rules to the devices post modifying the Device Traffic Rules, administrators must click **Save and Publish**. Save and Publish adds a version to the VPN profile and republishes Device Traffic Rules to all the devices.

Note:

- If the adminsitartor changes the Android application in the Device Traffic Rules and clicks **Save and Publish**, the VPN profiles for both iOS, Android profiles gets a version update and the VPN profile installs are queued for all the assigned devices.

- Reinstalling the profile reissues the client certificate to the device with a new thumbprint.

VPN-Managed Application fails to honor Device Traffic Rules on Overriding the Device Traffic Rules

VPN-managed application fail to honor the Device Traffic Rules on overriding the Device Traffic Rules rules for the Child OG. The VPN profile fails to map the correct Device Traffic Rules configuration.

- Make sure that you create the application and the VPN profile at the OG level which has the traffic rules that are overridden.

Unable to view internal and public applications under the Device Traffic Rules application list

Internal and public applications are not displayed under the Device Traffic Rules application list.

You might encounter this issue if the VPN profile is not mapped with the correct Tunnel Configuration.

1   Navigate to **Profile** > **List View**.

2   Select the profile that is mapped to the application and click **VPN Payload**. Verify the Tunnel server configuration.

3   If the `Tunnel not configured` message is displayed, click **Add version** and remove the VPN payload.

4   Add a new VPN Payload.

Tunnel Server is not up to update with respect to the Compliance Change Events

Devices fail to honor compliance policy updates.

You might encounter this issue if the device compliance change event fails to reach the Tunnel server.

1   In the Workspace ONE UEM console, navigate to **All Settings** > **System** > **Advanced** > **Site Url**.

   a   Verify the AirWatch Cloud Messaging connection.

2   Perform the Tunnel test connection from the Tunnel configuration page.

3   From the Tunnel server, verify the service status by running the following commands:

   a   `systemctl status vpnd`.

   b   `systemctl status vpnreportd`.

> **Note**
>
> If you have multiple AirWatch Cloud Messaging that uses implicit clustering, configure the load balancer to use the cookie persistence that routes the AirWatch Cloud Messaging traffic.

Tunnel Front-End server fails to communicate with the Back-End server

Due to the incorrect network configuration or usage of an incorrect certificate for the server-client authentication, you might experience a communication failure between the Tunnel Front-End server and the Back-End server.

1 Ensure that the Front-End server can communicate with the Back-End Tunnel server on the port mentioned in the tunnel configuration.

2 Run the following command in the Tunnel Front-End server :

```
openssl s_client —connect <dest_fqdn>:<port> —servername
          <backend_fqdn>
```

.Must display the Tunnel Back-End server SSL certificate.

3 In the server.conf file, verify the following:

On the Tunnel, front-end server verify if the c_r_t (that is, cascade_root_thumbprint) has the thumbprint of the Back-End server's SSL certificate.

a The c_r_t in the Tunnel front-end server is same as the cascade_back_end_thumbprint in the Back-end server.

On the Tunnel back-end server c_r_t should have the root CA's thumbprint of the Tunnel front-end server's SSL certificate.

a When the AirWatch certificate is used for Server Auth, the c_r_t in the back-end server is always same as the ssl_thumbprint in the Tunnel front-end server.

b When a third-party SSL certificate is used for Server Auth, the c_r_t in the back-end server is the third party's root CA's thumbprint.

4 Verify if there are any firewall or load balancer rules blocking between the Front-End server to Back-End Tunnel Server.

Note

- SSL Offloading and SSL Bridging are not supported for the Per-App Tunnel configuration.

- If you are using Public certificate for the server authentication, the certificate must have a Server and Client authentication under **Enhanced Key Usage** field .

Unable to load and add Device Traffic Rules and Server Traffic Rules in the Tunnel configuration Page

When you load the Tunnel configuration page, `Tunnel Configuration doesn't exist` is displayed and you may not be able to add Device Traffic Rules or Server Traffic Rules.

1   Open the Internet Information Services (IIS) Manager on the API server.

   a   In the Windows Start menu, click Administrative Tools > **Internet Information Services (IIS) Manager**.

2   In IIS Manager, under Connections, expand your server name, and then expand **Sites**.

3   Right-click on a website, and click **Edit Bindings**.

4   In the **Site Bindings** window, select the http/https binding for this website, and click **Edit**.

5   In the **Edit Site Binding** window, keep the hostname blank , and click **OK**.

6   Restart the IIS sites for the changes to take effect.

7   Alternatively, instead of clearing the IIS bindings hostname and keeping the hostname blank, you can complete the following steps:

   a   Update the Tunnel microservice appsettings.json's `Host` key under the `AirWatchApiClient` to include the hostname that is used in the IIS bindings.

```
"AirWatchApiClient": {
    "Host": "acme.example.com",
    "ClientTimeoutInSeconds": 40,
    "HostDiscoveryTimeoutInSeconds": 30,
    "Port": 8081
```

   Note   The port key will only be used if the customer is using a custom port.

   b   Restart the Airwatch Tunnel Service

   c   Refresh the browser if you are using the Tunnel configuration screen after the service restart.

Verify VMware Tunnel Microservice

You can use the VMware Tunnel health endpoint to verify the upstream or downstream connectivity to the VMware Tunnel microservice.

1   Use the following REST API to get the VMware Tunnel microservice health from Workspace ONE UEM API Explorer.

```
GET {environment}/api/mdm/tunnel/health
aw-tenant-code: API key configured
Basic auth
```

2   Verify the API response of VMware Tunnel health endpoint.

```
200 ok
{
 "api_to_tunnel_microservice_connectivity": "True",
 "tunnel_microservice _to_api_connectivity": "True",
 "database_connectivity_status": "True"
}
```

Unable to upload third-party SSL certificate

You may not be able to upload third-party SSL certificate when the third-party library currently used for the encryption/decryption (BouncyCastle) fails to read the certificate password due to a pad block corrupted issue.

1   Import the non-working certificate onto the windows certificate store on the app server of the console where this issue is seen.

2   Once imported, export the certificate from the store with the same password if required. The exported certificate will be available on your local machine on the path you chose to save it.

3   Use this exported certificate for uploading on the third-party server authentication tab of the Tunnel configuration. The certificated should upload successfully and the Tunnel config can be saved.